

Assessing the Availability of Forensic Evidence from Social Networking Sites: Tool Capability

SAUD ABDULAZIZ ALSHAIFI
Bachelor of Computer and Information Sciences (AUT, NZ)

A thesis submitted to the graduate faculty of design and creative technologies
Auckland University of Technology
in partial fulfilment of the
requirements for the degree of
Masters of Forensic Information Technology

School of Engineering, Computer and Mathematical Sciences

Auckland, New Zealand
2016

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

.....
Saud Abdulaziz Alshaifi

Publications

Cusack, B., & Alshaifi, S. (2015). Mining Social Networking Sites for Digital Evidence, *In Proceedings of the 13th Australian Digital Forensics Conference*, (pp. 15-21). Perth, Western Australia.

Cusack, B., & Alshaifi, S. (2015). The Evidential Value of Social Networking Sites. *Digital Forensics Magazine*, (24), 26-30.

Acknowledgements

This thesis was completed at the Faculty of Design and Creative Technologies in the School of Engineering, Computer and Mathematical Sciences at Auckland University of Technology, New Zealand. First and foremost, I thank Allah the most gracious and the most merciful, for giving me the opportunity, strength, and determination to complete my thesis. His continuous blessings and grace helped me to believe in myself, and his continuous support to achieve what I dream of since I was a child.

I would like to thank my parents, my brothers, and sisters for their limitless support over the past years of my studies in New Zealand, I would like to thank my wife for her continuous support and courage during my thesis study, and for being positive and cheerful whenever I get into stressful times, and for her understandings whenever I am too late for coming home.

I would like to express my deepest gratitude to my supervisor, Dr. Brian Cusack, who has been supportive since the first day of my thesis. Dr. Cusack was there for me every time I needed, his opinions, discussions, critiques, motivations, sense of humour, helped me get through this thesis, without him I would not have achieved to this point. Likewise, I would like to thank Dr. Alastair Nisbet for being very supportive, and for his teachings of advanced knowledge on the fields of security and digital forensics during my postgraduate year. Dr. Nisbet has given me the opportunity to understand and prepare for the thesis year prior starting my own thesis.

In addition, I would like to thank the software vendors who provided free trial access to their tools who are SiQuest Corporation, Magnets Forensics, and Belkasoft. Also I would like to thank the Ministry of Higher Education in Saudi Arabia, and the Saudi Cultural Mission in New Zealand for providing me the scholarship, and for their continuous support.

Lastly, I would like to thank my friend Emad Alsaiani, for being supportive, and for sharing ideas, challenges, and solutions throughout my thesis.

Abstract

The evolution and popularity of Online Social Networking Sites (OSNSs) has produced a new platform for communications and collaborations. Features provided by OSNSs allow users to share information in different types of digital forms such as pictures, text messages, audios, and videos, and for different purposes of use such as social communication, advertisements, online dating, and learning. Due to the public space that OSNSs offer, many users have become psychologically attached to the continuous use of these sites, as they can freely share information about themselves including opinions, feelings, beliefs, locations, and relationships. Thus, OSNSs hold a vast amount of information about individuals, organizations, and governments.

OSNSs unfortunately are getting used for crime and illegal activities, including drug dealing, fraud, terrorism, child pornography and so on. Consequently, they have become a source of forensic evidence that can be used in courts of law. However, there is insufficient research that is focused on extracting forensic evidence from OSNSs, and also there are no forensic tools that are designed exclusively for OSNSs forensic investigation. Moreover, several digital forensic tools may have the ability to extract OSNSs artefacts but remain untested. Thus, it is crucial to review and evaluate the capability of these tools in extracting admissible forensic evidence.

The purpose of conducting this research is to evaluate three digital forensic tools in terms of recovering forensic evidence from Facebook, Twitter, Instagram, Bayt, and LinkedIn; and to identify the scope of evidence using three different browsers. This research also aims to identify the location and sources that store OSNSs forensic evidence. The testing research was conducted in a laboratory environment based on an exploratory approach. In the preliminary test, functions, and types of data acceptable in each OSNS are identified. Two separate case scenarios were used to generate data using three browsers and to populate the respective test sites. Digital forensic investigation was carried out using three digital forensic tools, which are validated using the SWGDE approach for tool validation testing. Browser files stored in the hard drive, RAM, and pagefile.sys were all examined by the three tools in order to assess the scope and the capabilities. Advice for forensic investigators and guidelines for forensic investigation of OSNSs were developed based on the data collected.

The findings from this research showed that extracting forensic evidence from OSNSs is difficult, as artefacts are stored in different locations that are variable. The choice of a web browser used to investigate OSNSs directly influences the scope of digital evidence obtained. Moreover, vital forensic evidence such as Facebook messages, Tweets, and wall posts can be recovered only from RAM and pagefile.sys. It was discovered that the selected digital forensic tools cannot extract the entire evidence available. This is due to the fact that OSNSs activities are not guaranteed to be stored on the computer system. However, the selected digital forensic tools have succeeded in reconstructing sufficient evidence that determines the possibility of illegal, and criminal activities through OSNSs. The findings show that some tools can recover private messages sent and received on Facebook, LinkedIn, and Bayt, and some tools can also recover the message metadata such as unique message ID, sender and receiver names and IDs, date and times of the messages.

The findings of this research provide a comprehensive understanding of the capability, strengths, and weaknesses of the selected tools, and the recoverable OSNSs forensic evidence, which can assist forensic investigators, and law enforcement personnel when conducting similar investigations. Opportunities for future research and development in the area of online social network forensics are also listed.

Table of Contents

Declaration	ii
Publications	iii
Acknowledgements	iv
Abstract	v
Table of Contents	vii
List of Tables.....	xi
List of Figures	xii
List of Abbreviations.....	xiv

Chapter 1: Introduction

1.0 BACKGROUND	1
1.1 MOTIVATION FOR RESEARCH	2
1.2 RESEARCH APPROACH AND FINDINGS	3
1.3 STRUCTURE OF THESIS.....	5

Chapter 2: Literature Review

2.0 INTRODUCTION	8
2.1 DIGITAL FORENSICS	9
2.1.1 Definition of Digital Forensics	10
2.1.2 Goal of Digital Forensics	11
2.1.3 Digital Forensics Investigation Process	11
2.2 DIGITAL EVIDENCE.....	15
2.2.1 Definition of Digital Evidence.....	15
2.2.2 Characteristics of Digital Evidence	16
2.2.3 Admissibility of Digital Evidence	17
2.3 ONLINE SOCIAL NETWORKS	18
2.3.1 Overview of Online Social Networks	18
2.3.2 Features of Online Social Networks	20
2.3.3 Popular Online Social Networking Sites	22
2.3.4 The Impact of Online Social Networks on Societies	24
2.3.5 Online Social Networks Usage by Country	25
2.3.5.1 New Zealand.....	25
2.3.5.2 Saudi Arabia	26
2.3.5.3 United States of America	26

2.3.6	Online Social Networks Forensics.....	27
2.3.7	Digital Evidence in Online Social Networking Sites.....	28
2.4	DIGITAL FORENSIC TOOLS	30
2.5	EVALUATION OF ONLINE SOCIAL NETWORKS FORENSIC TOOLS	33
2.5.1	Belkasoft Evidence Center.....	33
2.5.1.1	Core Capabilities & Features of Belkasoft Evidence Center	34
2.5.2	Internet Evidence Finder (IEF)	34
2.5.2.1	Core Capabilities & Features of Internet Evidence Finder	34
2.5.3	Internet Examiner Toolkit (IXTK)	35
2.6	SUMMARY OF ISSUES AND PROBLEMS.....	35
2.6.1	Lack of Standardization.....	36
2.6.2	Lack of Online Social Networks Forensic Tools.....	36
2.6.3	Jurisdictional Issues across Borders	37
2.6.4	Admissibility of Evidence Collected from OSNSs	37
2.7	CONCLUSION	37

Chapter 3: Research Methodology

3.0	INTRODUCTION	39
3.1	REVIEW OF SIMILAR STUDIES	39
3.1.1	Computer Forensics Guidance Model with Case Study	41
3.1.2	General Testing Methodology for Computer Forensic Tools.....	44
3.1.3	Recommended Guidelines for Validation Testing by SWGDE	45
3.1.4	Validation of Computer Forensic Software Utilizing Black Box Testing Techniques.....	46
3.1.5	Digital Forensics Investigation Methodology Applicable for Online Social Networks	49
3.2	RESEARCH DESIGN	50
3.2.1	Summary of Similar Studies	50
3.2.2	Review of the Problems and Issues	51
3.2.3	The Research Questions and Hypotheses	52
3.2.4	Research Phases	54
3.2.5	Data Map.....	56
3.3	DATA REQUIREMENTS.....	57
3.3.1	Data Collection	57
3.3.2	Data Processing.....	59

3.3.3	Data Analysis	59
3.3.4	Data Presentation	61
3.4	LIMITATIONS	61
3.5	CONCLUSION	62

Chapter 4: Research Findings

4.0	INTRODUCTION	64
4.1	VARIATION AND MODIFICATION ENCOUNTERED	65
4.1.1	Data Collection	65
4.1.2	Data Processing.....	66
4.1.3	Data Analysis	67
4.1.4	Data Presentation	67
4.2	ONLINE SOCIAL NETWORK PRELIMINARY TESTS	67
4.2.1	Facebook	68
4.2.2	Twitter.....	70
4.2.3	Instagram	72
4.2.4	LinkedIn.....	73
4.2.5	Bayt.....	74
4.2.6	Findings of Preliminary Test	75
4.2.7	Online Social Networks: Environments Setup & Case Scenarios	76
4.2.7.1	First Case Scenario (Public Threat).....	78
4.2.7.2	Second Case Scenario (Policy Breach)	78
4.2.8	Conclusion	79
4.3	FIRST CASE SCENARIO - PUBLIC THREAT	79
4.3.1	Forensic Investigation Environment Setup.....	80
4.3.2	Digital Forensics	81
4.3.2.1	Evaluation and Assessment	82
4.3.2.2	Acquisition of Evidence	82
4.3.2.3	Survey of Digital Scene.....	83
4.3.2.4	Digital Evidence Examination.....	83
4.3.2.5	Reconstruction of Extracted Data.....	88
4.3.2.6	Conclusion.....	99
4.3.3	Comparative Analysis.....	100
4.4	SECOND CASE SCENARIO – POLICY BREACH.....	101
4.4.1	Forensic Investigation Environment Setup.....	102

4.4.2	Digital Forensics	102
4.4.2.1	Evaluation and Assessment	102
4.4.2.2	Acquisition of Evidence	102
4.4.2.3	Survey of Digital Scene.....	103
4.4.2.4	Digital Evidence Examination.....	103
4.4.2.5	Reconstruction of Extracted Data.....	106
4.4.2.6	Conclusion.....	109
4.4.3	Comparative Analysis.....	109
4.5	CONCLUSION	110

Chapter 5: Discussion of Findings

5.0	INTRODUCTION	112
5.1	RESEARCH QUESTIONS AND HYPOTHESES	112
5.1.1	Sub-Questions.....	113
5.1.2	Hypotheses Testing.....	118
5.1.3	The Research Question	122
5.2	DISCUSSION	124
5.2.1	Discussion of the Case Scenarios Environment	124
5.2.2	Discussion of the Findings for Tool Evaluation	126
5.2.2.1	Belkasoft Evidence Center	126
5.2.2.2	Internet Examiner Toolkit	128
5.2.2.3	Internet Evidence Finder	130
5.2.3	Method Recommendations	132
5.3	CONCLUSION	133

Chapter 6: Conclusion

6.0	INTRODUCTION	135
6.1	SUMMARY OF RESEARCH	135
6.2	LIMITATION OF RESEARCH	138
6.3	FUTURE RESEARCH	139
	REFERENCES	142
	APPENDICES	151

List of Tables

Table 2.1: Previous & Current Digital Forensic Investigation Process Models (Adapted and updated from Mumba & Venter, 2014, p.85)	14
Table 2.2: Types of Users' Data that can be found in OSNSs. (Adapted from Schneier, 2010, p.88)	20
Table 2.3: Core Characteristics of Online Social Networks	21
Table 2.4: Facebook Formats	22
Table 2.5: Digital Forensic Tools Categorized in Terms of Their Usage	31
Table 4.1: Types of Data Can be collected from Facebook	69
Table 4.2: Types of Data Used in the Experiments	75
Table 4.3: Detailed Web Browsers and Versions Used in the Experiment	77
Table 4.4: Detailed Hardware and Software Specifications	81
Table 4.5: Comparative Analysis for Facebook & Instagram Activities	100
Table 4.6: Comparative Analysis for Twitter & Instagram Activities	101
Table 4.7: Comparative Analysis for LinkedIn Activities	110
Table 4.8: Comparative Analysis for Bayt Activities	110
Table 5.1: Sub-Question 1 and Answer	113
Table 5.2: Sub-Question 2 and Answer	114
Table 5.3: Sub-Question 3 and Answer	114
Table 5.4: Sub-Question 4 and Answer	115
Table 5.5: Sub-Question 5 and Answer	116
Table 5.6: Sub-Question 6 and Answer	117
Table 5.7: Hypothesis Testing 1	118
Table 5.8: Hypothesis Testing 2	119
Table 5.9: Hypothesis Testing 3	121
Table 5.10: Hypothesis Testing 4	121

List of Figures

Figure 2.1: Top 5 Browsers in the Market Share (Net Market Share, 2015)	29
Figure 2.2: Screenshot of Internet Examiner Toolkit Capability for OSNSs	35
Figure 3.1: Computer Forensics Guideline Model (Noureldin, Hashem and Abdalla, 2011, p.564)	42
Figure 3.2: Acquiring Digital Evidence (Noureldin, Hashem and Abdalla, 2011, p.564)	43
Figure 3.3: Stages of Digital Forensics Phase (Noureldin, Hashem and Abdalla, 2011, p.566)	44
Figure 3.4: Proposed General Methodology for Testing Computer Forensic Tools (NIST, 2001, p.2)	45
Figure 3.5: Plan for the Testing Environment (Whittaker, 2000)	47
Figure 3.6: Evaluation Process for Forensic Computing Tools (Wilsdon & Slay, 2006)	47
Figure 3.7: The Proposed Methodology for OSNSs Forensics Investigation (Jang & Kwak, 2014, p.3)	49
Figure 3.8: Research Phases	55
Figure 3.9: The Proposed Research Data Map	56
Figure 4.1: Facebook Timeline Page (Profile Page) Layout	68
Figure 4.2: Twitter Homepage Layout	71
Figure 4.3: Instagram Homepage Layout	72
Figure 4.4: LinkedIn Homepage Layout	74
Figure 4.5: Bayt Homepage Layout	75
Figure 4.6: HD Acquisition Using Tableau Imager & eSATA Forensic Bridge	82
Figure 4.7: HD Acquisition & Verification Process	83
Figure 4.8: RAM Processed and MD5 Calculation & Verification	84
Figure 4.9: Evidence Extracted Using Belkasoft Evidence Center	85
Figure 4.10: Evidence Extracted Using Internet Examiner Toolkit	86
Figure 4.11: Data Carving in IXTK	86
Figure 4.12: Evidence Extracted Using Internet Evidence Finder	87
Figure 4.13: Evidence for Facebook Chats Extracted in Belkasoft	89
Figure 4.14: Facebook Chats Extracted in IXTK Received Using Firefox	90
Figure 4.15: Facebook Chats Extracted in IXTK Received Using Chrome	90

Figure 4.16: Facebook Chats Extracted by IEF	91
Figure 4.17: Evidence Found on Belkasoft for Facebook & Instagram (RAM & Pagefile.sys)	92
Figure 4.18: Evidence Found on Belkasoft for Facebook & Instagram (HD)	93
Figure 4.19: Evidence Found for Facebook & Instagram & Twitter from RAM.....	94
Figure 4.20: Evidence Found for Facebook & Instagram & Twitter from HD	94
Figure 4.21: Facebook & Instagram Evidence Reconstructed From RAM & Pagefile.sys on IEF	95
Figure 4.22: Facebook & Instagram Evidence Reconstructed from HD on IEF	96
Figure 4.23: Evidence Found on Belkasoft for Twitter & Instagram (RAM & Pagefile.sys)	98
Figure 4.24: Evidence Found on Belkasoft for Twitter & Instagram (HD)	98
Figure 4.25: Evidence Found on IEF for Twitter & Instagram (RAM & Pagefile.sys)	99
Figure 4.26: Evidence Found on IEF for Twitter & Instagram (HD)	99
Figure 4.27: Evidence Extracted Using Belkasoft Evidence Center.....	104
Figure 4.28: The LinkedIn Evidence Extracted From IXTK.....	104
Figure 4.29: Evidence Extracted Using Internet Evidence Finder.....	105
Figure 4.30: LinkedIn Evidence Found from RAM on Belkasoft	106
Figure 4.31: LinkedIn Evidence Pictures from RAM on IEF.....	106
Figure 4.32: LinkedIn Evidence Found from HD on Belkasoft.....	107
Figure 4.33: Bayt Evidence Recovered from RAM on Belkasoft	108
Figure 4.34: Bayt Evidence Recovered from HD on Belkasoft.....	109

List of Abbreviations

CFTT	Computer Forensic Tools Testing
DBAN	Darik's Boot and Nuke
DD	Disk Dump
DFRW	Digital Forensics Research Workshop
DNA	Deoxyribonucleic Acid
ESD	Electrostatic Discharge
EVS	Evidentiary Value Scoring
EXT2	Second Extended File System
F2FS	Flash-Friendly File System
FAT	File Allocation Table
FTK	Forensic Toolkit
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface
HD	Hard Drive
HEX	Hexadecimal
HFSX	Hierarchical File System (HFS)
HTML	Hyper Text Markup Language
ID	Identity
IE	Internet Explorer
IEEE	Institute of Electrical and Electronics Engineers
IEF	Internet Evidence Finder
ISO	International Organization for Standardisation
IT	Information Technology
IXTK	Internet Examiner Toolkit
MD5	Message Digest algorithm 5
NIJ	National Institute of Justice
NIST	National Institution of Standards and Technology
NTFS	New Technology File System
OS	Operating System
OSNSs	Online Social Networking Sites
PC	Personal Computer

PDA	Personal Digital Assistant
PDF	Portable Document Format
RAM	Random Access Memory
SATA	Serial Advanced Technology Attachment
SHA1	Secure Hash Algorithm version 1
SQL	Structured Query Language
SWGDE	Scientific Working Group on Digital Evidence
TSWG	Technical Support Working Group
UI	User Interface
URL	Uniform Resource Locator
XCML	eXtensible Critter Markup Language

Chapter 1

Introduction

1.0 BACKGROUND

Online Social Networking Sites (OSNSs) have become very popular among people all over the world. They have become indispensable to many online users to be connected with others through OSNSs. There are many different online social networks with different purposes of use but all communicate information about the individual and their networks of association. Many users of these sites have become psychologically attached to the interaction and the self-promotion to a point where they freely post information about themselves, including pictures, status, comments, likes, locations, beliefs, opinions, and feelings. Some of these communications may be exaggerations or fabricated using information tools but many users are simply conveying stories in various forms about themselves and their communities. Moreover, Users tends to share information for different purposes, such as for communication with others, advertisements, business promotions, and so on. According to Cheung and Lee (2010), “Participation and continuance in online social networks represents a new social phenomenon that depends largely on the interactions with other users in a personal network” (p.24).

There are many cases where people have used OSNSs to reveal their admission of committing offenses. Often the motivation is to brag or to seek popularity. Zainudin, Merabti and Llewellyn-Jones (2010) indicated that the emergence, and growth of online social networks have resulted in an increase in their use for cyber-criminal activities. Evans (2015) from “The Telegraph” reported that more than 16000 alleged crimes involving Twitter and Facebook social networks were reported to the British police during 2014. This indicates that OSNSs have become a host to many criminals for their illegal activities, and crimes. From a forensic point of view, OSNSs are a potential source of forensic evidence that can help during investigations (Mulazzani, Huber & Weippl, 2012). This is due to the vast amount and types of data that can be found from each OSNS. However, due to dynamic nature of OSNSs, obtaining

evidence can be challenging. The recovering of forensic evidence from OSNSs depends on several variables, such as the web browser used by the suspect, the status of the computer when seized, the acquired sources to be investigated, and the digital forensic tools that are used for examinations and analysis.

The literature reviewed in this research shows that there is no standardized model, or forensic tools specified for OSNSs forensic investigation. The aim of this research is to test, evaluate, and compare the capabilities of three digital forensic tools in extracting forensic evidence from five OSNSs, which are Facebook, Twitter, Instagram, LinkedIn, and Bayt. The research also aims to identify whether the recoverable evidence using the selected forensic tools, may vary depending on the browser used by the suspect. Recovering OSNSs artefacts is difficult, because the artefacts can be stored in different locations such as the hard drive and in browser files, RAM, and the pagefile.sys. In this research, these sources are to be examined and analysed using three digital forensic tools, in order to answer the research questions and hypotheses presented in Section 3.2.3. The main research question proposed for the research is:

What evidence can be extracted from online social networking sites when using different forensic extraction tools?

1.1 MOTIVATION FOR RESEARCH

In criminal cases, such as homicide, Fraud, Sexual assaults, possession of drugs, terrorist attacks and so on, digital devices owned by the suspect such as Desktop Computers, laptops, mobile phones, and PDAs are target objects for forensic seizure, and examination for forensic evidence. According to Al-Zaidy, Fung, Youssef, and Fortin (2012) examining a digital device may help in finding crucial evidence related to a case. They may also provide important data about the suspect's OSNSs activities, and communications, in which other suspects involved in the criminal case may be identified. Moreover, OSNSs are currently used as a tool by several law enforcement agencies in order to collect forensic evidence such as pictures, wall posts, GPS locations, messages, and videos. Law enforcement use OSNSs such as Facebook in order to run a search on a particular suspect using search engines (Hayes, 2011). However, what would happen if criminals do not use their own names for their OSNSs accounts, and they disabled search results for their accounts? Law enforcement

agencies will no longer be able to retrieve any information about them using a search engine. When a criminal is detained, and denies that they have any association to a crime, neither relations with other criminals, and denies that they have any accounts on OSNSs, it is still possible to prove or disprove these allegations by examining their machines. Further examinations of suspect's devices can recover suspicious, illegal, or criminal activities performed on OSNSs, including recovering private messages sent to other suspects, photos, videos, wall posts, and shared links. Thus, the requirement for a forensic investigation of OSNSs is necessary.

Moreover, forensic investigators are relying on digital forensic tools, which are developed to acquire, process, examine, and analyse forensic evidence from general digital devices. Although, digital forensic tools can examine and recover digital evidence from digital devices, there are not any digital forensic tools that are exclusively specified for OSNSs forensic investigation. This is because OSNSs is relatively new area, and OSNSs artefacts and activities are not stored on the digital devices like typical files, such as PDF and documents files which are stored on the hard drive. Moreover, most of the data posted and activities performed, are stored on the OSNSs provider's servers. There are few digital forensic tools that may extract OSNSs artefacts from different sources of evidence such as from the hard drive, browser files, RAM, and pagefile.sys (Swap file).

The prime motivation for conducting this research is to identify and evaluate three digital forensic tools, and their capabilities in terms of recovering forensic evidence from OSNSs. It is to also explore the scope of evidence available in the selected online social networks, and the source location of each type of evidence that is posted online. The researcher is motivated to gain a better understanding of what the selected digital forensic tools can offer to the forensic investigator during a forensic investigation of OSNSs. Tools performance is of interest when similar cases happen in real life scenarios where Facebook, Twitter, Instagram, LinkedIn, and Bayt are used for committing crimes.

1.2 RESEARCH APPROACH AND FINDINGS

In order to answer the main research question proposed for this thesis, and to ensure that the proposed research is conducted with an appropriate and effective methodology, exploratory research is proposed. The research methodology has been

developed from a review of five relevant studies that have been previously published. Six associated sub-questions that are related to the investigation environment and problem area were developed. Four hypotheses have been developed for the purpose of verifying the validity of the research findings, and to assist in answering the main research question.

The proposed research phases are developed based on the exploratory approach, and designed to evaluate the selected digital forensic tools in a systematic and forensically trusted manner. The investigation and analysis of the collected data forms a major part of the research. This research consists of five phases. In the first phase, a preliminary test of OSNSs is conducted in order to identify their functionalities (Definition of term: The range of operations that can be run on a computer or other electronic system), capabilities, and to recognize the types of data that are allowed to be posted on each OSNS. Based on this phase, case scenarios are then developed which are designed to be as similar as possible to real world scenarios. Prior to posting data on OSNSs, the target machine was wiped (Zeroed) using Darik's Boot and Nuke (DBAN) in order to ensure that any previous artefacts were fully removed. Subsequently, data is placed using three different browsers on the selected OSNSs, and documented as controlled data. The second phase was developed using a method of tool validation testing proposed by SWGDE. In this phase, test plans were developed which include the purpose of the test, the scope, requirements to be achieved, expected results, and the test scenarios. In the third phase, the computer forensic guidelines methodology proposed by Nouredin, Hashem and Abdalla (2011) was adopted for conducting the experiential forensic investigation. In the fourth phase, the data is reconstructed on the previous phase to conduct a comparative analysis between the controlled data generated in the first phase with the forensic evidence reconstructed from each tool. The method recommendations are delivered in the fifth phase.

The research found that extracting forensic evidence from OSNSs is a complex task, and that OSNSs artefacts are typically not stored on the target's hard drive. This research showed that the selected tools have succeeded in reconstructing crucial forensic evidence from the selected OSNSs. In addition, the results showed that the recoverable OSNSs evidence varies depending on several factors. These factors are: which browsers have been used by the suspect, the source of evidence acquired and examined by the investigator, and the tool used for data examination and

reconstruction. The research findings show that certain activities cannot be recovered at all. However, most of the activities simulated in both case scenarios can still be recovered. In this research, it has been proven that private messages sent to another person on Facebook, LinkedIn, and Bayt are recovered, but cannot be recovered on Twitter.

The research found that Belkasoft Evidence Center is the most efficient tool among the other two tools when conducting a forensic investigation on Twitter, LinkedIn, and Instagram, followed by Internet Evidence Finder (IEF), and then Internet Examiner Toolkit (IXTK). For Facebook and Bayt activities, IEF is the most efficient tool, followed by Belksoft Evidence Center, and then IXTK. Although IXTK succeeded in recovering some artefacts from Facebook, Twitter, and Instagram. It was not satisfactory in recovering forensic evidence from Bayt and LinkedIn. There were several concerns regarding recovering forensic evidence using IXTK. The most notable issue is that the activities performed using Chrome, and Firefox were recovered, but the source of evidence was incorrectly presented in Internet Explorer (IE) browser files. This is because IXTK has only included IE files artefacts to be carved. In addition, the researcher also discovered a software bug that directly affects the bookmarking evidence process, and notified the software vendors. The bug has been confirmed and fixed by the software vendor in their newer release.

The research found that Belkasoft scored 1st in terms of identifying and presenting the locations of evidence, IEF scored 2nd and IXTK 3rd. Moreover, IEF scored 1st in terms of recovering accurately the evidence metadata including date/time of the evidence (activities) posted by the suspect, Belkasoft 2nd, IXTK 3rd. The findings of this research show that OSNSs artefacts can be recovered without help from the OSNSs's providers. In addition, the scope of forensic evidence will vary deepening on the status of the machine when seized, and depending on whether the investigator was able to acquire RAM and pagefile.sys from the system. Other crucial evidence such as Facebook messages, Tweets, and wall posts can be recovered only from RAM and pagefile.sys.

1.3 STRUCTURE OF THESIS

This thesis is organized into 6 Chapters: 1. Introduction 2. Literature Review 3. Research Methodology 4. Research Findings 5. Discussion of Findings 6. Conclusion.

Chapter 1 introduces the area of research, and gives a brief introduction about OSNSs and digital forensic investigations, and tools. Moreover, the Chapter introduces the importance, the background, and the motivations for this research, along with the research approach.

Chapter 2 presents a comprehensive literature review of recent research studies in the area of digital forensic investigation relevant to online social networks. Areas reviewed by Chapter 2 include digital forensics, digital evidence, online social networking sites (OSNSs), forensic evidence in OSNSs, digital forensic tools, and a review of investigation process that is related to the research area. Chapter 2 concludes by summarizing the issues and problems that are encountered when conducting a forensic investigation for OSNSs.

In Chapter 3, five approaches that are similar to the chosen research field are studied and evaluated, in order to assist the researcher in developing and adopting a suitable research method for the proposed research. Furthermore, the research sub-questions, hypotheses, data requirements, and the limitation of the proposed research are presented in this Chapter.

Chapter 4 presents the research findings. The first section in this Chapter is to identify and discuss the changes encountered during the field-testing. The changes to data collection, data processing, data analysis and presentations are reviewed. The second section presents the findings of the OSNSs preliminary test, the environment setup for conducting the experiment, and the created case scenarios. The third section presents the results of data collection, processing examination, analysis and presentations for the first case scenario which involves Facebook, Twitter, and Instagram, the results from each digital forensic tool, and the comparative analysis. The fourth section presents the findings results of the second case scenario where LinkedIn and Bayt are involved in the digital forensic investigation, Comparative analysis were also given for the second case scenario.

Chapter 5 discusses the key findings presented in Chapter 4, answers the research sub-questions, tests the asserted hypotheses with arguments for and against, and ultimately answers the main research question. Chapter 5 also presents a comprehensive discussion based on the findings presented in Chapter 4, from each digital forensic tool, and provides each tool's capabilities, strength and weaknesses, and limitations. Chapter 5 also delivers a critical reflection on the thesis, where the experiment results presented in Chapter 4 are reconciled with the reviewed literature

in Chapter 2. Finally, the Chapter concludes with method recommendations for OSNSs forensic investigation.

Chapter 6 concludes the thesis as a whole. In this Chapter, a summary of research findings is presented, followed by an analysis of the limitations of the conducted research and investigation environment. The Chapter then concludes with providing recommendations for further research opportunities and development in the area of online social network forensics. The suggestions provide for future research in and around the gaps identified in the discussion of findings, and the evaluated limitations. In addition, the references and Appendices are presented after this Chapter as supplementary information. The Appendices include the controlled data, forensic image acquisitions and verifications, test plans, generated forensic reports from three digital forensic tools, and additional results gathered from the conducted experimentations.

Chapter 2

Literature Review

2.0 INTRODUCTION

The greater use of online social networking sites (OSNSs) has produced many different ways of communication between people. Features provided by the online social networks enabled users to be more interactive, and more interested in sharing their daily lives experiences. However, they provide evidence for law enforcement, since it is getting widely used for suspicious activities including drug dealing, terrorism, cybercrime activities and knowledge distribution. According to Zainudin, Merabti and Llewellyn-Jones (2010) cyber-criminal activities have been increased due to the rapid increase of users who interact with online social networks. According to Lau, Xia and Ye (2014, p.32) OSNSs have played a role in distributing cyber-attack information between hackers. Thus the motivation for other hackers may increase the number of attacks by following links, downloading distributed plans, and using these resources by either using the downloaded tools, or redistributing information to others. The tools and information that are visited or download from OSNSs may be stored within the computer which can be presented as evidence in courtrooms.

The objective of this Chapter is to gain a comprehensive understanding of the recent literature on digital forensics investigation, and the digital evidence that can be found in OSNSs. To define the scope of this Chapter, the area of focus in this literature review will be based on digital forensics, digital evidence, online social networking Sites (OSNSs), digital forensic tools, and a review of investigation process that is related to the topic. This literature review will also provide a summary of issues and problems that are identified in order to produce areas of focus for possible research.

Chapter 2 consists of 7 sections. Section 2.1 discusses the past and present of digital forensics, its definition, what are the goals of digital forensics, and reviews the processes of digital forensic investigations. Section 2.2 discusses digital evidence, its characteristics, and when digital evidence can be acceptable and admissible in court rooms. Section 2.3 introduces online social networks, their usage across different countries, their characteristics, impacts on modern societies, and discusses online

social networks forensics. The issue of OSNSs use for committing crimes is followed by a review of how to collect digital evidence from OSNSs. Section 2.4 and 2.5 discusses and evaluates a number of well-known digital forensic tools, and tools that can be used for investigation of OSNSs. Section 2.6 presents a summary of issues and problems that are related to OSNSs forensic investigations. Section 2.7 concludes the Chapter.

2.1 DIGITAL FORENSICS

Dictionaries defined the term forensic as collecting or obtaining evidence that can be suitable to be presented in courts of law and public debates. It is also defined as the process of obtaining information and knowledge by revealing rudimentary evidence (Civie & Civie, 1998). The consistency between the practices of modern forensic specialists and these two concepts is explicit, as forensic specialists may use suitable tools and procedures in order to extract evidence that may not be found by a regular observation. Hence, finding evidence from a crime scene may not constitute a forensic achievement. For example, when finding a man covered with a blood in crime scene, and identifying a knife at the same crime scene as the weapon used for committing the crime may not be a forensic act. In fact, it should be derived from comparing the samples of the blood on the knife and the body by conducting DNA test, thus gaining a knowledge and evidence based on revealing rudimentary evidence is called a forensic activity.

The early use of forensic techniques dates back to 2000 B.C. where the Babylonians used fingerprints as a brand marked on cuneiform tablets and clay pottery to identify the person who made them. The Babylonians were the first civilization that used fingerprints for the purpose of identifying criminals in 1792-1750 BC (Ashbaugh, 1991). Forensic Science has different branches including forensic anthropology, entomology, biology, and computer forensics. Computer forensics mainly deals with crimes related to computers. However, with the rapid development of technology, and digital world that allow users to perform different types of activities, including activities that may be treated as evidence or a trail of evidence, computer forensics has been extended to cover many types of digital technologies that are currently being used, and hence, is now called digital forensics. Moreover, there are different areas that digital forensics covers which include web and internet forensics, mobile

forensics, network forensics, and the new areas which recently emerged which are social networking forensics and cloud computing forensics (Chen, Xu, Yuan & Shashidhar, 2015).

2.1.1 Definition of Digital Forensics

As computer forensic services is limited to dealing with traditional computers, digital forensics is a more contemporary expression and more comprehensive in description. Caloyannides, Memon and Venema (2009) stated that computer forensics only performed a static analysis on one single compromised computer whereas there is other dynamic information that is not obtainable such as connecting to networks and performing a live forensic investigation. There are many devices that have been merged into new technology such as smartphones, iPads, PDAs, printers, and digital cameras. Currently, the term digital forensics represent the recent state of the IT forensics environment as it refers to investigations of any recent digital device. Palmer (2001) defined digital forensics as:

“The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations” (Palmer, 2001, p.16).

There are many other definitions of digital forensics according to Jeong (2006). This is because each definition is restricted to the perception of the individual who is involved in an investigation. However, some common elements may be found in different definitions to exhibit the meaning of digital forensics. Venter, Labuschagne and Eloff (2007) stated that digital forensics is determining potential evidence through the application of computer investigations, analysis and techniques. Willassen and Mjolsnes (2005) defined digital forensics as:

“The practice of scientifically derived and proven technical methods and tools toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of after-the-fact digital information derived from digital sources for the purpose of facilitating or furthering the reconstruction of events as forensic evidence” (Willassen & Mjolsnes, 2005, p.92)

2.1.2 Goal of Digital Forensics

Generally, Digital Forensics aims to identify any type of evidence stored in any type of digital media. Evidence may have different formats whether if it is stored as pdf, pictures, emails, logs and so on. However, any investigations must follow an investigation process and scientifically proven methods for collecting evidence whether it is physical or digital evidence in order to draw conclusions that can be presented in courts of law (Carrier, 2009). Digital forensics is used in many types of investigations including unauthorized access to corporates computers, child pornography, and any typical crime that involves the use of computers. The goal of digital forensics is not only identifying evidence, but also keeping that evidence in its original form when it has been collected. The following section discusses the development of digital forensic investigation processes, and reviews recently proposed models. A further discussion on digital evidence, and credibility of evidence will be given in Section 2.2

2.1.3 Digital Forensics Investigation Process

Throughout the years, many digital forensic investigation frameworks have been proposed. Each of these investigation processes have a different number of phases or steps. However, the objective remains similar, which is ensuring that the phases will assist in evidence that can potentially be accepted in legal courts.

Digital Forensics Research Workshop (DFRW) recommended seven phases for digital forensics process which are: identification, preservation, collection, examination, analysis, presentation, and decision. (Palmer, 2001). Reith, Car and Gunsch (2002) have expanded the DFRW model to 9 phases: Identification, preparation, Approach Strategy, Preservation, Collection, Examination, Analysis, Presentation, and Returning Evidence (Reith, Car & Gunsch, 2002, p.6).

The integrated digital investigation process proposed by Carrier and Spafford (2003). The proposed model has applied investigation procedures used in the crime scene to the examination of computers. The proposed model consist of 17 phases, which are organized into 5 groups: phase 1: Readiness, phase 2: Deployment phase, phase 3: Physical crime scene investigation phase, phase 4: Digital crime scene investigation and the lastly phase 5 which is Reviewing. Beebe and Clark (2005) proposed a hierarchical objective based framework which consists of six phases:

preparation phase, incident response, data collection, analysis of data, presentation of the findings, and the last phase which is incident closure, where legal actions are taken. National Institution of Standards and Technology (NIST) published a guide to internet forensic techniques for incident response. They stated that regardless of the situation, there are four basic phases that are included in forensic process, which are 1. Collecting, identifying and labelling data from possible sources, 2. Examination of the collected data with keeping integrity, 3. Analysing the result of the examination and 4. Reporting the result of analysis, including the actions, methods used, and explaining how to procedures and the tools used during the investigation were selected and used. Similar process proposed by the National Institute of Justice (NIJ, 2008) which consist of four core phases 1.Collection, 2.Examination, 3: Analysis, and 4: Reporting (NIJ, 2008).

Recently, several digital forensic investigation processes have been proposed, such as the systematic digital forensic investigation model that was proposed by Agarwal, Gupta, Gupta and Gupta (2011). The proposed model consists of 11 phases. These phases include identifying processes such as communication shielding, and differentiating between volatile and non-volatile evidence in the collection phase. The phases consist of: “1. Preparation 2. Securing the scene 3. Survey and recognition 4. Documenting the scene 5. Communication shielding 6. Evidence collection 7. Preservation 8. Examination 9. Analysis 10. Presentation 11. Result and review” (Agarwal, Gupta, Gupta & Gupta, 2011, p.127).

One of the most recent digital forensic investigation processes proposed by Shrivastava and Gupta (2014). They recommended a model for forensic investigators, which they stated that it will help them to accomplish the investigation in an appropriate structured manner that ensures evidence will not be lost during the investigation. The proposed approach consists of several process which are organized into five phases, the outcome of each current phase will become an input to the following phase. This ensures that each phase of the investigation has to be successful in order to continue with the next phases of the investigation. The recommended model starts with Requesting an audit. In this phase, the infected organization request conducting a forensic investigation from police, forensic team, or assessment team working in the organization. Secondly, a Bureau of Investigation should respond to the request on whether the audit or forensic investigation will take place or not, based on the event description. The benefit of this phase is to build a foundation of the event

before continuing for investigation. The second phase is (planning) where a comprehensive plan is made of the activities, and steps that will be conducted during the investigation. The third phase is (Investigation) which has four processes to be accomplished: 1. Identify all the evidence that are collected from the crime scene. 2. Probing, where investigators search any data that are relevant to the case from the collected data. 3. Sieving, where the investigator dispose any irrelevant or unnecessary data and focus on the relevant ones. Irrelevant data includes any data that does not hold or provide any clues about what the forensic investigators are looking for (Beebe & Clark, 2007). 4. After discarding irrelevant data, the rest of the data are preserved in order to provide integrity, and confidentiality to the data. The next phase (Analysis) where the data are examined with reliable tools. After the data is examined and analysed, a report containing scrutinised data is prepared, which includes evidence, and suspects involved in the case. Phase 5: Presentation is the last phase of the investigation, which is presenting the document prepared in the previous phase to the jury, judge, or the higher authority of the organization if it is an internal investigation.

As shown above that each digital investigation process has its own phases and frameworks. Throughout the years, the proposed models are getting expanded in terms of the number of phases that should be considered. However, they all share the same distinct goals (Beebe & Clark, 2005) which are:

- 1 Achieve scientific consistency and relevance;
- 2 Facilitating to understand the underlying structure by simplifying complex processes;
- 3 Keep an adequate amount of granularity; and,
- 4 Precisely describe standards, practices and concepts.

Despite the number of phases proposed by many authors, there are some common phases in digital forensic investigations which are: 1. Preparation of the case, phase 2. Collection and preservation, 3. Examination and Analysis 4. Presentation and reporting, and 5. Incident closure. A summary of several digital forensic investigation processes frameworks are presented in Table 2.1 The summary shows the phases proposed by each model.

Table 2.1: Previous & Current Digital Forensic Investigation Process Models (Adapted and updated from Mumba & Venter, 2014, p.85)

Process model name	Reference	Phases
A Road Map of Digital Forensics Research	DFWRS (2001)	7 Phases
Electronic Crime Scene Investigation- A Guide for First Responders	DOJ (2001)	8 phases
An examination of Digital forensic models	Reith et al (2002)	9 phases
Incident Response & Computer Forensics	Mandia et al (2003)	11 phases
Getting Physical with the Digital Investigation Process	Carrier & Spafford (2003)	5 Groups, 17 Phases
An Extended Model of Cybercrime Investigation	Cuardhuain (2004)	12 phases
A Hierarchical, Objectives-Based Framework for the Digital Investigation Process	Beebe & Clark, (2005)	6 phases
NIJ Investigation process: a guide for first responders	NIJ (2008)	4 phases
Good Practice Guide for Computer-Based Evidence	ACPO (2008)	13 phases
A Chapter in Forensic Analysis, in: Handbook of Digital Forensics and Investigation	Casey et al (2010)	4 phases
Fundamentals of Digital Forensic Evidence, Chapter in Handbook of Information and Communication Security	Cohen (2011)	11 phases
systematic digital forensic investigation model	Agarwal, Gupta, Gupta & Gupta, 2011	11 phases
Harmonized Digital Forensic Investigation Process (HDFIP) model	Valjarevic and Venter (2012)	14 phases
An Encapsulated Approach of Forensic Model for Digital Investigation	Shrivastava & Gupta, (2014)	5 phases

Table 2.1 shows a review of a number of previous digital forensic investigation approaches. Each model consists of different number of phases, but they all share the same common phases. To conclude, it is clear that a standardized scientific approach for digital forensic investigation has not been established yet, which makes it one of the challenges that forensic investigators encounter. Thus, an additional work on standardization is required in order to conduct a successful investigation. Section 2.2 present an overview of digital evidence, its definition, characteristics, and discusses admissibility of evidence.

2.2 DIGITAL EVIDENCE

In the past, when a murder crime occurred, forensic investigators collected as much evidence that relates to the cause of death as possible, and putting valuable evidence together may lead to the perpetrator. However, collecting evidence from the crime scene used to be limited to traditional evidence, such as papers, photographs, calendars, personal mail letters, notebooks, and collecting messages stored in the answering machine. With the rapid growth of digital technology, the type of evidence that are collected in crime scenes has also changed. Forensic investigators are now more aware of digital evidence that indeed may reveal much information which may be used against the offenders. Thus, digital evidence has increased the scope of investigation, and it can be valuable for developing theories of how the crime happened (Casey, 2004).

There are many sources that can be crucial for finding digital evidence, including computers, hard disk drives, flash drives, Emails, smartphones, websites, database, and online social networks. Schofield (2007) stated that the explosion of modern technology and digital devices improve both security and forensic capability and with these technologies and the information collected from new digital devices, the evidence can be used in courtrooms. Recently, there are number of crime cases where digital technology and information presented as evidence in courtrooms has led to convictions (Tipping, Farrell, Farrell & Woodward, 2014). Digital evidence has many forms that can be presented as reliable evidence. However, there are some types of digital information that may not be relevant to the investigation. The following sections will review multiple definitions of digital evidence, and discusses digital evidence sources and types.

2.2.1 Definition of Digital Evidence

There are several definitions of digital evidence that has been previously proposed. Casey (2011) defined digital evidence as “any data stored or transmitted using a computer that support or refute a theory of how an offence occurred or that address critical elements of the offence such as intent or alibi” (Casey, 2011, p.7) The Scientific Working Group on Digital Evidence (2013) defined digital evidence as “any information of probative value that is stored or transmitted in binary form” (SWGDE,

2013). However, these definition put a full concentration on using the transmitted and stored information as a proof rather than using it to further an investigation.

Another Definition for digital evidence proposed by the National Institute of Justice (2008) and stated that “Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination” (NIJ, 2008, p.ix). Carrier (2005) proposed a more general definition of digital evidence. He stated that digital evidence is “Digital data that contain reliable information that support or refute a hypothesis about the incident being investigated” (Carrier, 2005, p.3). This means that digital evidence can be collected from a wide range of sources, but not all sources are admissible in courts due to the characteristics of the digital information. In order to accept digital evidence as admissible and reliable evidence, it has to follow several criteria. Section 2.2.2 will discuss these characteristics and when digital evidence can be considered admissible in courtrooms.

2.2.2 Characteristics of Digital Evidence

In order to accept digital evidence in courts, it has to go to several tests and assessments to make sure that the evidence is accurate. This is because the integrity of digital evidence can be lost, which leads to losing the acceptability of the evidence. This may happen because of the volatility or handling of the digital evidence. The issue is discussed in this section.

Digital evidence may be fragile, which means that the evidence may be tampered, altered, or even destroyed. There are many reasons that may change the evidence from its original state, such as by inappropriately handling and collecting the evidence, or by performing mistaken examinations of the evidence. Digital evidence also may be effected by the way it is stored. Digital forensic investigators are aware of this matter and follow best practices in order to keep the evidence in its original state. As Carrier (2003) stated that digital evidence is hard to keep in its original form, and it is easy to copy the evidence and to modify it.

Digital evidence can be collected from many types of electronic devices, and each device may contain multiple types of stored data such as a recorded video, images and pictures, audios, messages which may be received as a text or as an email, saved maps, and digital notes. Cohen (2010) stated that that digital evidence has many forms that can be used as an evidence, these types are also subject to challenges that may

affect the admissibility of the evidence. Digital evidence share a same characteristics as DNA evidence or fingerprints. Which is the latency of the evidence (NIJ, 2008, p.ix), However, DNA evidence or fingerprints do not change from its original state as digital evidence may. Digital evidence is a time sensitive. For example, investigating files stored in a hard disk, and last access to the files, or investigation involves videotaping a crime being committed.

Digital crimes do not have a fixed area. It can happen anywhere in the world, because a digital forensic investigation may be conducted at one place, and the evidence can be found in different jurisdictions (NIJ, 2008, p.ix). Thus, cross jurisdictional borders will make digital investigation much harder, as each country has different laws for digital forensics, which is indeed one of the many current challenges and issues faced by the digital forensics community. These characteristics of digital evidence has an effect on the integrity of the original evidence, and it affects the admissibility of the evidence in courts of law. Section 2.2.3 will discuss the admissibility of digital evidence in courts.

2.2.3 Admissibility of Digital Evidence

Admissible evidence is the evidence presented to the trier of fact to support those taking decisions in court case. The evidence must meet several requirements to be admissible. These requirements are based on two major guidelines for deciding whether the evidence are admissible or not. The first guide is Daubert Standard, which is an applied test of five criteria for deciding whether to accept the evidence presented by expert witness or not (Daubert v. Merrell Dow Pharmaceuticals, Inc., 1993, p.1). The Daubert test criteria are:

- Testing: the procedure or technique used by expert witness have been tested
- Publication: has the procedure or the technique been published and they are subject to peer review?
- Error rate: what is the possible or error rate for the procedure/technique used?
- Acceptance: has the procedure/technique been accepted by the relevant scientific community?
- Standards and Control: is there any standards used in the procedure/technique?
And how it is controlled and maintained?

The second significant U.S. guide for evaluating the admissibility of evidence is Rule 702 of the Federal Rules of Evidence, which supported Daubert guidelines and

transformed it into the form of law. In rule 702, there are three requirements that make evidence presented by expert witness admissible. The requirements are:

- The testimony is based on sufficient facts or data,
- The testimony is the product of reliable principles and methods
- The principles and methods has been applied reliably to the facts of the case.

2.3 ONLINE SOCIAL NETWORKS

The use of social media has become a pervasive activity in the lives of many users. There are many different online social networking sites with different purposes of use. Users of these sites have become more attached psychologically to these sites and they post much information about themselves, including pictures, status, comments, locations, and feelings.

From a forensic point of view, OSNSs are a potential source of evidence that can help during a forensic investigation. There are many cases where criminals use these OSNSs to reveal their admission of committing a crime in a way of bragging. Others are seeking popularity by getting attention from the public. In Saudi Arabia, a hacker has admitted unauthorized access to a governmental website, a couple of hours later, the post was deleted. If the post was extracted by a proper tool, and best practises were applied, then the post would be admissible evidence against him. OSNSs especially Facebook, are becoming a source of crimes according to United Kingdom Police Mostyn (2010). These crimes include illegal firearms trade, fraud cases, identity theft, and harassment.

The following sections will give an overview of online social networks, by providing comprehensive definitions, features and characteristics of OSNSs. Current popular OSNSs, and their data features are presented. A review is made regarding the social impact of OSNSs on societies. Finally a comparison of online social network usage is made between three countries.

2.3.1 Overview of Online Social Networks

Online social networks are basically online forums that provide easiness and effectiveness for unlimited amount of users to share information in digital forms such as images, texts, links, audios, and videos. Users tend to share information in different forms for different purposes, such as for communications with others, advertisements, chatting with friends, and learnings, or sometimes just to post their thoughts regarding

feelings, economy and politics. There are many definitions of online social networks. Cheung and Lee (2010) have defined online social networks as;

“Sites that provide online spaces where individual can create a profile and connect that profile to others to create personal network” (Cheung & Lee, 2010, p.24)

Another definition made by Boyd and Ellison (2007) who stated that an online social network is;

“Web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system.” (Boyd & Ellison, 2007, p.211)

The definition above defines online social network in terms of its users and connections among them. Another definition made by Carter, Foulger and Ewbank, (2008) is that online social networking sites are:

“Interactive websites designed to build online communities for individuals who have something in common--an interest in a hobby, a topic, or an organization--and a simple desire to communicate across physical boundaries with other interested people” (Carter, Foulger & Ewbank, 2008, p.682)

The dramatic development of Web 2.0 which allows users to be involved and interactive with the internet applications, has produced a number of online social networks, which are now representative of Web 2.0 applications. According to Mingming (2014) Web 2.0 websites changed the way of interactions with users, by providing them with more user-interfaces, more storage facilities, and more tools, which entuse users to be collaborative with each other, leading to the creation of virtual communities. Due to users' interaction with online social networking sites, the amount of data shared online has dramatically increased. According to Gao, Wang, Luan and Chua (2014) OSNSs are now the indispensable real-time source of information and data gathering due to the extensive range of applications used and the vast number of users who are connected to these websites. Thus OSNS is an ideal source for performing analysis on social data in the event of crisis, revolutions, global incidents, it is also an essential place to promoting social developments (Nagarajan, Sheth & Velmurugan, 2011).

The type of data that can be found in OSNSs is impressive. According to Schneier (2010) there are several types of user data that OSNSs deal with. Starting from the data that are considered the person's credential, such as their names, and date of birth. Another type of data is what each user post on their accounts, such as photos, and status. Users connected with others can also post on their each other's accounts. OSNSs can store many types of data about the users. Schneier (2010) summarized the types of data that OSNSs deal with and they are shown in Table 2.2.

Table 2.2: Types of Users' Data that can be found in OSNSs. (Adapted from Schneier, 2010, p.88)

Type of data	Description
Service data	Data that has to be provided by users to continue using the social networking site, examples of data is legal name, Date of Birth, and phone numbers for some websites
Disclosed data	Any data posted by the account user, it could be presented in any format such as pictures, videos, links, comments, and updating status
Entrusted data	Any data posted by someone else to a user account. Many OSNSs permit users to post information or digital data on other users (friends, subscribers, followers etc.) The difference between Disclosed and Entrusted data is that the user does not have control over the data once it's been posted
Incidental data	Incidental data is what other people write in their account about a particular user. Again the data could be anything, pictures, messages, videos, etc.
Behavioural data	The data collected by the OSNSs about users' practises and habits. By recording their activities either in gaming, politics points of views, believes and so on

In summary, users have the ability to pass any information they wanted by using the format type that each social website has permitted, because each OSNS has its own features, privacy settings, and objectives. The following section discusses features of OSNSs, and characteristics of OSNSs that differentiate them from regular websites.

2.3.2 Features of Online Social Networks

One of the most convincing features to start and to keep using online social networks is their simplicity of use. In general, users do not have any challenges in signing up, as it only requires a user to write their identity information. Once they finish filling up their information, then their account is created, and ready to explore the features of the site, adding friends, subscribing to pages, posting pictures, updating status, and chat

with friends. Most of the popular sites such as Twitter and Facebook have multiple privacy settings that permit users to choose from. For example, Facebook permit users to decide who can view their posts, and who can access the information displayed on their accounts. There are different levels of privacy setting in Facebook, Public, private, and custom settings which means only specified people who can view the account (Hattingh, Buitendag & Thompson, 2014). This feature limits the connection with others which provides security (Zainudin, Merabti & Llewellyn-Jones, 2010).

One of the characteristics of OSNSs is participations, which is encouraging users to communicate with others and exchange thoughts and information and discussions. The following Table 2.3 summarizes the core characteristics of online social networks that differentiate them from normal websites.

Table 2.3: Core Characteristics of Online Social Networks

Characteristics	Description
User-based	Before OSNSs, regular websites were managed by a single user, the content of the website could be also managed by a single user, and read by visitors. On the other hand, OSNSs is purposely built for the user to collaborate on adding content to the site
Interactivity	OSNSs are based on interactivity of the users. Users are decision makers on how much they want to interact with others, the more interaction with others the more beneficial and interactive
Relationships	OSNSs enabled users to have ubiquitous connections with friends and families, especially when OSNSs became accessible via multiple devices such as mobile phones and PDAs. Thus, connection with others became easier and faster
Community driven	OSNSs permit users to create their own community that share the same common interests and hobbies, OSNSs communities such as group pages can store unlimited amount of information regarding the users within these communities

According to Teoh, Pourshafie and Balakrishnan (2014) the growth of OSNSs is directly related to the rapid increase of number of users, who are attracted by the characteristics of OSNSs, and the number of OSNSs continue to grow due to the number of users who are connected via these websites. The growing number of OSNSs will lead to an increase of number of users visiting these sites, which means more data and information will be posted and shared. Thus, the evidence collected from OSNSs will most likely to grow (Bachrach, Kosinski, Graepel, Kohli, & Stillwell, 2012). According to Teoh, Pourshafie and Balakrishnan (2014) the most popular online social networking sites are Twitter, Facebook, LinkedIn, Google Plus, Instagram and

Myspace. A review of current popular OSNSs, and their usage will be discussed in the next section.

2.3.3 Popular Online Social Networking Sites

According to Facebook (2014) it is the most dominate online social networking site among users with 1.39 billion users as of December 31, 2014. This is because of the features that Facebook offers for its users. Using Facebook is never a hard task for the user. It simply starts with the user's choice of signing up by completing some specific information about themselves, for example, name, gender, place of birth, and date of birth. Eventually, the homepage is created, and the user is free to use multiple features, such as to start adding friends by searching their names, or by their email addresses. Facebook friends can have a constant communication via instant messenger, or by writing on their wall (friend's homepage). Users can also add pictures, videos and update status on their wall and their friends' wall, and tagging (mentioning) friends on specific post in order for them to read and respond by either posting a comment, like, or share.

One of the most fascinating feature of Facebook is the ability to create groups, which enable a number of users to collaborate with each other on a specific subject. Facebook groups enable users to share and post information depending on the purpose of creating the group, there are several formats of pages that can be created by the users (Wang, Woo, Quek, Yang & Liu 2012). Table 2.4 summarizes Facebook formats that can be created by users.

Table 2.4: Facebook Formats

Format	Description
Profile Page	A profile created for a specific user, their information, their photos, status, and friends
Open Group	A user can create an open group that allow other Facebook users to join any time by clicking on Join group. The page enable joined users to post information, discussions, and updates on a certain subject
Closed Group	Similar to open group, but it is not an open which means that the creator of the page is responsible for allowing other users to join by inviting them to join
Community	Created by Facebook user, permits other users who have similar interests, topic, or experience to connect to a community page by liking the page. Thus, users will receive updates, information regarding the topic, and they are to react by likes, commenting and so on

Twitter is another well-known online social networking site that enable users to communicate, and to spread information and news (Stringhini, Wang, Egele, Kruegel, Vigna, Zheng, & Zhao, 2013). Twitter allows its users to send short messages in form of tweet (Scellato, Mascolo, Musolesi & Latora, 2010). The short messages can only contain text with no more than 140 characters. The messages (Tweets) can be displayed in two ways, either in the users profile page, or the timelines of the user followers. In Twitter, users are able to follow other users depending on their interests. Whether it's on sports, politics, economy, fashion, and major events. Twitter permits users to create hashtags (#) which is used to relate to an event, specific topic, or trends. Lu and Lee (2015) mentioned that major trends and events are being discussed and reflected on by the users via hashtags. Twitter also permits users to send private messages and communication to other users. Message propagation which is called Retweet is another feature provided within the site to spread a message or tweet to others. This features enable users to broadcast another user's tweet, which is becoming a very effective way for broadcasting major events, status and emergency warnings (Itakura & Sonehara, 2013).

LinkedIn is business-oriented online social networking site, meaning that more focus on professional networking side. The purpose of using the site is to build a network where the users can access and communicate to professional people, finding jobs and opportunities, users are able to update their current professional statues, their previous employer, and current employer (Sorensen, 2009). LinkedIn users benefits from the site only by revealing their information publically in order for employers to view a user's information, skills, contacts, objectives, and their areas of interest (Broillet, Kampf & Emad, 2014). Another professional networking site is called Bayt, which focuses on connecting professionals in the Middle East. Similar to LinkedIn, Bayt users can build their own professional profile page, communicate with other users, send private messages, and apply for jobs by contacting organizations and companies that already have accounts on the site.

Instagram is an online social network that permit user to take photos and videos via their smart phone cameras, and share them on other OSNSs by posting the link to that specific picture or video. Each user has their Instagram account which can be accessed via different platforms either computers, or mobile phones. Instagram enable users to add comments, like photos and videos, and also following other users. According to Instagram (2014), the number of Instagram users has reached up to 300

million users across the world. Physical location of the picture taken is one feature that may be interesting for forensic investigator. The feature called “photo map” which can be enabled by the user to locate their exact physical location of the picture or the video taken (Silva, Melo, Almeida, Salles & Loureiro, 2013).

2.3.4 The Impact of Online Social Networks on Societies

The rapid growth of OSNSs has reshaped the social landscape and produced several different ways of interactive communication between users. It has played a major role in governance, uprisings, and campaigns through political communications between users. OSNSs are also playing a major part in revolutions. For example, Facebook and Twitter played a major role in the revolution of Egypt in 2011 (Ratto, Boler & Deibert, 2014). According to Attia, Aziz, Friedman and Elhousseiny, (2011) the revolution started when a group of people called OSNSs’ users to demonstrate. This call has spread very quickly across Facebook and Twitter users, and nearly 90 thousand Facebook users has accepted the call for the demonstration which started in 25th of January. During the demonstration, Facebook and Twitter were the real time source of information from different places in Egypt. Activists and non-professional journalist became influential during that time. Television and newspapers also started to extract and broadcast information from OSNSs. During the beginning of revolution, the Egyptian government decided to block telephone communications, and access to Facebook and Twitter by blocking the entire internet, which lasted for several days. However, this has aggravated the situation and turned it into a massive revolution in 28th of January with about 2 million people. This major event has made other governments across the world to consider taking action against online social networking sites by monitoring activities and usage. According to Ho (2011) the Egyptian revolution has made the Chinese government to block access to searches that contains the word Egypt. The Chinese government was seemingly worried that this event may inspire Chinese people to revolution.

In 2015, Saudi Arabian King Salman Bin Abdulaziz has become a widely followed world leader on Twitter. While his popularity is rapidly increasing in various online social networking sites, King Salman has passed several world leaders on twitter with more than 2.5 Million followers, including scholars, world leaders and Saudi citizens. According to analytics site Topsy, King Salman has received more than 130,000 mentions after he changed his twitter account to @KingSalman. One of his

tweets reached up to 260,000 retweets in several hours. The King considered social media to be an open communication line with Saudi citizens, and the local media which indicate that OSNSs has an impact on societies, and it will continue to grow.

Online social networking sites has become crucial and ubiquitous in terms of sharing contents, and communication between people across the world. It is indeed changing the public dialogue in societies and setting discussions and agendas in topics that range from the environment, technologies, politics, and events. However, OSNSs have created a wide range of space for criminal activities, due to the privacy settings of each OSNS. Thus, the need of more sophisticated forensic tools for online social networks investigation has become crucial.

2.3.5 Online Social Networks Usage by Country

The use of OSNSs such as Twitter, Facebook and LinkedIn has grown rapidly across the world, due to the easiness and features that each social site provides to their users, and also because of the interactivity of users with what is happening around the world, comparing with traditional media where users used to receive information and content without making a reaction to it. Users are more open to each other and can respond to content and information produced by other traditional media.

Each country has their own jurisdiction, laws, and different cultural background on regarding the use of online social networks, this means that OSNSs trends vary across countries. Thus, comparing the use of online social networks in different countries would be beneficial to the field of digital forensics in order to gain comprehensive knowledge on what are the most dominate OSNSs in different countries, and to show why users chose to use these websites, and what is the content or the information that they post which could be treated as digital evidence. The following sections will discussed the use of online social networks in New Zealand, Saudi Arabia, and United States of America.

2.3.5.1 New Zealand

Online social networks has received a lot of attention in New Zealand during the last few years. Gibson, Miller, Smith, Bell and Crothers (2013) conducted a survey on the internet in New Zealand. The survey results show that almost every person under 40 years old is online, and 81% of users visit online social networks. According to (Nielsen, 2012) Facebook and Twitter are the most popular online social networking

sites in New Zealand. There are almost 2.3 million New Zealanders who use Facebook, which makes it the most dominate OSNS in New Zealand (Maas, 2013). Many companies in New Zealand became closer to their customers via social media marketing. According to the survey conducted by (Icehouse, 2013) 92% of New Zealand business owners stated that social media is a key factor of achievements and professional development. Currently, many NZ companies have an account on Facebook or Twitter, or even both. Recently, AUT University has launched their Instagram account which is linked to their Twitter, Facebook accounts.

2.3.5.2 Saudi Arabia

Online social networks is increasing in Saudi Arabia. According to Saudi Social Media Summit and Arab Social Media Report, one of the highest usage rate of online social networks is in Saudi Arabia with more than 3 million users are on Twitter, and around 840,000 Saudi users are registered in LinkedIn. A survey conducted by Alwagait, Shahzad and Alim (2014) on the use of online social networks, 90% of participants have twitter profiles. Their results show that the most dominate online social network in Saudi Arabia is Twitter. There are several purposes that Saudi citizens use online social networks. A survey conducted by Alothman (2013) on social media users in Saudi Arabia. The results showed that most participants use OSNSs for social communication, and for political discussions, as information is easier to obtain from social media. The evolution of online social networks in Saudi came along with the new emerging smartphones. There are currently many social networks that are very active among Saudi citizens. Twitter, Facebook, and LinkedIn are not the only ones who are very active. But even WhatsApp, Instagram, and Snapchat which are popular social media platforms that are used via smartphones.

2.3.5.3 United States of America

Online social networks have been widely used in USA. As of 2013, almost 72% of online adults use online social networks in USA, from around 66% in 2012. According to (Duggan, Ellison, Lampe, Lenhart and Madden, 2014). Facebook is still the most popular social media used across the US. However, there is a significant increase of users in other platforms such as Twitter, Instagram, Pinterest and LinkedIn.

2.3.6 Online Social Networks Forensics

Online Social Networking Sites (OSNSs) have become a major part in the lives of people, who are attracted to using these sites on a regular basis. Apparently, OSNSs do not only attract regular people, but they also attract companies, organizations, and even governments' attention, because of the usefulness of these OSNSs, which gives them the ability to interact with others instantly. OSNSs holds numerous amounts of information such as instant conversations between users, pictures of the users, the exact locations that users have been to, personal information such as date of birth, relationship status. OSNSs even contain feelings of the users and their psychology. This information can be used as admissible evidence in digital forensic investigation. Recently, there are cases where information stored in online social networks is used as evidence. According to Abbas (2015) a female was sexually assaulted while she was unconscious. The local police have identified and arrested a group of rapists who are recognised by the videos and pictures posted on OSNSs. Another incident happened in Boston Marathon attacks in 2013. OSNSs enabled users to post their messages along with the exact geographic information. When the attacking took place, the police department started to collect information about the people who were present at the site via OSNSs in order to identify the suspects, information collected including pictures, status, locations and so on. The police have identified the suspect's appearance and clothing through collecting information from OSNSs, they also have identified the reasons for committing the crime and the suspect's political thoughts (Cassa, Chunara, Mandl, & Brownstein, 2013). With the rapid popularity of social media, it is also getting used for criminal activities (Zainudin, Merabti & Llewellyn-Jones, 2010). Athanasopoulos et al. (2008) reported that online social networks offer multiple motivations for criminals to use as a platform for committing their crimes. This includes a) huge datasets about users' identities and personal information b) same social interests are shared by cluster of users and c) the easiness of distributing fraudulent resources to a vast number of users. So criminals are able to use the social information as an inspiration for committing crimes. For example, distributing a picture of targeted places for robbery to other criminals in the team through the use of uploading pictures in Facebook, including the physical location attached with the post of the picture. Another example is selling unlicensed weapons, and advertising through posing information about the weapons, pictures, and the location where the deal will

be made. To date, there is still no accepted definition for online social networks forensics, since it is still new to most law enforcement agencies, and the IT community still does not have sufficient familiarity with it. According to Muda, Choo, Abraham and Srihari (2014) there will be a major focus on social network forensics in the future. There are few proposed models for OSNSs investigations, Zainudin, Merabti and Llewellyn-Jones (2011) have proposed a model for investigation in online social networks. The proposed model consists of several activities that need to be performed; Preliminary, Investigation, Analysis, and Evaluation.

Abdalla and Yayilgan (2014) have identified the type of investigative activities done via online social networks, which include identifying persons of interests, criminal activity identifications, and monitoring person of interests. They stated that law enforcement agencies have changed their traditional techniques and procedures by starting to use forensic tools for extracting evidence in OSNSs.

2.3.7 Digital Evidence in Online Social Networking Sites

Online social networking sites are indeed becoming a crucial source of evidence that is collected during a forensic investigation. The types of evidence can vary from one social networking site to another depending on their architecture and the features provided by the OSNSs. Mulazzani, Huber and Weippl (2012) have presented different data sources that may lead to feasible evidence during a forensic investigation of OSNSs:

- 1 Social footprint with other users, including friend lists, connected groups, who are the followers, and following who.
- 2 Communications methods between the users within the site, e.g. private messages, instant messenger, comments, likes, group communications, and events.
- 3 Pictures and videos posted by the users, and who were tagged in the pictures, what other pictures a certain user was tagged on.
- 4 The times of activities: when a specific user logged on into the site, and what sort of activities were performed in a specific time.
- 5 Apps: identifying all the apps used by the user, and identifying the purpose of the used apps, and what information be deduce in the social context.

Although the general data could help during the forensic investigation, the authors indicated that all of the information cannot be extracted from the hard drive (HD), because they are only stored at the social network's provider. However, most often,

some of the data can be stored in Random Access Memory (RAM), which may be difficult to recover depending on the computer status, whether it is switched on once found or not. If the system is turned off then RAM acquisition may not be feasible, because turning the system back on to acquire RAM may change the system data. Alternatively, the forensic investigator may find valuable evidence and activities stored in the virtual memory swap file. During the system's normal operation, the data stored in RAM is swapped into a file named pagefile.sys. (Mutawa, Awadhi, Baggili & Marrington, 2011). Though, the data swapped into pagefile.sys is volatile, and volatile data may be lost during swapping from RAM to pagefile.sys. Moreover, the data stored on RAM may not always be swapped into pagefile.sys, which means that some data could still be stored in RAM and have not been swapped (Mutawa, Awadhi, Baggili & Marrington, 2011). A potential source of data can be restored from the web browser cache that is stored in the hard drive, because web browsers create log files, and it writes and stores data in the cache files. Also it stores cookies on the computers, depending on the type of the browser used, and the version. This information could be found in different places including browsing history, cookies, and cache. Since web browsers are used by users to connect to OSNSs, there is a possibility that web browsers may hold potential admissible evidence. Thus, the web browser is an essential place that has to be considered when conducting a digital forensic investigation. The most used browsers up to date are Internet Explorer (IE), Chrome, Firefox, Safari, and Android browsers. Figure 2.1 shows the top browser share trend in the markets as at February, 2015.

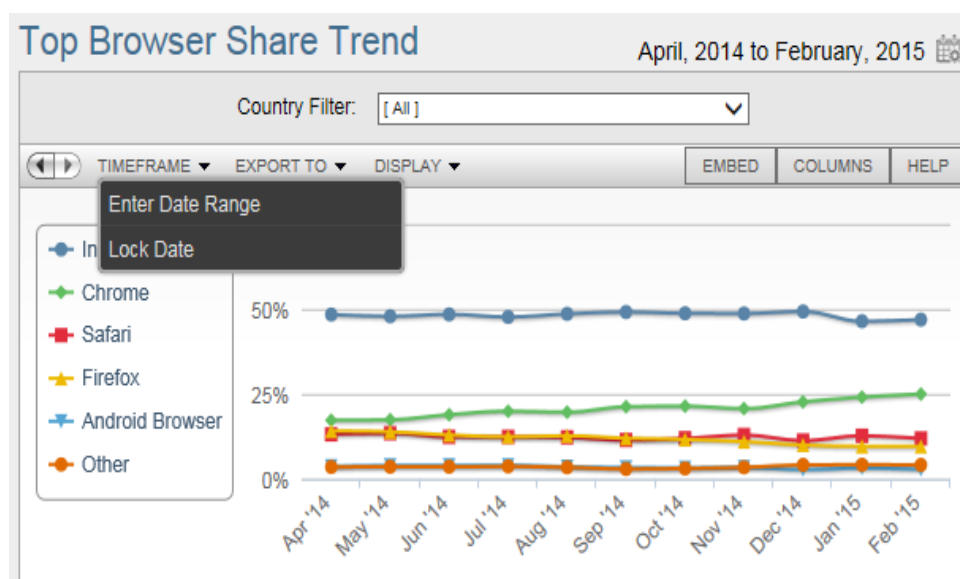


Figure 2.1: Top 5 Browsers in the Market Share (Net market share, 2015)

2.4 DIGITAL FORENSIC TOOLS

Historically, the amount of digital evidence was small in any digital investigation compared to more recent digital events. The type of digital evidence was also limited. Early digital forensic investigation did not have sophisticated tools to work with during forensic investigations. In fact, digital investigators used to examine the entire digital media in order to extract data files and evidence, so every file in the data storage used to be examined. Forensic investigators used to examine the suspect computers by performing a live analysis in order to view the evidence, which is not an applicable method nowadays, as there is a high probability the evidence is changed or altered. Casey (2011) stated that digital evidence may face alteration, or changing from its original state accidentally during the collection phase of evidence. Thus, using proper tools during forensic investigations will ensure that the data collected are not altered or destroyed, and if the data were altered, the investigators will know because of these trusted forensic tools.

With the rapid development of technologies, it is nearly impossible to conduct a digital forensic investigation without the use of existing tools. Systems have become more sophisticated in terms of their structures. Portable devices and hard drives technologies have developed rapidly in terms of their capacity and usage. During the 1990s a number of forensic tools were developed such as IMDUMP, and SafeBack that were used for acquiring data from the source media without making an alteration to the data. It provided the integrity of the data, and these tools were one of the first introduced that enabled investigators to perform a forensic image “bit for bit” copy of the data in a forensically acceptable manner. By the end of the 1990s, more advanced tools had been developed, such as Encase and FTK (Casey, 2011), which extended the performance of the tools to also performing a complex analysis on the forensic images, and recovering deleted files. These tools are now widely used by the digital forensic community, and government enforcement agencies. Currently there are many digital forensic tools that have developed over the years to serve forensic investigations. These tools are different in terms of their usage and purpose, they are also different in terms of providing a graphical user interface (GUI), or command line based interface. Some of the tools are publically available to the public users, such as BackTrack which is based on Linux OS that is used as a penetration testing tool. Whereas there are number of commercial tools that are only available for certain communities such as

Law enforcement, governments, organizations, academic researchers and digital forensic specialists. Table 2.5 summarizes the recent well-known digital forensic tools, they are categorized into their type of usage.

Table 2.5: Digital Forensic Tools Categorized in Terms of Their Usage

Computer Forensic Tools				
Name	From	Description	Licence	Platform
EnCase Forensic	Guidance Software	One of the most powerful tools for acquiring data, email, artefact, and internet investigation, with the ability to perform data analyses and reporting	Proprietary	Windows
BackTrack	Linux	Linux-based OS build for security professionals, mainly focused on penetration testing, providing sufficient amounts of digital forensic tools	Open Source	Linux
DEFT	Linux	Digital Evidence & forensic toolkit based on Linux OS. Offers wide range of free tools including incident response and computer forensics	Open Source	Linux
Forensic Tool Kit (FTK)	Access Data	One of the most innovative forensic tools that can handle huge data sets from different source, and finding relevant evidence to the case. Widely used by law enforcement agencies, and it is known as digital forensic investigation solution (Accessdata,2015)	Proprietary	Windows
X-ways forensics	X-ways	Integrated computer forensic software, based on WinHex hex, and disk editor	Proprietary	Windows
Live RAM Capture	Belkasoft	Extract RAM dump from a computer, even if it is protected with any anti-dumping systems (Belkasoft, 2015)	Open Source	Windows
Email Forensic Tools				
Name	From	Description	Licence	Platform
eMailTrackerPro	Visualware	Tracing the send of a message by analysing the header of the message	Proprietary	Windows
EmailTracer	RCCF	Developed by the Indian premier centre for cyber forensic, gives a complete detail of the sender by analysing IP header of the email	Proprietary	Windows
EDB Viewer	Lepide Software	Viewing Outlook EDB files without the need of Exchange server, used for E-mail analysis	Open Source	Windows

Mobile Device Forensic Tools				
Name	From	Description	Licence	Platform
XRY	Micro Systemation	Recover information from mobile phones, including deleted data, cover many different types of phones (Micro Systemation, 2015)	Proprietary	Windows
Oxygen	Oxygen Software	Mobile Forensic software for logical examination and analysis of data can be found in mobile phones, and PDAs	Proprietary	Windows
Paraben's DS Forensic tools	Paraben Corporation	Mobile Forensic tool. Acquiring and Extracting logical, physical files. As well as password bypassing and file system extractions	Proprietary	Windows
Mobilyze	BlackBag	Designed to give forensic investigators immediate access to data from iOS mobile phones and Android devices	Proprietary	Windows /MacOS
Network Forensic Tools/ Online Social Networks forensic Tools				
Name	From	Description	Licence	Platform
Wireshark	Wireshark	Capture and analysis of network packets, and then displaying details of each packet data as possible (Wireshark, 2015)	Open source	Window/ Mac/Linux
Belkasoft Evidence Center	Belkasoft	Forensic tool for extraction evidence found in the hard drive or computer volatile memory	Proprietary	Windows
Internet Examiner toolkit (IXTK)	SiQuest	Recover internet browsers artefacts, chats, emails, social networks by searching and analysing hard drives	Proprietary	Windows
Internet Evidence Finder (IEF)	Magnet Forensics	Recovers OSNSs, online chat, web browsing history, from hard drives and live memory captures, including deleted data (Magnet Forensics, 2015)	Proprietary	Windows
Network Mapper Nmap	Nmap	A Network scanner and security auditing	Open source	Windows/ Mac/Linux
CacheBack	Digital Investigation group	Rebuild internet cache, history and perform analysis of OSNSs	Proprietary	Windows
TcpDump	TCPDUMP	Packet analyser based on command line, it has the ability to intercept TCP/IP packet information	Open Source	Window/ Mac/Linux
Other Tools				
Name	From	Description	Licence	Platform
softBlock	BlackBag	A software-based write-blocking tool, when a hardware device connected, software identifies and mount device with read-only	Proprietary	MacOS
UltraBlock	Digital Intelligence	A hardware-based write-blocking device. Used for connecting hard drives to computers with read-only	Proprietary	Not specified

There are other digital forensic tools developed for digital forensic investigations, which are helpful but not listed in Table 2.5. Developing digital forensic tools is not the only challenge, the major challenge is developing digital forensic tools that are reliable in collecting evidence and providing integrity for evidence, in order to be admissible in court of law. Fortunately, some of the tools are already accepted in court rooms, due to their efficiency of providing admissible evidence. Evidence extracted by these tools is correctly acquired, and analysed, which means that the evidence is never changed from its original state. Examples of these well-known tools are Encase and Forensic Tool Kit (FTK). For the purpose of this thesis, the next section will identify the digital forensic tools that will be used for investigation of online social networking sites.

2.5 EVALUATION OF ONLINE SOCIAL NETWORKS FORENSIC TOOLS

For a digital forensic investigator, it is very important to know the right tools that would be efficient and related to a case. For example, it would not be sensible to use Wireshark to investigate a computer when this computer has never been connected to a network. Using the right tools will indeed save the investigator time, and also will enhance the investigation outcomes. Thus, Forensic tools play a significant part during the investigation process. In this section, a review of the major tools that are selected for searching and collecting evidence from OSNSs will be made. The selected tools were chosen after an intense research on different types of digital forensic tools that could be used for OSNSs forensic investigation.

2.5.1 Belkasoft Evidence Center

Belkasoft Evidence Center is a forensic tool developed by Belkasoft Company in 2002. According to Belkasoft, the tool aids computer forensic investigators and security professionals (Belkasoft, 2015). They stated that the toolkit will make it easy for the investigator to look for digital evidence, as the toolkit have the ability to search, analyse, store and share the digital evidence that can be found in the hard drive or RAM. They stated that the toolkit has the ability to extract digital evidence from different sources. They stated that “Belkasoft Evidence Center will help investigators quickly locate and analyse information found in social network remnants, instant messenger logs, and internet browser histories, mailboxes of popular email clients,

peer-to-peer data, multi-player game chats, office documents, pictures, videos, encrypted files, mobile backups, and system and registry files. “ (Belkasoft, 2015).

2.5.1.1 Core Capabilities & Features of Belkasoft Evidence Center

- Belkasoft keeps the integrity of the evidence by preventing any alteration or modification on the data on the hard drive or disk image investigated.
- It can perform an advanced analysis on the hard drives or the computer volatile memory.
- Full examination of more than 500 types of artefact, including online social networks, browser histories, instant messengers, and documents.
- Recovering destroyed evidence by performing data carving (Belkasoft, 2015).

2.5.2 Internet Evidence Finder (IEF)

IEF is an offline digital forensic tool that is able to examine and search for artefacts from different locations. According to (Magnet, 2015), IEF can be used to examine different digital devices such as computers, mobile phones, and tablets. IEF also supports different Operating systems including Windows XP, Vista, Windows 7, and 8; Mac OSX, and Linux. The supported mobile Operating systems include iOS, Android, Windows phones. It also support different file systems including NTFS, HFS+, EXT2, FAT32, and F2FS.

2.5.2.1 Core Capabilities & Features of Internet Evidence Finder

- Advanced Image search and examination, and support different forensic image formats including E01, Ex01, L01, and dd image format.
- Powerful search capabilities, allowing search for more than 220 internet artefact, including web browser activities.
- It can perform forensic analysis of different files structure including Pagefile.sys
- IEF categorizes Facebook activities into different forensic artefacts which are Chats, Messages, Facebook wall posts, Facebook pictures, and Facebook URLs.
- Can recover forensic evidence from different OSNSs, including Instagram, LinkedIn, Twitter, Myspace, and Google+.
- Built-in functions: Web Page Rebuilding, hex, text viewer, Reporting features

2.5.3 Internet Examiner Toolkit (IXTK)

According to (SiQuest, 2015), Internet Examiner toolkit gathers evidence from a wide range of artefacts, including browser activities, multimedia files, keyword artefacts, and social networking sites. They stated that the toolkit can perform chat recovery of (Facebook, Bebo, Skype, Gtalk, AIM, and YIM). It is also able to locate and analyse browser cache, history, cookies for several browsers including (Internet Explorer, Safari, Firefox, Opera, and Google Chrome). A sample screenshot from SiQuest's software Internet Examiner Toolkit is shown Figure 2.2, which shows the ability and feature of IXTK that can perform for acquiring evidence from online social networks.






















Social Networking				
Artifact Description	File	Trace	PC	Mobile
Facebook				
Chat Message – Common JSON format		✓		
Chat Message – HTML formatted message		✓		
Chat Message – Left sidebar snippets of last chats		✓		
Online Profile – online profiles as shown in Facebook page right sidebar		✓		
Photo Url – Fully qualified Url to Facebook profile picture		✓		
Twitter				
Photo Url (Big) – Fully qualified Url to large size thumbnail		✓		
Photo Url (Normal) – Fully qualified Url to normal size thumbnail		✓		
Tweet HTML – Tweeted message in HTML format		✓		
Twitter ID: Full Name – Full Name related to Twitter account User ID		✓		
Screen Name ID – User ID and Screen Name attributes from HTML page		✓		
YouTube				
Evidence of Played Video – Recover video Url and attributes		✓		

Figure 2.2: Screenshot of Internet Examiner Toolkit Capability for OSNs

Source: SiQuest at: <http://www.siquet.com/index.php/ixtk-supported-artifacts/>

2.6 SUMMARY OF ISSUES AND PROBLEMS

With the rapid development of technology, digital forensics and digital forensic investigators are facing an increasing of complexity and difficulties due to many factors. The most noticeable factor is the huge amount of data being transferred across networks globally. Online social network forensics is still new to the field of digital forensics. Digital forensics itself has major challenges and issues that directly affect the new areas like online social networks forensics and cloud computing forensics. Digital Forensics is yet to have a standardised model for conducting digital forensic

investigations. As shown in the literature that standardisation is still developing and many models have been proposed. Online social networks forensics is new and it is still to be developed and researched, and more effort should be made to develop guidelines, standards, and even tools that are specialised for online social networks.

OSNSs is growing rapidly around the world, which changes the way internet users interact with each other. According to the literature, crimes are growing due to the growth of OSNSs. From a forensic point of view, OSNSs is still new to most law enforcement and IT communities. The review of literature has raised several issues and problems related to digital forensics and OSNSs forensics which will be address in the following sections.

2.6.1 Lack of Standardization

Some of standards have been proposed for investigation of OSNSs, and as shown in the literature that there are some cases where information stored in OSNSs have been used as evidence in court rooms. However, there is still no standardized model for the investigation, which may impose more major ethical issues during the investigation such as dishonest or immoral investigation of OSNSs, or even invasion of privacy. So, forensic investigators have to follow best practices. This is includes following an accepted model for forensic investigation. Thus, more work should be done in regarding this matter in order to have a clear standardized model for investigation of OSNSs, where best practises are maintained.

2.6.2 Lack of Online Social Networks Forensic Tools

As shown in the literature there are many digital forensic tools and network forensic tools, and even mobile forensic tools that could be used for conducting forensic investigation and to acquiring and analysing admissible evidence. However, there is no developed tools specified for online social networks forensics, and evidence that could be collected from other tools are found from different artefacts that interact with the OSNS. The need for a standardized model will be helpful for software developers to develop a tool that can meet accepted standards. The need for a well-developed tool for social networks investigation has become crucial.

2.6.3 Jurisdictional Issues across Borders

Online social networks are used across the world, and with crimes and evidence which can easily cross jurisdictions, especially with the use of OSNSs as there is no access limitations for these websites. Therefore OSNSs forensics investigation is complicated as there are different jurisdictions have different legislation and law regarding digital evidence. Some countries still do not have sufficient laws for digital law enforcement. For example “ Unauthorized access”, whereas other countries have strict laws for it, which indeed need to be resolved and standardized across the world, in order to make digital forensic investigation much easier.

2.6.4 Admissibility of Evidence Collected from OSNSs

As shown in the literature that there are different types of evidence that can be collected from different OSNSs, and only several tools enable investigators to find evidence. However, it is very hard to decide whether the collected evidence are admissible in courts, as presented in 2.2.3 there are several requirements that need to be met. It is difficult to examine these requirements with the evidence collected from OSNSs, because these requirements based on procedures, techniques, and standards which have not been developed yet for online social networks forensics.

The identified problems and issues have to be explored for further research and studies in the area of social networking forensics in order to create methods, and models for investigation of OSNSs, and to create reliable tools that could serve digital forensics investigators for social networking forensics.

2.7 CONCLUSION

The literature reviewed in Chapter 2 provides a comprehensive knowledge and overview of five major areas which are: digital forensics, digital evidence, and online social networking sites (OSNSs), digital forensic tools, and online social networks forensic tools. The review covers an overview of forensics and a brief history background. Digital evidence can be collected from many types of electronic devices, and it has many types of stored data. Some of the collected data may not be relevant to the case, which is discussed in Section 2.2.3. Section 2.3 introduced online social networks, and their usage according to the recent literature, which clearly indicate that OSNSs are continuing to be one of the leading mediums of communication in the

digital world. Features of online social networks were presented in 2.3.2, followed by the characteristics of OSNSs. As shown in 2.3.4 there is an impact of OSNSs on modern societies, because they contributed to changing of the public dialogues in societies, but they also created a wide range of space for criminal activities. Thus, Section 2.3.6 discussed online social networks forensics, and how they are being used for committing different types of crimes including drug dealing and selling unlicensed weapons.

The increasing number of OSNSs enabled users to communicate in different ways and platforms, also with the rapid development of smartphones that are used for connecting to OSNSs. However, digital forensic investigation on online social networks is still in its developing phase. As shown in the literature that standardized guidelines for investigation on OSNSs need more attention in the near future. Section 2.4 reviewed some of the well-known digital forensic tools. Some of these tools are already acceptable by courts and law agencies such as EnCase forensic and FTK forensic toolkit. However, developing tools that are specified to OSNSs has become crucial. Section 2.5 presented a review of the major tools for searching and collecting evidence from online social networks. Finally, a summary of issues and problems were outlined in Section 2.6.

The following Chapter 3 will select one problem and develop a methodology that will be used. Relevant questions and hypotheses will also be developed.

Chapter 3

Research Methodology

3.0 INTRODUCTION

Chapter 2 critically reviewed a wide range of literature that are relevant to the research area. The reviewed literature provided an in-depth knowledge about digital forensics, digital evidence, online social networks, a range of tools used in digital forensic investigations, and online social network forensics. The Chapter has also discussed several models for digital forensic investigation processes, and discussed the recent model proposed by Shrivastava and Gupta (2014). A number of issues and challenges have been identified along with digital forensic tools that can be used for OSNSs. Consequently, it is noted that digital forensic investigations for OSNSs are still developing as a systematic study area. The main objective of Chapter 3 is to develop a methodology that can be suitable for the research area.

Chapter 3 consists of four main sections. The first Section 3.1 reviews five studies that are similar and related to online social networks research. The main objective of this section is to gain better knowledge, and understanding of what is the best way to construct an efficient methodology for the proposed research. Section 3.2 is the design of the proposed research. In this section, a summary of related studies is presented to address the main points of each method. Secondly, a summary of issues and challenges is identified in order to carefully formulate the main research question, which is presented in Section 3.2.2 along with related sub-questions and hypotheses. The proposed research methods are presented in Section 3.2.4. Section 3.3 is data requirements which defines and determines the data to be collected during this research, and how the data will be processed, analysed and presented. Finally the limitations of the proposed methodology are evaluated and presented in Section 3.4.

3.1 REVIEW OF SIMILAR STUDIES

This section analyses and reviews five relevant studies that have been previously published. The reviewed studies will assist in developing an appropriate methodology for this research. Section 2.3.7 reviewed different types of data that can be collected

from OSNSs, and the section has also reviewed multiple source of evidence that can be collected from OSNSs for a forensic investigation. Section 3.1 reviews five different studies that aim to provide relevance to testing and evaluating digital forensic tools. The selected approach is based on the robust reputation of their sources, and they assist in developing an appropriate methodology that will be applied in conducting a forensic investigation of online social networks.

The first approach, by the Nouredin, Hashem and Abdalla (2011) discusses in detail the previously proposed guidelines model for computer forensics which consisted of a set of phases that need to be followed. The proposed phases are then reconstructed in a flow chart in order to make each phase more comprehensive and easier for the digital forensics investigators to follow. The second approach by National Institute of Standards and Technology (2001) aims to provide a general approach that tests the tools used for computer forensics and digital forensic investigations; and discusses the importance of creating test methods for examining forensic tools. The third study by the Scientific Working Group on Digital Evidence (SWGDE) (2014), created recommended guidelines for validation testing, based on scientific principles. The validation guidelines are for digital forensic tools used in the investigation, procedures, and the applied techniques such as extraction. The fourth study is by Wilsdon and Slay (2006). They developed a framework for testing computer forensic tools based on a black box technique. The authors discuss two well-known methods including the method discussed in the third study for evaluation and tool testing, and the limitations. The authors propose a similar framework with better capabilities in terms of time constraints, financial requirements, and evaluation results. The proposed framework aims to simplify previous framework models for the digital forensic community. The last study has been recently proposed by Jang and Kwak (2014). This paper proposed a digital forensics investigation methodology that is applicable for online social networks. The authors aim to classify digital evidence extracted from OSNSs based on the examined digital device whether computers, or smartphones (IOS, Android). According to the authors (2014, p.2) the proposed methodology ensures that the collected evidence from OSNSs environments are protected from being damaged, or change, by designing the methodology with effective control processes, and with classification of digital devices, and collecting and analysis of evidence (2014, p.1).

3.1.1 Computer Forensics Guidance Model with Case Study

Noureldin, Hashem and Abdalla (2011) conducted a methodical study based on their two previously proposed models “Guidelines Model for Digital Forensic Investigation” and “Team Responsibilities for Digital Forensic Process” (Noureldin, Hashem and Abdalla, 2011, p.564). The authors focused on the deployment of their model in practice in order to expound the flow of the information between each phase of the forensic investigation. Furthermore, flow chart diagrams are used to show the flow of information between every stage and every phase of the investigation process. According to the authors, the purpose of using flow charts for the investigation process is to make sure that that investigation process is organized and well-structured in a way that makes it clear for the investigator to accomplish. They also stated that using flow charts ensures proper handling of the evidence, and minimizes the probabilities of errors made in other models (Noureldin, Hashem and Abdalla, 2011, p.564).

According to the authors, the proposed model has been validated by applying two different real computer related cases. The objective of the first case study is to find whether the suspect hides secret data in a hard drive. The hard drive has been examined and evaluated by following the proposed model. The second case concerns an Information Technology Industry Development Agency in Egypt. They requested a forensic investigation on some of their machines suspected to contain an illegally copied program. Live acquisition and examination of the machines has been made using the proposed model. The result of these two different case scenarios show that the proposed model is suitable for computer forensics investigation. They stated that the proposed model “can be applied to law enforcement investigation and corporate investigation” (Noureldin, Hashem and Abdalla, 2011, p.571).

The proposed model consists of five phases, starting from preparation phase. They stated that “the purpose of this phase is to make sure that the operation and infrastructure can support the investigation (Noureldin, Hashem and Abdalla, 2011, p.564). The second phase is the physical forensics and investigation, which aim to collect and examine physical evidence, and identify suspects who are involved in the incident. The digital forensics phase comes after physical forensics, for identifying more evidence that is stored electronically. The reporting and presentation phase is the fourth phase in the model where evidence is clearly presented in a way so that anyone can understand what is written. The last phase is closure. Each one of these

phases has its own procedures to be followed and they are also structured with a flow chart in order to make it easier for forensic investigators to follow. Figure 3.1 shows the flow of the main phases of the model, which are used in two computer related scenarios.

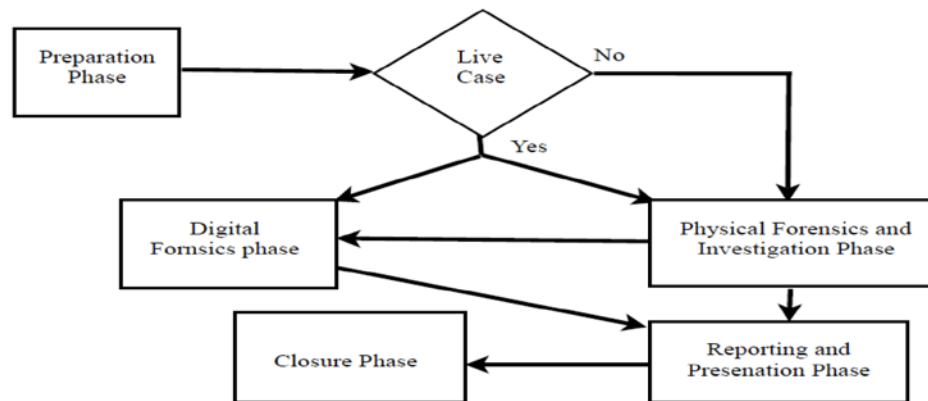


Figure 3.1: Computer Forensics Guideline Model (Noureldin, Hashem and Abdalla, 2011, p.564)

For the purpose of this research, the focus will be on the third phase the “Digital Forensic phase”. The authors stated that digital media is the second source of evidence that can be collected from the crime scene after the physical evidences. The objective of this phase is to find evidence from different digital sources, and artefacts and to analyse the collected evidence, in order to draw a conclusion that answers the questions that are derived from the physical evidence found in the crime scene. The conclusion of this phase comes after following five steps in the digital forensics phase. The first stage of the digital forensics phase is Evaluation and assessment where the seized physical evidence is checked and evaluated. For example evaluation of a computer found in the investigation scene and its status if it’s live system or switched off. Ensuring proper documentation of the seized materials are addressed in the chain of custody. In this phase, a digital investigator decides what tools they are going to use in their investigation based on the current materials that they collected. The second stage is acquiring digital evidence which depends on the status of the targeted system: that is if the system is switched off or live, and verifying that the copied image is the same as the original machine. Figure 3.2 shows the proposed flow chart for acquiring digital evidence depending on the status of the system.

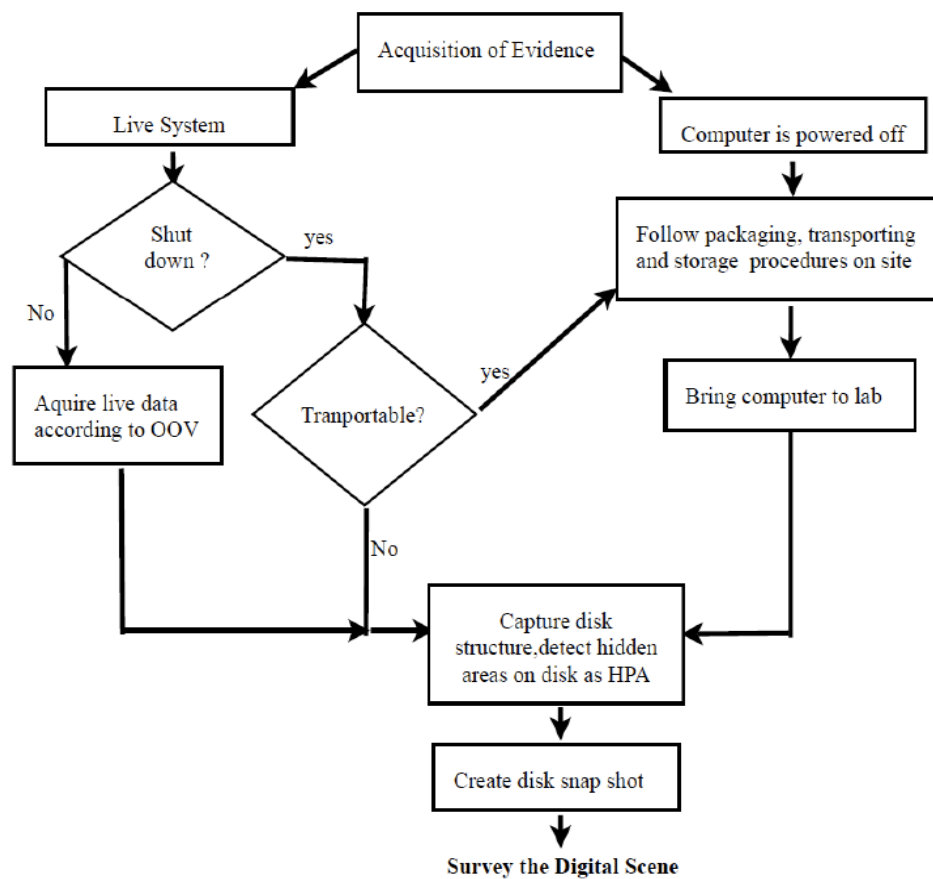


Figure 3.2: Acquiring Digital Evidence (Noureldin, Hashem and Abdalla, 2011, p.564)

As shown above, the third stage is surveying the digital scene, where the investigator identifies the locations of evidence in order to evaluate the suspect's skill level. This stage is important because it gives the investigator additional indications on where to find additional evidence and what new methods that can be taken based on the suspect's skill level. The next stage is examining digital evidence which aims to locate and extract every possible data including hidden, deleted, and inconspicuous data or any data that cannot be viewed by a normal operation mode. Then stage five, is the reconstruction of located and extracted data that will assist the investigator to find more evidence related to the case. The last phase is a conclusion where the investigator has clear results based on the findings. However, consideration needs to be made over both phases of digital forensics and physical forensics in order to "link a person to the digital events" (Noureldin, Hashem and Abdalla, 2011, p.567). And also to answer the questions that are derived from the physical evidence found at the crime scene. Figure 3.3 show the stages that need to be followed in the digital forensics phase.

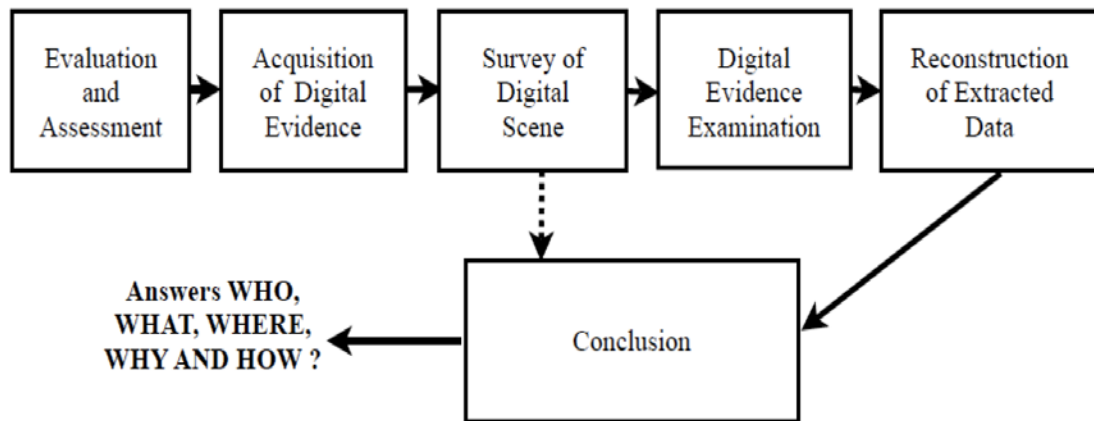


Figure 3.3: Stages of Digital Forensics phase (Noureldin, Hashem and Abdalla, 2011, p.566)

3.1.2 General Testing Methodology for Computer Forensic Tools

The National Institute of Standards and Technology (NIST) ran this project with the Department of Commerce in the US. This project was conducted to provide law enforcement and digital forensic investigators the ability to measure computer forensic tools in terms of their reliability and capability. They gave them the ability to decide whether a particular computer forensic tool is suitable for a certain purpose or not depending on the proposed approach used for testing the tool. According to NIST (2001), the proposed approach is supported by an agreement between NIST and several agencies including the Technical Support Working Group (TSWG), and Department of Justice in the US. The developed approach is based on well-known standards and methodologies for quality testing and conformance testing, including (ISO/IEC17025) ‘General requirements for the competence of testing and calibration laboratories’ (NIST, 2001, p.1).

The approach developed by NIST for testing computer forensic tools consists of seven phases. Figure 3.4 shows these phases that need to be accomplished when testing computer forensic tools.

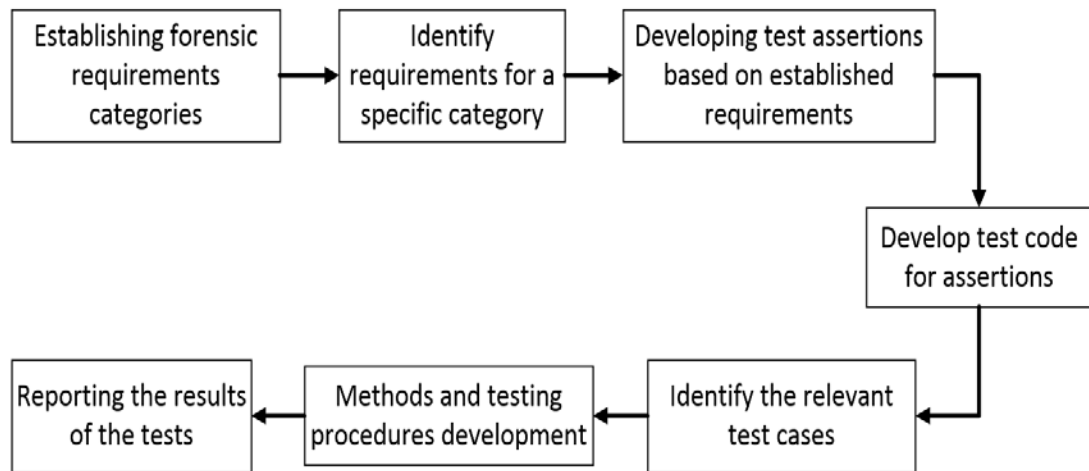


Figure 3.4: Proposed General Methodology for Testing Computer Forensic Tools
(NIST, 2001, p.2)

3.1.3 Recommended Guidelines for Validation Testing by SWGDE

Due to the necessity of test validation SWGDE has proposed step by step guidelines. These guidelines assess if the selected digital forensic tools can be used in an investigation, the techniques of use, the procedures followed, and it operates exactly as expected to ensure correct results. According to SWGDE (2014, p.2) they stated that the main objective is “to ensure the integrity of the components utilized in the forensic process”. The proposed guidelines is intended to be useful and suitable for every organization conducting investigations using digital forensic tools.

The proposed guidelines methodology consists of two parts: the test plans and the test scenarios. Before conducting any test, the test plan is created which outlines the scope and the purpose of a particular test. The requirements to be examined also need to be addressed, which means that the examiner or tester should include what a particular tool has to perform. The test plan is required to address the methodology including any additional tools that support the test or software which will be used to evaluate the expected findings, for example naming tools that will be used for verifying the integrity of the acquired image such as Tableau Imager and EnCase. After outlining the above steps, then each requirement in the test plan should have a test scenario, and each scenario has its specific procedures, and techniques. The last thing in the test scenario is to write down the expected result from the test and documentation. The second part of the proposed guidelines is to conduct the test scenarios created in the first part, and then documentation of findings is written in the testing report. All the tested scenarios must be documented. If one scenario is tested twice then it has to be

documented twice. However, each particular scenario has its own documentation, including dates of the test scenario. Then final report should address the overall results for all scenarios whether if it is pass or fail.

During testing the proposed guidelines recommended the examiner to use only tools and resources with known conditions. It also recommends using these tools and resources with their known configurations without making changes during the testing. The recommended guidelines outlines the processes that need to be taken if there is an event of anomaly during the test. The process consists of three phases, firstly by recognizing the reason of why the anomaly has occurred during the test. Secondly verification of the reason that caused the anomaly, and finally consider the previous two process to modify the test scenario if feasible to prevent the occurrence of an anomaly and then re-test using the modified test scenario.

3.1.4 Validation of Computer Forensic Software Utilizing Black Box Testing Techniques

Wilsdon and Slay (2006) begins with a comprehensive discussion on the needs for evaluation of computer forensic tools. There are a wide range of digital forensic tools that have many functions such as FTK and EnCase, Open Source, and so on. This makes it more complex for identifying testing requirements, which is unlike tools with a certain objective, that makes it easier to define the testing requirements (2006, p.3). The author stated that the methodologies proposed by SWGDE and CFTT (Computer Forensic Tools Testing) are forensically trusted, and these approaches are “extremely comprehensive” (Wilsdon & Slay, 2006, p.3). However, they stated that both of these testing methodologies are unable to meet the industry’s demands which is developing very rapidly (2006, p.3), because the tests can take too much time for an evaluation. Thus, the alternatives aim to propose a new testing framework that is similar to SWGDE and CFTT in terms of testing level, but more efficient in terms of time for testing, output and financial requirements (2006, p.3). The authors emphasise that the proposed framework is an evaluation that is focused on the reliability and the accuracy of the tools that are being used for computer forensics. In addition it is built based on two well-known standards that are designed for software testing, IEEE 610.12-1990 and ISO 17025-2005. The authors discuss the need for planning of the testing environment before conducting the actual test, and summarize the process suggested

by Whittaker (2000). It consists of four phases to be completed before conducting the testing (See Figure 3.5).

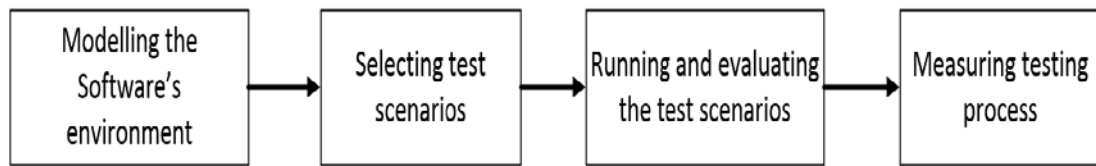


Figure 3.5: Plan for the Testing Environment (Whittaker, 2000)

The following Figure 3.6 illustrates the proposed framework by Wilsdon and Slay (2006) to evaluate forensic software applications. The proposed framework consists of six phases shown as a flow process.

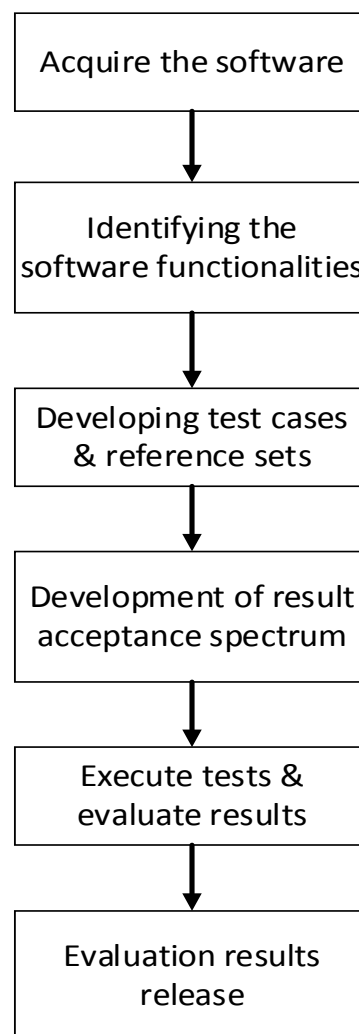


Figure 3.6: Evaluation Process for Forensic Computing Tools (Wilsdon & Slay, 2006)

The first phase for software tools evaluation is acquiring the software. This means that the software that needs to be evaluated and additional supporting tools are acquired and documented accurately. The documentation must meet the requirements presented in both the Australian Standard 4006-1992 and the ISO 17025-2005 standard.

Signature software is crucial in this phase, as it prevents any confusion between the tested versions of the software with future updates of the version. Thus, a unique signature of the software is obtained using MD5 hashing or another hash functions such as SHA1. The second phase is identifying the functionalities of the software, this phase is essential because it determines what sort of functionalities can be provided by the tool that will be tested. Some computer forensic tools provide a number of functionalities such as Encase, but only the identified functionalities will be examined depending on the investigation case. Tool functionalities can be obtained from the documentations presented by software vendors, or any other sources such as community discussion boards and online forums and so on. After identifying the functionalities of the tool to be tested, they need to be accurately documented, because the next phase of evaluation is based on the documented functionality. The next phase is using black box testing techniques to develop the test cases. According the authors (2006, p.7) the black box testing technique can be applied for software that prevents users from accessing its source code. The test cases ensure that all the identified software functions will be tested, and the identified functions are presented as a reference set. Each functionality has its own reference set, which can be applied if another software has the same functionality. According to the authors (2006, p.7) it can be practical to allow the community to review the reference set, as they can evaluate if the tests are suitable and sufficient. The next phase is creating a result acceptance spectrum, in order to assess the results collected from the test against the expected outcomes, which are predefined in the acceptance spectrum. According to the Wilson and Slay (2006, p.7-8) the method proposed by ISO 14598.1-2000 is applied to categorize the result acceptance spectrum into four levels; “Exceeds requirements, target range, minimally accepted, and unacceptable” (Wilson and Slay 2006, p.7-8). The fifth phase is to conduct the test and documents the results as per the requirements identified in the first phase, and then evaluate the results by checking them against the expected results that is developed in the fourth phase. The last phase is enabling the forensic community to access the final evaluation results. The authors (2006, p.8) stated that if there is any modification on the evaluated software, including software updates, and patches then the final evaluation results may not be suitable for a newer version of the software.

3.1.5 Digital Forensics Investigation Methodology Applicable for Online Social Networks

Jang and Kwak (2014) aim to provide a digital forensic methodology that can be adopted when conducting an investigation of online social networks. This paper started with a broad discussion on digital evidence from online social networks. The authors discussed the need for classifying digital devices such as computers and smartphones and other types of device since most of them can be used in online social networks. Thus, the proposed method considered different digital devices such as computers and smartphones. According to Jang and Kwak (2014, p.1) the proposed methodology is efficient in terms of its process, digital device classifications, evidence collection from OSNSs, and evidence analysis. Applying this proposed investigation methodology into the OSNSs environment will also ensure that different types of evidence will not be manipulated or damaged, including chats, suspect's friend's lists, and so on (Jang & Kwak, 2014, p.2). Figure 3.7 shows the proposed process for investigating online social networks.

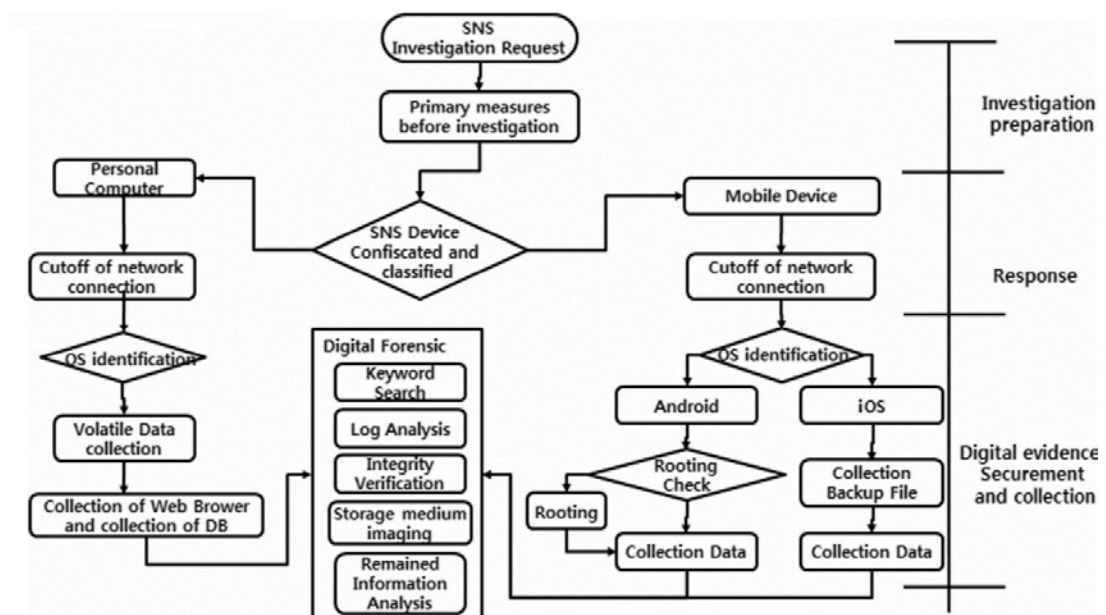


Figure 3.7: The Proposed Methodology for OSNSs Forensics Investigation (Jang & Kwak, 2014, p.3)

The proposed methodology consisted of four major phases which are: investigation preparation, response, collection and securing digital evidence, delivering evidence and confirmation, and finally examination and analysis. The proposed framework can be used when investigating two different types of smartphone operating system which are Apple IOS and Android from Google Inc. When an investigation is conducted for

computers, the authors included collecting volatile data using memory dump techniques. The authors discuss how to extract online conversation if the suspect logs go through a web browser. The methodology is useful for this research as it reflects on how OSNSs data can be acquired, and processed in a forensically sound manner, and gives insight into the proper handling of OSNSs investigations.

3.2 RESEARCH DESIGN

Section 3.1 provided five studies relevant to this thesis project. Each study is explained comprehensively in order to gain more knowledge on how to design and construct a suitable methodology that can be adopted when conducting a forensic investigation for online social networks. This section will describe and explain the research methodology that has been subsequently developed for this research, and is derived from the methodologies shown in the previous section reviews.

Section 3.2.1 summarises the five studies reviewed in Section 3.1 in order to address the strong points of each study, and to discard the points that are not relevant to this research. Section 3.2.2 reviews and discusses the issues and problems presented in Section 2.6, where several issues and challenges are encountered when performing a forensic investigation for OSNSs. After summarizing the relevant studies and reviewing the issues and problems, Section 3.2.3 will derive the main question of this research, sub questions, and the hypotheses which will be developed based on the established sub questions. Based on the relevant studies the methodology will be elaborated in Section 3.2.4. Section 3.2.5 is the data map for this research that links all the parts of the research design.

3.2.1 Summary of Similar Studies

The objective of this section is to summarise the five studies reviewed in 3.1 in order to extract the main strong points of each study which will give guidance for this thesis. The first approach by Noureldin, Hashem and Abdalla (2011) focused on proposing a guidance model that can be adapted when conducting a forensic investigation. The strongest point in this study is that the authors expanded their previously proposed model by using flow charts to addresses each phase of the investigation. The authors used flow charts to enhance and clarify each investigation phase, and to confirm that all evidence are handled correctly and with forensically sound method. This approach was tested on two case scenarios and they were effective in terms of forensic and

scientific principles. Thus, it is suitable for the proposed research. The second study by NIST (2001) and the third study by SWGDE (2014) focuses on developing approaches for testing forensic tools, with the purpose of evaluation and validation. Both methodologies are known in the forensic community. The objective of these studies is to precisely validate each function a digital forensic tool can perform after recognizing these functions. However both studies do not include the requirements that need to be tested, as stated in the fourth study done by Wilsdon and Slay (2006). The methodologies developed by NIST and SWGDE could not satisfy the forensic community demands for testing tools fast enough (2006, p.3). In the fourth study, the authors aimed to simplify what has been developed by NIST and SWGDE. The authors did not focus on identifying what is to be tested but adopted the testing requirements similar to what has been proposed in the previous studies. However, the authors propose a simplified methodology for tool testing, with more emphasis on how to conduct the test. The proposed methodology uses sets which identify different functionalities to be tested, and each functionality has its own reference set. This method does not require programming skills as it is based on a black box technique, and provides several benefits such as simplified processes, community interaction, and different environment testing.

The last study by Jang and Kwak (2014) classified digital devices into two sets, and developed an investigation methodology that can be used in online social networks. The proposed method can be useful for this research as the proposed method focuses on collecting the volatile data, and collection of Web browser data. It also has a database element and analysis processes for the collected data. The analysis phase consists of verifying the integrity of the collected data, keyword search, log analysis, storage medium imaging, and analysis of the remaining information.

3.2.2 Review of the Problems and Issues

Section 2.6 in the previous Chapter outlines the issues and challenges that forensic investigators encounter when conducting an investigation of online social networks. As discussed in 2.6.1 one challenge is that there is no standardized model that can be followed when performing an investigation for OSNSs. Thus the standardization issue may raise several concerns including relevancy or privacy concerns. However, this is not the most noticeable challenge as there are developed best practices that can be followed, and some standards that consider OSNSs investigation. The most noticeable

challenge to this field is the rapid growing of technology and social services whereas OSNSs forensic tools are still in its initial stages. Recently many online social networking sites have been developed, and each has its own objective and functionalities. Many of them are being used on a daily basis, which rapidly increases the percentage of data being transferred across the global network. Conversely, forensic tools for online social networks are yet to be developed in order to reach a sufficient level of technology where digital evidence can be extracted in a forensically trusted manner. Thus, commercial vendors are competing with developing efficient tools that can serve the forensic community by enhancing and providing more functionalities to their software, such as Internet Evidence Finder (IEF), Internet Examiner toolkit (IXTK), and Belkasoft Evidence Center. According to the vendors, these tools can be used for online social networks investigation, since all OSNSs interact with several artefacts which may be used for finding evidence. The problem areas were located in Section 2.6 and now a researchable question can be derived for this research. The following section presents the research question, sub questions and hypotheses for this research.

3.2.3 The Research Questions and Hypotheses

Chapter 2 has provided a comprehensive review of the relevant literature. Digital forensics was defined and the main goals presented. Also a list of digital forensic investigation process were reviewed that have been proposed by number of different authors. The characteristics of digital evidence and their admissibility were also reviewed. Section 2.3 discusses online social networks, their types, features, characteristics, and their impact on the society. The question of how these OSNSs can hold forensic evidence that could be used in a forensic investigation was considered. The different types of evidence that could be found in OSNSs is reviewed in Section 2.3.7. Digital forensic tools were comprehensively discussed according to the literature cited, and the tools that could be suitable for OSNSs investigation identified. Section 2.6 discussed some of the issues and challenges that are encountered when conducting a forensic investigation of OSNSs, which are summarized in Section 3.2.2. There are number of forensic tools that have been developed; some of them were recently developed and only a few can provide functionalities that are suitable for examining OSNSs. Some vendors update or upgrade their tool versions in order to enhance their capabilities. Forensic investigators may not be able to decide which tool is considered

better in terms of collection and analysis of evidence from OSNSs without actually conducting tool testing and comparison of these tools. Some tools may have better acquisition ability whereas other tools can be more capable in terms of evidence analysis. Therefore, the main research question of this thesis is based on the literature reviewed in Chapter 2, and the presented challenges and concerns. Thus the main research question of this thesis is:

What evidence can be extracted from online social networking sites when using different forensic extraction tools?

In order to answer the main research question a set of related sub-questions need to be addressed and answered:

Sub-Question 1 (SQ1):

What are the types of data that can be found for each online social networking site?

Sub-Question 2 (SQ2):

Can the selected tools perform a successful acquisition without the need for other tools?

Sub-Question 3 (SQ3):

What are the hardware and software applications used for extraction and acquisition of OSNSs data which best suits the three selected forensic tools for examination?

Sub-Question 4 (SQ4):

How are the collected data validated?

Sub-Question 5 (SQ5):

What types of data are within the scope for each digital forensic tool?

Sub-Question 6 (SQ6):

What is the ranking of the selected digital forensic tools in terms of accuracy and capability of extraction OSNSs data?

A set of hypotheses has been developed from the research sub-questions as follows:

Hypothesis 1 (H1):

It is expected that all of the chosen forensic tools will not recover everything posted on each OSNS. However, the chosen tools will be successful in acquiring sufficient information and from different locations that could be suitable for the digital forensic investigation.

Hypothesis 2 (H2):

When conducting a forensic investigation on different OSNSs, evidence collected from each OSNS will vary depending on the tool that is used to examine and search for evidence, and depending on the complexity of how each site is operated.

Hypothesis 3 (H3):

The chosen forensic tools will share common capabilities and functionalities. However, it is expected that Belkasoft will perform better in extracting private messages in all OSNSs, and by contrast IEF and IXTK will perform better in searching for evidence.

Hypothesis 4 (H4):

The collected evidence from each digital forensic tool will vary depending on the source of evidence RAM, Pagefile.sys, or HD, and it is expected that RAM and pagefile.sys analysis will add more value to the collected evidence during OSNSs forensic investigation.

3.2.4 Research Phases

In order to test the above hypotheses, and to answer the sub-questions and main question, the following five research phases have been developed (Figure 3.8). The first phase is a preliminary test of online social network functionalities and capabilities, and includes identifying the types of data that can be posted on each OSNS (Facebook, Bayt, Twitter, LinkedIn, Instagram), and the possible ways of posting data on each OSNS. This phase also aims to identify several browsers that will be used for accessing OSNSs. The review of literature related to tool testing methodology, and a review of technical documentation of the three selected tools produced by the tool vendors (Belkasoft Evidence Center, Internet Evidence Finder, and Internet Examiner Toolkit) are required to document test process. The result of this phase will determine what techniques should be used for posting data on each site, the usage of different browsers, and Case Scenarios for posting data on OSNSs. The posted data will be documented and labelled as controlled data

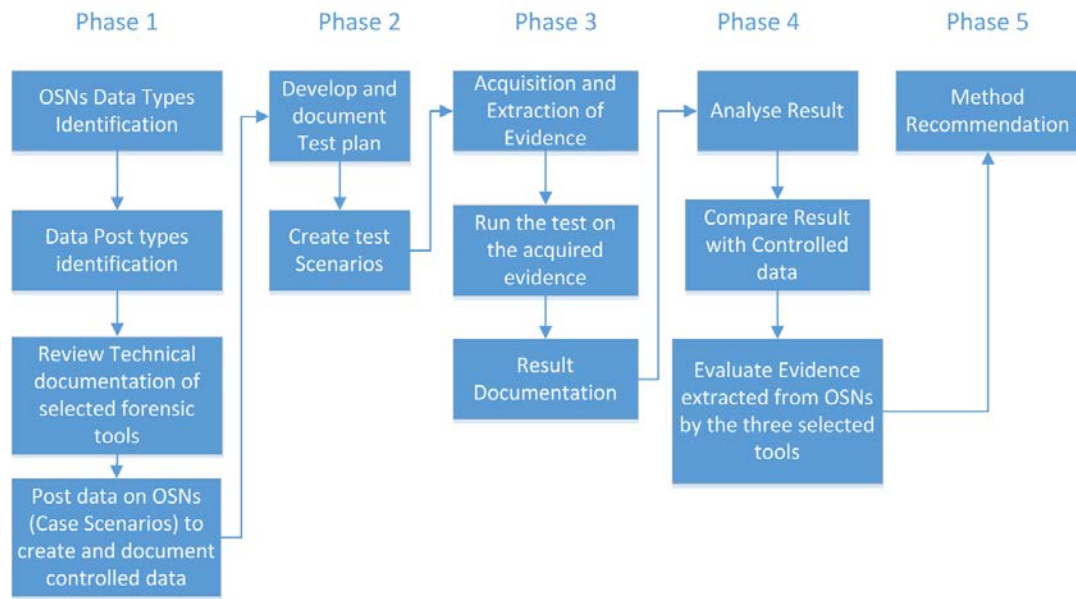


Figure 3.8: Research Phases

The Second phase is develop and document test plans based on the SWGDE approach for validating testing of tools. The test plan should include the purpose of the test, the scope, specify all the requirements that need to be tested, and develop the methodology that is used for conducting the test, and create test scenarios. The third phase is performing acquisition and extraction of evidence based on the computer forensics guideline methodology proposed by Nouredin, Hashem and Abdalla (2011). The fourth phase is data analysis. This phase will analyse the extracted evidence in the previous phase using the three selected digital forensic tools in order to reconstruct and conduct a comparative analysis between the controlled data generated in the first phase and the evidence reconstructed from the tools. Documentation will be made for each phase of the investigation in order to preserve a record of every step carried out during the investigation and to ensure that the experimentation is conducted in a forensically trusted manner. The last phase is method recommendation, which will provide other forensic investigators a recommended method for conducting an investigation related to OSNs. The recommendation will include a comprehensive discussion of the developed methodology, and how efficient this methodology is when conducting a forensic investigation on OSNs. The following sub section illustrates the proposed research data map that links all the data components of the research design.

3.2.5 Data Map

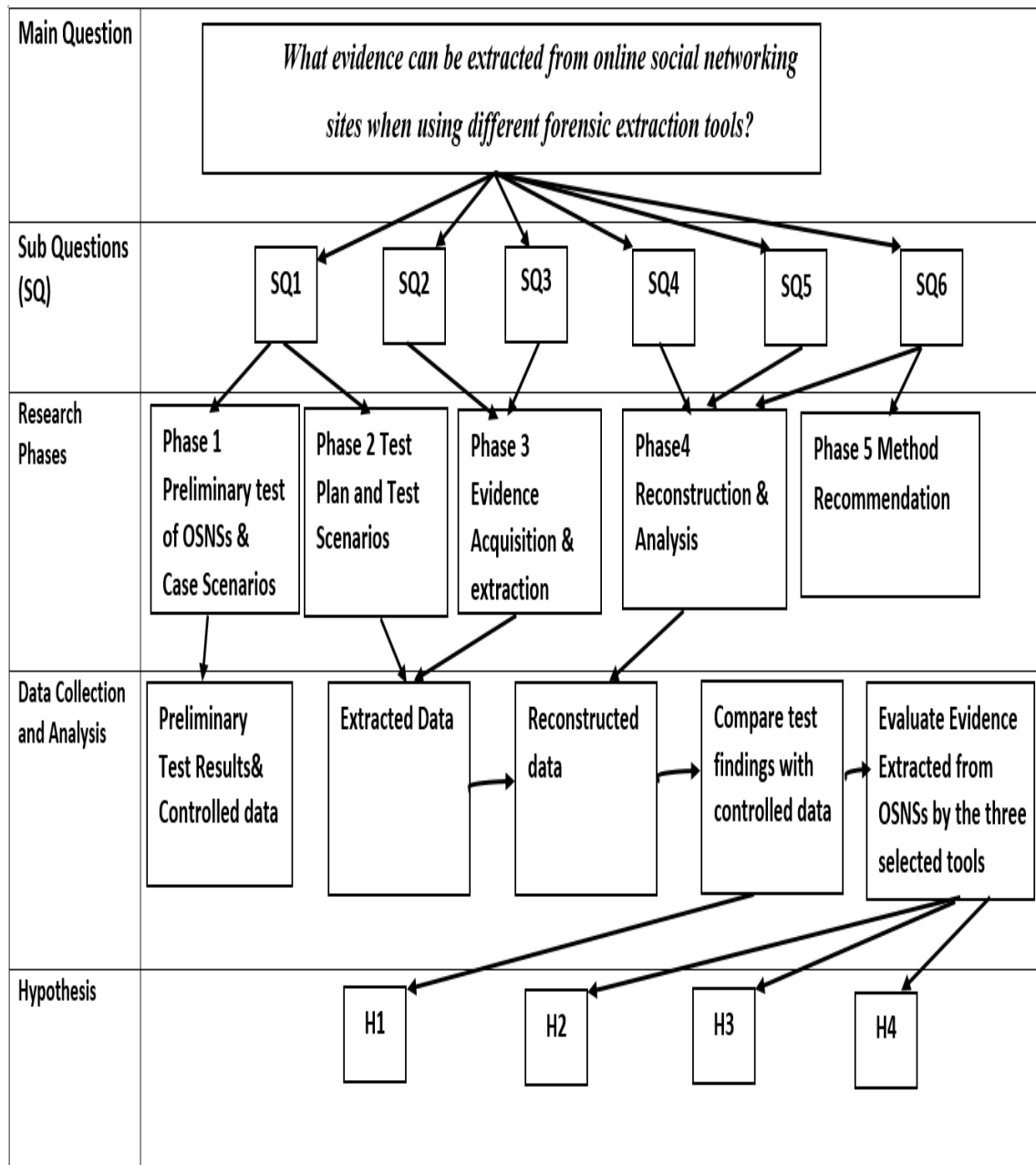


Figure 3.9: The Proposed Research Data Map

3.3 DATA REQUIREMENTS

For this research, there are different sources of data that are required to be collected in each phase including the preliminary test, controlled data, extracted data, and reconstruction of data. Also the result of the comparison between findings and controlled data, and documentation of each phase. In the preliminary test the result of this phase will determine the types of data and the ways it is posted on the selected OSNSs. Thus, case scenarios are important to be made in order to define the types and the amount of data that will be treated as evidence before conducting the investigation phases. It is also crucial to know what sort of information that needs to be analysed. The first phase will confirm that the intended computer to be analysed contains data from OSNSs which needs to be collected by applying the proposed research methodology.

The required data from phase 2 is test plans which are developed based on the SWGDE approach for tool validation testing. Documentation will be made for each test plan, which identifies requirements, scope and the testing methodology. The third phase is to performing acquisition and extraction of evidence based on the computer forensics guidelines methodology proposed by Nouredin, Hashem and Abdalla (2011). The fourth phase is data analysis. This phase will analyse the extracted evidence in the previous phase in order to reconstruct and conduct a comparative analysis between the controlled data generated in first phase and the evidence from each tool. The following sections will describe in more detail what the data for testing are, and how it is going to be processed and analysed, and how it is going to be presented.

3.3.1 Data Collection

There are several types of data that need to be collected. The Preliminary test phase will result in the following: 1. Determine the types of data that can be posted in OSNSs. For example Facebook accepts posting images, text, videos, likes post, comments, and so on. 2. Identify ways of performing posts such as private messages, wall posts, chats, group or community pages, friends' wall posts and so on. Then case scenarios will be created where different types of data will be uploaded on the selected OSNSs, different ways of posting evidence will be made. This process ensures that there is evidence that can be collected from OSNSs when performing the next phases. The generation of data

activities will be conducted on the experimental computer in a controlled lab environment. All the created activities will be recorded including the data posted on OSNSs which are called the controlled data. The controlled data will be used in a later phases of the investigation where a comparative analysis will be conducted.

After performing all the above, the plan for tests will be developed. The test plan will be based on the approach proposed by SWGDE for validating testing. There are number of requirements of data that need to be collected in this phase. Firstly, identifying the scope and the purpose of each test plan, identify the requirements needed to be tested. For example: what does the selected tool have to do? Identify the method that will be used for testing (Phase3). Based on these requirements, test scenarios will be made. Note that the case scenario developed in the first phase is different from the test scenarios. The case scenario is developed to generate evidence (controlled data), but the test scenario will determine the following: 1. The environment required for the test scenario such as identifying which selected tool will perform in this scenario (Belkasoft, IEF, IXTK). Also identifying supported tools for acquiring evidence image files (for example, Tableau bridge write blocker). Identify the action to perform during utilizing the tool, and identifying the expected result which is known as the controlled data that is documented in the first phase. The last part of the test scenario is to determine if the test is (Pass / Fail) based on comparing the controlled data with the result of analysis.

The data collected in the previous phase, will be documented accordingly and will be used in the third phase, Extraction and Acquisition. In this phase, the extracted data will be collected in a forensically trusted manner. The write blocker will be used for acquiring evidence from the storage media. The purpose of using a Write Blocker is to ensure that the evidence is imaged without any changes during process, and it permits investigators to read information from the target machine but it does not allow any alteration or modification to the data. Thus, using a Write Blocker ensures the preserving of the integrity of evidence, by calculating a MD5 hash value after acquiring the evidence.

After acquiring the image and verify the integrity of the evidence, the extracted information can be collected. During the forensic analysis process in phase four, the reconstructed data will be collected and documented accordingly. The reconstructed data will be the result of the case scenarios created in the previous phase, and will be compared with controlled data. Data reconstruction will enable the investigator to

determine how the evidence got where it was and to give traces on where this evidence came from (Carrier, 2009, p.26). In order to make investigation phases repeatable, all the procedures made in the investigation phases will be recorded and documented. This step is very important not only enabling repeatability of procedures and phases, but also it will assist in making recommendation for conducting a forensic investigation on online social networks.

3.3.2 Data Processing

The previous section discussed the types of data that is required to be collected during the investigation. These data include: preliminary data of OSNSs, evidence data (Controlled data), and the extracted data in phase 3. Also the constructed and analysed data in phase 4 and comparison result data between the final data and the controlled evidence. All the presented data will be documented in an excel sheet in order to make it easier to follow what has been done during each phase. The first data to be processed is the controlled data, and this will be done in controlled lab environment where one desktop computer will act as the suspect's computer, and the other one is the forensic investigator's computer. The first computer will have a newly installed Windows 7 Operating system. The computer's hard drive will be wiped using an efficient wiping tool utility. There are two tools that will be considered in the experiment. The first one is Disk Wipe which erases data from hard drives in a secure manner. The other tool is called Darik's Boot and Nuke (DBAN), and both tools are free utilities. Then three well known browsers which are Internet Explorer (IE), Firefox, and Chrome will be installed. The browsers will all interact with the selected OSNSs in order to generate controlled data. Based on the preliminary test, there will be different types of data to be posted, and different ways for data posts in each OSNS. These data will be compared in the final stages of the investigation in order to draw a conclusion about the evidence found from each forensic tool. The investigator's computer will have the selected forensic tools installed. Each Scenario will be conducted with each of the three selected tools.

3.3.3 Data Analysis

There are three levels of data analysis for the proposed research. The first level is analysis of the preliminary test of online social networks conducted in the first phase of the proposed methodology. The second level of data analysis will be conducted on

the acquisition and extraction phase, and data reconstruction analysis. The third level of data analysis will be a comparative analysis between controlled data generated in the initial phase with the result of data analysis in the reconstruction phase.

The first level of data analysis will be based on selected OSNSs. It is crucial to analyse each of the selected social network's features and capability in order to understand what type of data are supported, and how the data are being processed within the site. This will help the investigator during the forensic investigation to have a clear picture on what sort of evidence can be collected from each site. Since each site has its own capability, it is expected that one site will have more capabilities in terms of posting methods, and allow several types of data to be posted. Analysis has to be made in order to build a fair result at the end of the thesis.

The second level of data analysis will be conducted in order to examine the integrity and the accuracy of the acquired data to ensure that the process is made in a forensically trusted manner, and for the next phases of the investigation. After the accuracy analysis of the evidence image, a forensic analysis on the evidence will be made in order to understand the meaning of the data, and to find out if the data is related to the case or not. The forensic analysis of the same image will be conducted using the three selected tools in order to analyse the evidence with the aim of answering questions like: what kind of information has been posted on which OSNS? What browsers have been used, and visited URLs? Analysis of the three selected tools will be conducted in depth, and the digital forensic phases will be based on the methodology proposed by Noureldin, Hashem and Abdalla (2011) which is discussed in Section 3.1.1 and Section 3.2.

The analysis of data by each selected tool will be a crucial part for the third analysis level which is a comparative analysis between controlled data generated in the initial phase with the result of analysis conducted on phase 4. The purpose of this analysis is to compare the evidence extracted from the three forensic tools, and to determine the types of evidence extracted from each OSNS. The result of this analysis will eventually be sufficient to answer the main research question:

“What evidence can be extracted from online social networking sites when using different forensic extraction tools?”

3.3.4 Data Presentation

In the first phase, the data collected in the preliminary test will show the features and capability of each OSNS. It will have types of data such as files, images, videos, text, audios, and documents and so on, and types of processing data such as instant messaging, wall post, hashtags, group, and community pages and so on.

After presenting the data from each site, then the controlled data (simulated evidence) will be presented. This operation is important to make sure that each examined OSNS has collectable data that can be used as evidence. The controlled data acts as the expected data in later phases. The presentation of the controlled data will be in a tabular form to show the types of data that will act as evidence in each OSNS.

The selected digital forensic tools provide comprehensive reports based on analysis findings. The analysed data in phase 4 will be presented in table format, and this is to make it easier to follow the guidelines proposed by the SWGDE on validation tools, where one of the requirements is expected results. The expected results will be exactly same as the controlled data initially presented. Comparing will be made after constructing all the table. A comparative analysis will be presented in a table format, which will show all the tools and if the data are found or not found.

Based on the final analysis results, a recommendation for effective forensic investigation on the three selected tools will be made, noting their capabilities of extracting evidence from OSNSs. The recommendation will also deliberate on the chosen OSNSs, and the chosen methodology for this research in order to present knowledge for future researchers.

3.4 LIMITATIONS

The proposed research is intend to evaluate evidence that can be extracted from online social networking sites using three well-known forensic tools. There are several limitations for the proposed research, and it is crucial to discuss these limitations in order to define the scope and the application of the study. Also such declared limitations provide starting points for future research areas.

There are several tools that could be used for evidence extraction from OSNSs, and the chosen tools were selected based on their reputation and availability. The three selected tools are advanced in terms of their functionalities and features. They provide capabilities in examining hard drives, computer's volatile memory, and extract

evidence from OSNSs from multiple sources and so on. However, none of these selected tools is designed for extracting evidence from OSNSs. There are other functionalities that these tools can provide, which are not going to be tested in this research because they are not relevant to the research area. Thus, this research area will focus on the relevant features of the tools, and the findings of the research will be specific to the examined features. The other tools are not selected due to the time constraints, and it is not possible to test all the forensic tools within the specified time frame for this research.

Secondly, there are many online social networking sites and the selected ones were based on their popularity. This research does not cover every social network, and the, procedures, proposed methods, and findings may not be efficient to be applied for other OSNSs, as each one has its own functionality and architecture. Another limitation is that all of the chosen OSNSs can be accessed via devices such as smartphones and PDAs, and many users may access these OSNSs via different devices, and there are several operating systems that are used for smartphones such as IOS and Android. Therefore, this research is limited to computer systems.

Thirdly, the operating system is used for the experiment is Windows 7 platform, since it is the most popular OS nowadays. However, there are other OS that are not considered in this research such as Linux and Mac platforms. Similarly, there are other web browsers that are getting popular by security experts users such as the Tor Browser which is used for securely browsing web pages. Browsers that have similar security enhancement maybe used for a real case scenarios where suspicious activities may be performed on OSNSs. This may result in making the forensic investigation even harder. This research will only examine three well-known browsers, and the researcher suggests focusing on other browsers for future research.

3.5 CONCLUSION

The literature reviewed in Chapter 2 provided a comprehensive introduction to the field of digital forensics and online social network forensics, and listed a number of issues and challenges for conducting a forensic investigation for OSNSs. Chapter 2 showed that there is a need for developing the area of OSNSs forensics in order to reduce the presented challenges and issues, and to enhance the digital forensics technology which will improve forensic investigators capabilities. Chapter 3 presented

a comprehensive overview of the proposed methodology that will be used in this research. The main research question and related sub-questions were derived for answering, along with hypotheses. The research phases are carefully explained which are crucial to be followed during the investigation in order to achieve the best results from this research. Chapter 3 analysed five similar studies for methodology that relate to the research area. The objective of reviewing different studies is to assist the researcher in developing and adopting a suitable methodology for the proposed research.

The data that needs to be collected in this research is divided into sections which was discussed in Section 3.3.1. The data map for this research is presented to show how each phase of the proposed methodology will be conducted and what data will be collected in each phase, and how are the questions, and hypotheses relate to the developed methodology.

Finally, the limitations of this research has been presented in order to clarify the scope. The limitations illustrated shows that there are several research areas that can be feasibly conducted in online social network forensics. The next Chapter will report the research findings gained by applying the proposed methodology from this Chapter.

Chapter 4

Research Findings

4.0 INTRODUCTION

Online Social Networking Sites (OSNSs) have become one of the crucial sources of forensic evidence due to the rapid increase of online social networking users. There are number of digital forensic tools that can be used when conducting a forensic investigation of OSNSs. However, as reported from the literature, there is still a lack of tools that are specified for online social networks. The existing tools may not be able to examine every social network site as there are many of them and each OSNS has its own architecture, security features, and different types of data that can be posted. The existing tools also cannot examine and extract all the types of data, nor artefacts from online social networks. The literature in Chapter 2 has reviewed a wide range of topics that are relevant to digital forensics, digital evidence, online social networks forensics, digital forensic tools, and OSNSs forensic tools. Subsequently, the Chapter concludes by reporting the challenges and issues with OSNSs forensics. Based on these challenges presented in Chapter 2, the main research question, sub-questions, and research hypotheses were derived and formulated in Chapter 3.

The purpose of Chapter 4 is to report the analysis and findings of the research phases outlined in the Chapter 3. Chapter 4 consists of 4 main sections. The first Section 4.1 discusses all the variations and modifications encountered between the proposed research methodology and data requirement in Chapter 3, and the actual testing experiment performed. Section 4.2 presents the findings of OSNSs preliminary test, the environment setup for conducting the experiment, the case scenarios created for the experiments and the controlled data simulated for the two case scenarios. Section 4.3 and Section 4.4 are the data collection and analysis for the first case scenario that involves Facebook, Twitter, and Instagram, and the second case scenario that involves LinkedIn and Bayt. Also the test plans, and investigator machine setup environment are implemented. The report of digital forensic investigation findings using the three digital forensic tools, and comparative analysis of each case scenario are included.

4.1 VARIATION AND MODIFICATION ENCOUNTERED

The purpose of this section is to discuss and clarify changes and variations from the methodology specifications in Chapter 3, Section 3.3 data requirements. The data requirements consist of data collection, data processing, data analysis, and data presentation. The following sub sections will discuss the variations encountered during the testing in each of these four elements. The purpose of outlining variations is to clarify what exactly has been done and to ensure that the outcome of the research findings is not affected by such changes.

4.1.1 Data Collection

In Section 3.3.1 there are several types of data to be collected which are from the preliminary test phase, controlled data (Case Scenarios), test plans, test scenarios, acquisition of data, data analysis, and comparative analysis. In the actual experiment, there were some changes made to the preliminary test phase. The objective of this phase is to comprehend what type of data each OSNS allows to be posted, and how it is posted, and then creating case scenarios to generate the controlled data. During preliminary test, it has been found that each OSNS provides a wide variety of features, and each site differed from the other. Facebook for example, permit users to create groups, write notes, assign places, and create a community. By contrast, Twitter can be used for tweeting, direct messages to friends, adding users and following trending topics. Twitter doesn't have features for community or group pages except using hashtags. Thus, the experiments were conducted on the primary and the main features of each OSNS which includes posting text, pictures, videos, posting on friends wall, private messaging, sharing links, viewing pictures and videos. And also Tweeting to friends, retweeting, posting comments, like pictures, posting questions, making recommendations, and answering questions. Furthermore, Section 4.2 discusses the types of data that are acceptable on each OSNS and the types of data used in the experiments.

Memory dumps are an invaluable source of ephemeral evidence and volatile information. The RAM may contains crucial information including account login credentials and posted data for many OSNSs such as Facebook, twitter, and google plus (Belkasoft, 2015). Thus, RAM acquisition and analysis was added to data collection during the experiment.

There was one laptop available which is used as the suspect's computer. The laptop is equipped with 2 GB of RAM and 160 GB of HD. RAM analysis may be effected due to the small amount of GB available comparing to newer devices which have between 8 and 64 GB, and since there are five OSNSs to be tested on three different browsers, it is more likely that the initial data posted may not be found, because RAM overwrites when it is full (or signals the user to back up and delete). To ensure that evidence is not lost because of the size of the RAM, two separate case scenarios were developed. Case Scenario one is for Facebook, Twitter, and Instagram, and, Case Scenario two is for LinkedIn and Bayt. Each case scenario has its own controlled data, test plans, and test scenarios. Pagefile.sys is another crucial system file, which may store crucial data for OSNSs activities. Since the system may run low on RAM because of applications that may take too much memory like Firefox (Nair, Ajeena, 2014), these activities may be swapped to the pagefile.sys. Thus, it has been added to the data collection along with the RAM.

Due to the addition of RAM and pagefile.sys examinations, more test plans were created for both case scenarios in the data collection, and analysis of evidence. The number of digital forensic tools remain unchanged which are Belkasoft Evidence Center, Internet Examiner Toolkit (IXTK), and Internet Evidence Finder (IEF), and the three selected browsers remain unchanged which are Firefox, Chrome, and Internet Explorer (IE).

4.1.2 Data Processing

The proposed method for processing the controlled data remained unchanged. The investigation was done in a controlled lab environment where one computer acts as the suspect's machine, and another computer is for the investigator.

An additional process was added for acquisition and extraction of evidence. The proposed method did not include processing a RAM memory dump. However, it has been done in the actual testing. An additional tool was needed for acquiring RAM which is FTK imager lite 3.1.1. FTK imager is also used for imaging the evidence by performing an image bit for bit of the data in a forensically trusted manner.

There are four images processed for analysis using the three selected digital forensic tools. Each one of the images has its own test plan and test scenarios. The testing plans and scenarios remain unchanged from the proposed methodology, which is developed based on SWGDE approach for validating the testing of tools. Processing

evidence for acquisition and extraction and analysis has been done based on the computer forensics guidelines methodology proposed by Nouredin, Hashem and Abdalla (2011) as proposed in Chapter 3.

4.1.3 Data Analysis

There are three levels of analysis (Section 3.3.4) that shows the preliminary test of OSNSs, acquisition and extraction and data reconstruction analysis, and comparative analysis between controlled data and the found evidence. It is stated that forensic analysis of the same image will be conducted using three forensic tools. However, in the actual experiment there were four images. Case scenario 1: Hard drive image, and RAM memory dump and Case scenario 2: Hard drive image, and RAM memory dump along with their pagefile.sys acquired during the RAM acquisition. Thus, four cases have been created on each digital forensic tool. For example: in Belkasoft the first case is for case scenario 1, with the image analysed: RAM & Pagefile.sys. The second case is for case scenario 1, with the image of the suspect's hard drive, and so on for the second case scenario, and then for the other two forensic tools.

4.1.4 Data Presentation

Data presentation of the preliminary test and test plans, and scenarios remain as proposed in the Chapter 3. However some changes applied to presenting analysed data. Instead of presenting analysis of the three tools used to analyse one image, the analysis presentation will be made for three tools against four images with the same methodology proposed by SWGDE approach for tool validation.

4.2 ONLINE SOCIAL NETWORK PRELIMINARY TESTS

The purpose of preliminary phase is to explore each OSNSs capabilities and limitations of posting data into each OSNS, and identifying the types of the allowed data to be posted, and the possible ways of posting these data on the five selected online social networks: Twitter, Facebook, Instagram, LinkedIn, and Bayt. Each site has its own distinctive User Interface (UI) design. This section discusses the structures, applications, features and data of these OSNSs. Findings of this section will assist in creating a case scenarios for extermination testing, and will also determine the types of data that will be used as evidence in each OSNS.

4.2.1 Facebook

Once a new user creates a Facebook account, a new profile page is automatically created for the user. The profile page is referred to as a timeline. Facebook has changed the name of profile page to timeline because it becomes an ongoing history of the user's life on Facebook since the day they registered. The following Figure 4.1 shows the timeline (profile page) layout of Facebook. The timeline permits users to specify all kind of privacy controls on every piece of information they post. Each user has the ability to specify who they want to view specific information or post via the timeline. In the timeline each post is categorized according to the time they were uploaded. Through Timeline a user can post statues, photos, videos, life events, share links, and post files as attachments.

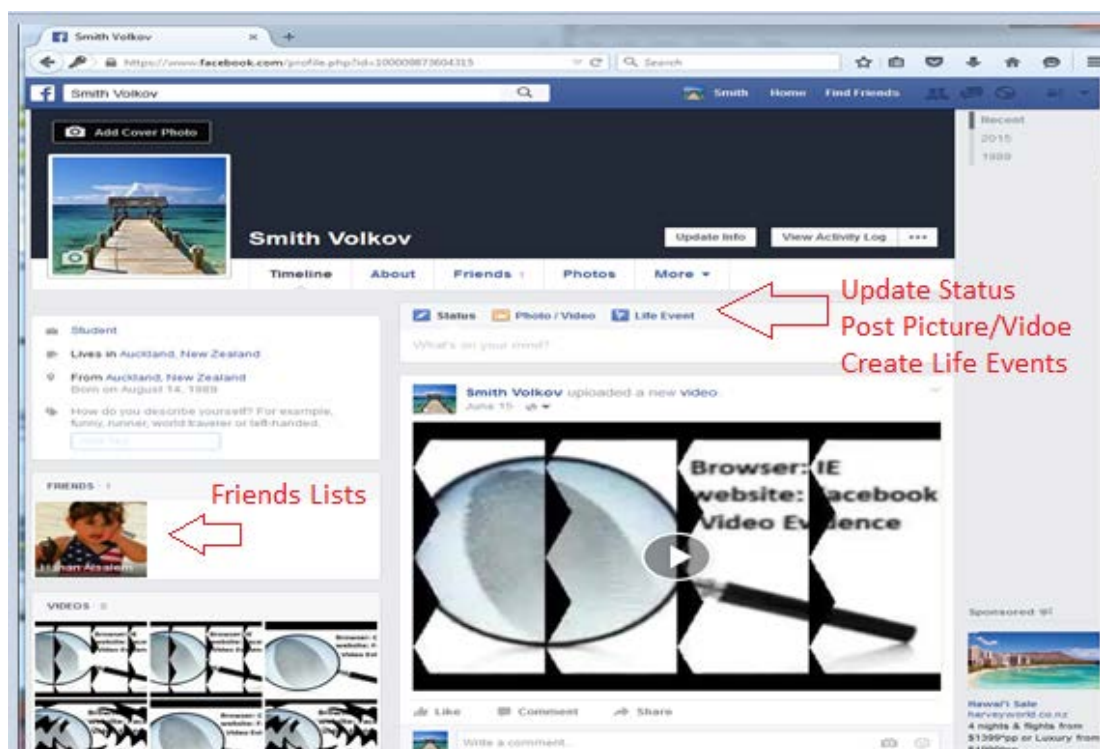


Figure 4.1: Facebook Timeline Page (profile page) Layout

When timeline is created the user will be able to add friends, by firstly finding friends by searching their names, email addresses, or through phone numbers, and then to send a friendship request. The user can then send private messages to a friend, write or post pictures and videos on friends' walls, and like and comment on their posts, and invite them to group pages or events which can be created by individual users. Facebook groups are mainly used for collaboration and discussions between numbers of users, and the users in the group are permitted to post contents such as documents, questions,

status, comments, links, photos, and videos. Facebook groups also have their privacy controls, where the creator of the group page can specify on whether to make the group is open, closed, or secret. Events are different to groups, as events are a way of users to let their friends know about upcoming social gatherings or occasions. Locations can be added to all types of posts. The location means the physical place of the user when posting content. Users may also tag other friends within a post, which means that the posted content will show on their timelines too. Each Facebook post has unique information represented in a URL. For example, a user may post a picture on their timeline. The post will have a unique URL that shows the users ID, and the picture ID. A typical URL of uploaded image on Facebook may show as this:

<https://www.facebook.com/photo.php?fbid=xxxxxxxxxxxxxxxx&set=a.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx&type=1&theater>

Any media uploads on Facebook maybe accessible if the post URL is known. However, it depends on access privileges, this means that the user may customise post privacy by assigning only friends to view the post or make the post private which means it is not viewable for everyone. However, by default the posts were set to public which means that any user obtains the full URL of a post can view the post without even a login to Facebook. When conducting a forensic investigation on Facebook, evidence may be found in a verity of locations some of which may be inaccessible. Table 4.1 summarizes the types of data that can be collected from Facebook, and possible locations that maybe stored.

Table 4.1: Types of Data Can be collected from Facebook

Types of Data	Brief Description	Data Possible Location Stored
Images & Videos	Collection of all posted images from three selected browsers (Firefox, Chrome, IE) from internet cache and temporary files. Collectable data include the URL path, the post type (photo/video), User ID, post ID	Images maybe stored in: RAM, pagefile.sys, user data, temporary internet files, cookies, web cache, hiberfil.sys file, browser history, local files, and log files
Statues and wall posts	Collection of user's wall posts and status, and other posts made by the user on friend's wall. Collectable data includes the username and ID, and friend's username and ID, the post content includes text written as a post, shared links, and file attachments. Collectable data may include tagged users in the post, and the location & date/time of the post made	Posts maybe stored in: RAM, pagefile.sys, user data, AppData, temporary internet files, hiberfil.sys, web cache, browser history, and unallocated space

Types of Data	Brief Description	Data Possible Location Stored
Comments and reply and likes	Collection of user's comments on a post or status and replies to comments in comment section. Likes of any post, comments or replies	User posts maybe stored in: RAM, pagefile.sys, web caches of browsers, hiberfil.sys, user data folder, and unallocated space
Private messaging/ instant messaging	Facebook messages that are sent or received from one user to another, the data that can be collected from private messages are: The content of the message, Message id, the sender fbid, and the receiver fbid, timestamp of each message sent and received	Chats maybe stored in: RAM, temporary internet files, web caches of used browsers, system page file, and could be found in unallocated space

The web browser is an essential place that has to be considered when conducting a forensic investigation. Facebook data can be restored from the web browser cache that is found on the hard disk, and also from log files, and cookies which depends on the type of browser used, and version. Some evidence may not be found on hard disks, but it is possible to be found in RAM, pagefile.sys, or hiberfil.sys files.

4.2.2 Twitter

Twitter is different from Facebook. It is less about social friendships, and connection with friends. Twitter focuses more in the real time discussion, topics, and news. Users can send a continuous tweet, where each tweet cannot be more than 140 characters. The following Figure 4.2 shows the twitter homepage layout. The layout of Twitter homepage is designed into four sections. The first section above contains Home tab, Notifications, and Messages. The second section of the left of the homepage shows the account holder username, Number of tweets, number of followers, and number of the people who is following. In Below, it's a Trend section which illustrates the top trending topics around the world. The middle section of the homepage shows the instant tweets posted from other users who are being followed by the user, and the section bar where the users posts contents (Tweets). The right section is a list of users who are recommended by Twitter for the user to follow.

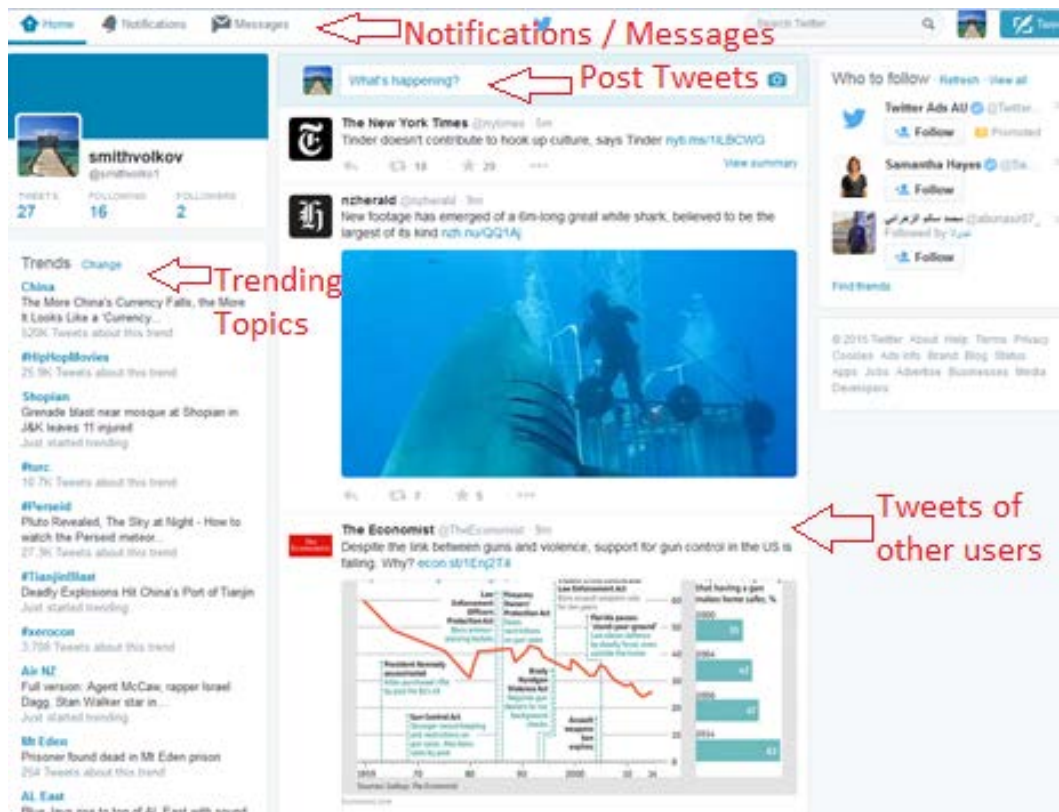


Figure 4.2: Twitter Homepage Layout

There are five ways a user can share their post on Twitter: normal tweets, mentions, replies, retweets, and direct messages. When user sends a normal tweet, it will appear on all of their follower's home timelines. Mentions are tweets that contain another user's Twitter username which is entered after "@" symbol, this will appear on the senders profile page, and the recipient profile page and home timeline. The mention will also appear on all the users' home timelines who follow the sender. Reply tweets is any tweet that begins with another username. This tweet will appear on the sender profile page, and the recipient's home timeline. The reply tweet will appear to the followers' home timelines who are following the sender and the recipient at the same time. Retweet is re-posting a tweet that other users have tweeted; the retweet will appear on the user's home timeline. Direct messages are private messages that a user can send to another user. However it depends on the user's privacy settings, if it is disabled then no one can send private messages to the user.

There are different types of data that can be collected as evidence on Twitter. Firstly evidence presented as texts (Tweets), and private messages between users, the retweets which are normally considered an endorsement of someone else's tweet such as: promoting violent ideology, threats, violation of laws, selling prohibited items.

A User ID is unique data which sometimes appears within URL that represents the status update. There are other evidence such as tweeting pictures and images, tweeting (sharing) links, and tweeting short videos. Twitter currently supports image formats of PNG, JPG, and GIF. Picture posts on twitter would normally appear as the following:

“<https://twitter.com/<username>/status/<uniquepost ID>/photo/1>”

In terms of videos, Twitter only allows sharing videos via twitter apps for mobile phones, and it permits only 30 seconds per video. Users might upload a video via desktop but with the need of a third party services such as YouTube, TwitVid, and Twiddeo. Evidence can be collected from twitter from a range of sources including RAM, pagefile.sys and hiberfil.sys files, Session store, temporary internet files, web cache, user data, cookies, and browser history.

4.2.3 Instagram

Instagram is an online mobile photo and video sharing, and online social network service that permit users to share their pictures and videos links on other OSNSs such as Twitter, and Facebook. Each user has their own account which can be accessed via mobile phones and desktops. Figure 4.3 shows an Instagram homepage layout logged in via a PC.

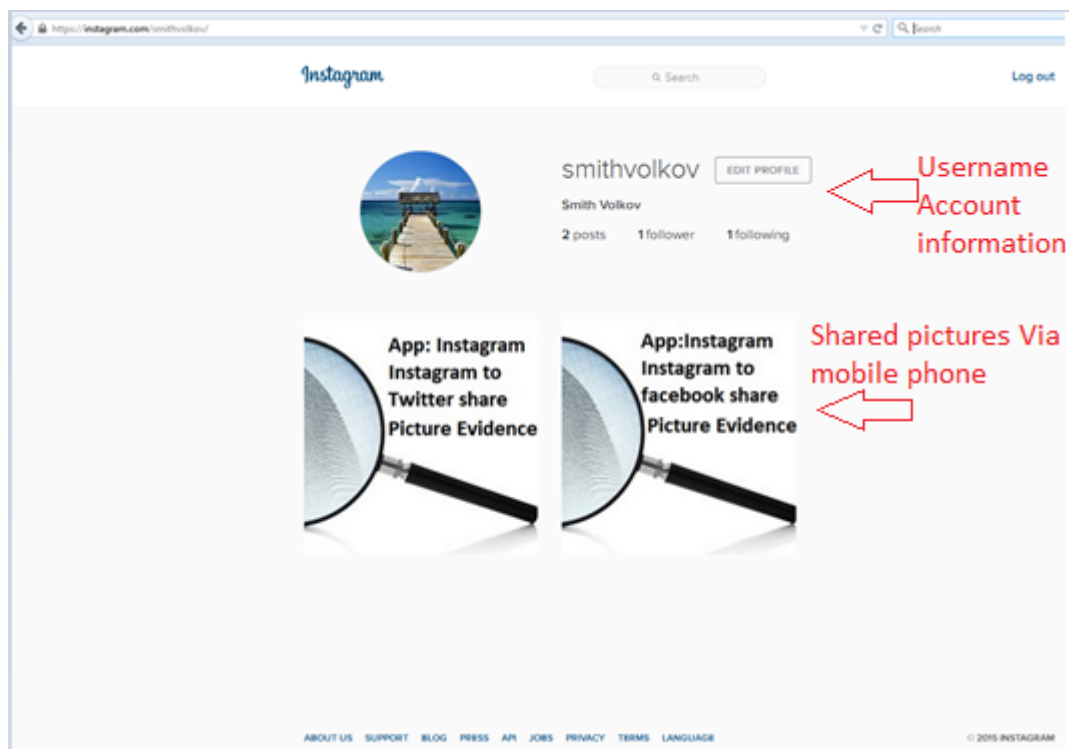


Figure 4.3: Instagram Homepage Layout

Users have the ability to like and comment on the posted pictures and videos. They also can comment on the shared links on other OSNs. Recently, Instagram has added a feature called Instagram Direct which is a private photo and video sharing feature with other users. There are no private messages (text) on Instagram as the main objective is sharing photos and videos and sharing their links with other online social networks. Instagram accounts can be accessed via PCs but the user cannot post photos or videos. However, users can view the previously posted content on their homepage and view other user accounts. The shared links can also be accessed via PCs if the links are known. Each Instagram post has its unique URL. The URL redirects to the data where it was originally posted. The posted contents can be viewed along with the username of the account holder. When an Instagram account is set to private it means that no one except the followers can view the post. However, if a non-follower knows the uniquely shared link to a post, then that specific post could be viewed no matter what the security settings. Instagram shared links would normally look like:

[“https://instagram.com/p/xxxxxxxxxxxxxxxxx/”](https://instagram.com/p/xxxxxxxxxxxxxxxxx/)

The types of collectable evidence in Instagram include usernames, photos and videos, shared URLs. These data might be found in browser history, Cache, Temporary files, RAM or pagefile.sys or hiberfil.sys.

4.2.4 LinkedIn

LinkedIn is another kind of social network with more focus on business-orientation, and where users build their own professional networking connections with others. The main objective of LinkedIn is to permit users to communicate with other users who have similar proficiency, and to communicate with vendors and seek jobs by promoting themselves through presenting their past and present jobs. In LinkedIn, there are a range of information and data the users can post, such as sharing an update status, posting a picture, comment or like pictures, adding professional user information, and sending private messages. The following Figure 4.4 shows the user homepage on LinkedIn. Similarly these posts can be found within a browser history, RAM, and system page file.

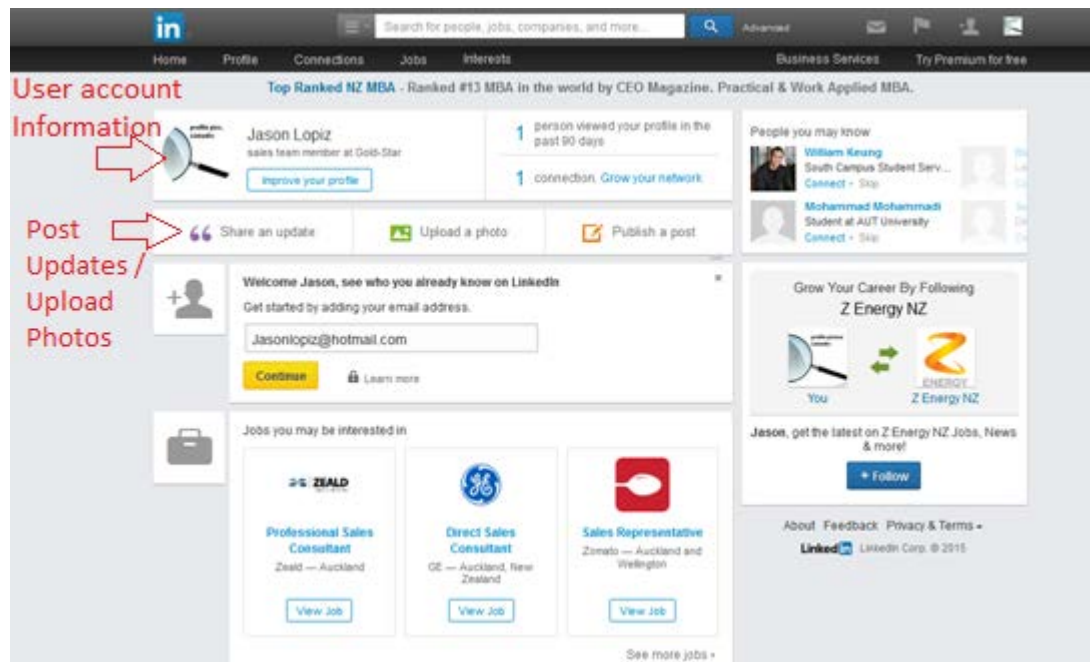


Figure 4.4: LinkedIn Homepage Layout

4.2.5 Bayt

Bayt is similar to LinkedIn in terms of its objectives, but it is more focused on connecting professionals in the Middle East. Bayt users can establish their own professional profile, build and maintain their professional network, find and connect with their friends who are in the same field, find a wide variety of companies and industries, and apply for jobs. Bayt users can post questions (in text only) which can be read by a wide range of professional users within the same field. Recommendation can be made by users to other users. All the posted questions can be answered by anyone within the field area. When a user connects with professionals and companies, they can send private message to each other. Posting pictures and videos on Bayt is not permitted. The only post that can be acceptable is in text type. These posts could be extracted from the web browsers used, Swap file, RAM, and unallocated space. When a company or industry publish a new job, they publish all the requirements and objectives of the job, and users can view everything on a particular job including the salary, and then apply for the job if they are interested. The company can then access the users profile page and view their CV. If the company is interested in a particular user then they contact them via private messages. The homepage layout in Bayt is called (My Workspace). Figure 4.5 shows the Workspace of Bayt.

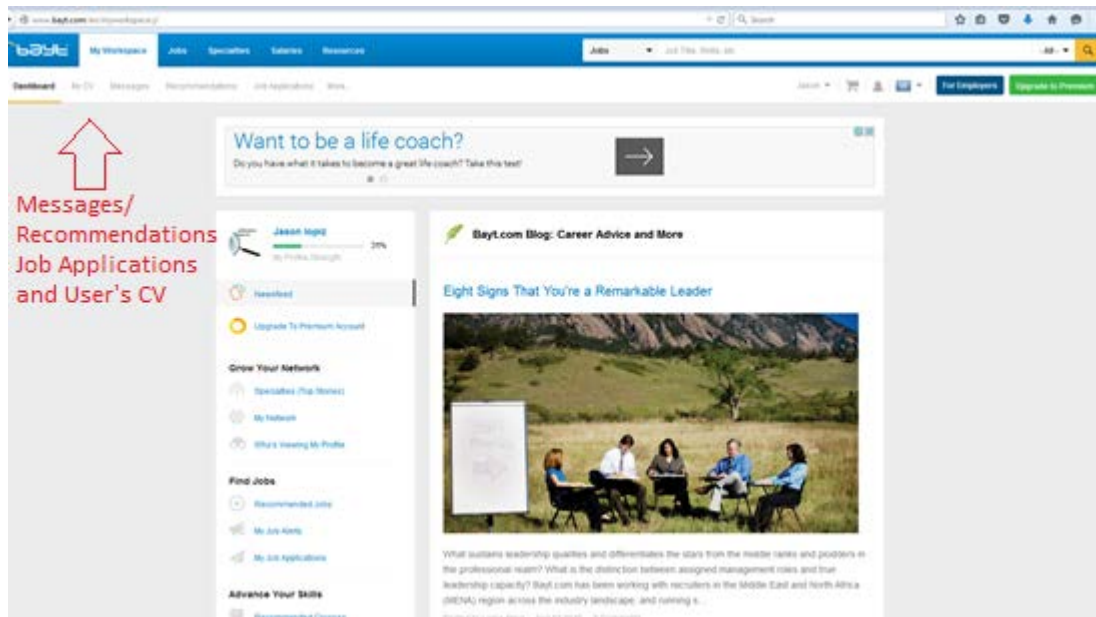


Figure 4.5: Bayt Homepage Layout

4.2.6 Findings of Preliminary Test

The previous sections discussed the types of data that can be posted on five OSNSs, along with the way it is posted, and the possible sources that it can be stored in. This section reports the findings of the preliminary investigation and determines what evidence will be used in the experiments. Since there are three browsers that will be used for posting on each OSNS, three separate tables for each browser are created in each controlled data and test plan, with the same type of posts which are summarized in Table 4.2.

Table 4.2: Types of Data Used in the Experiments

Social Network	Types of Post Used
Facebook	1. Texts post on profile page (timeline)
	2. Upload a pictures
	3. Post on Friend's Wall
	4. Private Messaging with Friend (Instant messaging)
	5. Post videos
	6. View shared Instagram pictures on Facebook
	7. View the pictures on Instagram website
Twitter	1. Text posts on home page (Tweet)
	2. Upload a pictures
	3. Tweets on friend's wall
	4. Direct messaging with friend
	5. View shared Instagram pictures on Twitter
	6. View the pictures on Instagram website
	7. Retweet posts

Social Network	Types of Post Used
LinkedIn	1. Status text posts on homepage
	2. Upload pictures on LinkedIn
	3. Post comments on the uploaded pictures
	4. Like the pictures
	5. Send private messages to a friend
Bayt	1. Post questions as evidence on Bayt
	2. Post recommendation
	3. Answer posted questions
	4. Send private messages to a friend

Instagram is embedded with Facebook and Twitter. Hence, there are no separate test scenarios for Instagram, because it will be used for only sharing picture links on both Facebook and Twitter. Since Instagram does not permit posting using Desktop based PCs, then it is posted through a Samsung mobile, and then shared on Facebook and Twitter. During the simulation of data, the shared links are accessed and viewed from the three browsers on Facebook, Twitter, and the Instagram website.

There are several other activities and features that can be performed on each OSNS as shown in previous sections; these activities such as creating groups and Hashtags were not performed in order to narrow down the scope of the tests, and due to time limitations.

4.2.7 Online Social Networks: Environments Setup & Case Scenarios

In Section 4.2.6 the types of activities used in the experiment were outlined. In this section the software and hardware used on the suspect's machine, the controlled data, and the developed case scenarios for the experiment are reported.

There was only one laptop equipped with Wi-Fi which acts as the target's machine to be examined. The laptop was a TOSHIBA Centrino Intel® Core™ Duo CPU T7100, 1.80GHz with 2 GB of installed memory (RAM), and 160 GB hard drive. The target computer has a small RAM, which will be examined along with HD. Two case scenarios have been developed, the first case scenario involves Facebook, Twitter, and Instagram, and the second case scenario involves LinkedIn and Bayt. The target computer is first wiped with Darik's Boot and Nuke tool version 2.2.8 (DBAN), to ensure any previous data is completely removed by zeroing the hard drive. After zeroing the laptop, it is equipped with Windows 7 professional 32-bit Operating System with service pack 1. A new user with full administration privileges is created, and then the latest version of the three selected browsers were installed. After

installation of the web browsers, they were checked for the standard out of the box configurations, and confirmed that each browser was installed in their own native format and location. They store website access information on their own browser's file history, Cache, and cookies by default. There were no changes or modifications made to browsers file locations, by either installing additional plugins, or extensions. This method seeks to generalize the experience that any user may have when accessing the selected five OSNSs with the three selected browsers. Table 4.3 shows the browsers and the versions installed on the suspect's machine.

Table 4.3: Detailed Web Browsers and Versions Used in the Experiment

Browser Type	Browser Version	Description
Microsoft Internet Explorer (IE)	Ver. 11.0	The latest version released for IE at the time of conducting the experiment
Mozilla Firefox	Ver. 38.0.5	The latest version released for Firefox at the time of conducting the experiment
Google Chrome	Ver. 44.0	The latest version released for Chrome at the time of conducting the experiment

The case scenarios are then developed; first case scenario involves a public threat where the suspect is using Facebook, Twitter and Instagram, and law enforcement acts accordingly for digital forensic investigation. The Second case scenario is performed on LinkedIn and Bayt and is associated with an internal policy breach in a company, and the forensic team conducts an internal investigation. The case scenarios are introduced in the next Sections in 4.2.7.1 and 4.2.7.2. To conduct the investigations, a simulation of data is posted on each of the five OSNSs (Controlled data). Accounts for Instagram, Facebook, and Twitter were previously created with the name Smith Volkov, who plays as the suspect in first case scenario, then the same type of evidence and the way of posting were generated on each selected browser. The data is documented and labelled in a form of tables, as shown in Appendix 1, where there are six tables. The first table involves Facebook and Instagram posts on Firefox on the target's computer. Each table is documented with Event number and Date/Time specified for each post performed. The second and third tables are for Google Chrome and IE. The fourth table is the controlled data posted on Twitter and Instagram on Firefox and so on for the other two browsers. Appendix 2 shows the controlled data for the second case scenario, which is similar to the previous tables but involves LinkedIn and Bayt activities performed by Jason Lopiz who plays as the employee

who breached the company's policy. After finishing with acquisition and imaging of the HD in the first case scenario, the same steps were taken for wiping the HD using DBAN to install the same versions of the browsers. New accounts for Jason on LinkedIn and Bayt was previously created in order to simulate the data. The following sub sections show the two case scenarios developed for posting the data on the selected OSNSs.

4.2.7.1 First Case Scenario (Public Threat)

A person named Smith Volkov used his personal social networking sites pages to post information about him and social updates. Smith Volkov has one friend on his friend list. The suspect used Facebook website to communicate with his friend, commenting and posting on friend's wall page, uploading pictures and videos. Smith also used Twitter to post tweets and pictures, he also shares his Instagram pictures to Twitter and Facebook. The Instagram pictures are shared with links to the pictures which can be accessed via the PC.

Smith has recently posted a threat message to the society. However, he forgot to disable the post location of the message. He also did not make the post private; this means that the post can be viewed by anyone who accesses his page. A Police department has received a call from a concerned citizen and notified them of this post. The law enforcement agency has identified the location of the threat posted on Smith's page, and a search warrant was obtained for examining the laptop which is identified in the place. The laptop was powered on, and was running when law enforcement seized it. A memory dump has been captured by a law enforcement officer, and then the power cord is pulled from the running system. The suspect's hard drive is seized, and sent to the forensic laboratory for further examination to finding any evidence that this laptop was used for posting threats in OSNSs.

4.2.7.2 Second Case Scenario (Policy Breach)

Gold-Star is an oil company that exports oil to several countries. The company has more than 2000 employees. Jason Lopez is one of the people who accepted an offer to work as a sales team member in the company. The company has very strict policies regarding the use of internet during working hours; another policy implemented by the company is regarding the use of OSNSs, which addresses that no one is allowed to use any OSNS using the company's network.

Recently, the company has conducted a security audit on all the computers and communication devices owned or operated by the company, the purpose of this audit is to ensure integrity, confidentiality and availability of resources and information, to investigate for any possible security incidents, and to make sure that all policies are properly implemented and followed by their employees. Any violation of the policies may be subject to disciplinary actions.

During the security audit, the auditors have found Jason's laptop powered on, and logged in to LinkedIn, and Bayt. Jason quickly logged off and closed his browser. In response, the security audit team has reported the incident while they are talking to Jason regarding the incident. Jason has denied that he used any OSNS, and he asked for exculpation. The audit team leader has requested a further investigation of the incident, and decided to seize Jason's laptop after capturing a memory dump and brought it to the forensic lab for further examination.

4.2.8 Conclusion

Section 4.2 discussed the selected OSNSs to be examined in the experiment, and illustrated the types of post each OSNS allows within the site, along with how these posts can be posted. Findings of the preliminary test describes what will be posted on each OSNS for the testing environment which is summarized in Table 4.2. The environment setups for the target machine to be examined were explained, and the case scenarios have been illustrated along with the controlled data, which will be used later stages for comparative analysis. This section has analysed and completes the first phase of the experiment. The following sections proceeds with the second phase in the proposed research phases.

4.3 FIRST CASE SCENARIO - PUBLIC THREAT

The first case scenario involves a public threat where a suspect named Smith Volkov is using the Facebook, Twitter, and Instagram to perform different activities as listed in table 4.2. The objective of this investigation is to preserve, collect, examine and analyse any possible evidence that can be found on the suspect's RAM, pagefile.sys, and the hard drive, by using three digital forensic tools namely Belkasoft Evidence Center, Internet Examiner Toolkit, and Internet Evidence Finder. It is expected that most of the activities (in Table 4.2) performed on the three OSNSs using the three browsers can be extracted.

As proposed in phase 2 of the research phases, test plans and test scenarios have been developed for the first and second case scenarios. The test plans were developed and documented based on the SWGDE approach for validating testing of tools. Each test plan describes the purpose, scope, requirements, methodology, and the test scenarios. There are 12 test plans developed for the whole thesis. Each digital forensic tool has four distinct test plans (Two for the first case scenario and two for the second case scenario). For The first Case Scenario: The first test plan in Appendix 7 (Test plan 1) is analysis of RAM using Belkasoft evidence Center. Appendix 8 (Test plan 2) is analysis of the HD using the same tool. Appendix 19 (Test plan 5) is the analysis of RAM using Internet Examiner Toolkit. Appendix 20 (Test plan 6) is analysis of the HD using the same tool. Appendix 25 (Test Plan 9) is analysis of RAM using Internet Evidence Finder, and finally Appendix 26 (Test plan 10) is analysis of the HD using the same tool. Each of these test plans have six distinct tables (test scenarios). The first three tables (test scenarios) are for Facebook and Instagram with Firefox, Chrome, and IE. The second three tables are for Twitter and Instagram with Firefox, Chrome, and IE and so on for every test plan. The other six test plans were developed for the second case scenario which will be discussed in Section 4.4.

4.3.1 Forensic Investigation Environment Setup

The environment setup for the suspect's computer has been described in Section 4.2.7, which includes the detailed software and hardware that are used for the suspect's machine, and details of the installed browsers and their versions. The suspect's machine has been selected according to the resources that were available at the time of conducting the testing experiments. This section discusses the forensic investigation environment and the prepared software and hardware for the testing.

The investigator machine is equipped with Intel® Ethernet Connection I217-LM, and located in the controlled lab environment. This machine is HP Intel® Core™ i5-4570 CPU @ 3.20 GHz 3.20 GHz with 16.0 GB of Installed memory (RAM), and 400 GB of HD. The machine is equipped with Windows 7 Enterprise OS with Service Pack 1. The prepared Hardware and software installed on the investigator's machine for testing is displayed in Table 4.4.

Table 4.4: Detailed Hardware and Software Specifications

Hardware / Software	Version / Model	Purpose
FTK imager Lite	Version: 3.1.1	Used for acquiring memory (RAM), and pagefile.sys of the suspect's computer
Tableau Imager	Version: 1.11	To image the computer's hard with the use of tableau eSATA forensic bridge
Tableau eSATA forensic bridge	Model: T35es	A forensic SATA/IDE bridge is used to acquire computer HD in forensic manner where the evidence is not altered or changed
AccessData® FTK® Imager	Version: 2.9.0.138	used for creating an image of memory dump and the acquired hard drives and to verify the integrity of the image by calculating MD5 and SHA1 values
WD Elements External Hard drive	2 TB size storage compatible with USB3.0	An external Hard drive Formatted with NTFS file system, the external HD is used for storing the image files of the evidence after verifications
Antistatic Wrist Strap	Manufacturer: POSH	Used for proper handling of HD when it is taken off from the laptop, and to prevent any electrostatic discharge (ESD)
Antistatic Bag	Size: 6 in. x 8 in.	Antistatic security bag is used for bagging the suspect's HD during the transfer to different places and storage of HD after acquisition
Belkasoft Evidence Center	Version: 7.2.1036	Used for analysing OSNSs evidence from the suspect's computer
Internet Examiner Toolkit	Version: 5.12.1507.2818	Used for analysing OSNSs evidence from the suspect's computer
Internet Evidence Finder	Version: 6.7.0.0447	Used for analysing OSNSs evidence from the suspect's computer

4.3.2 Digital Forensics

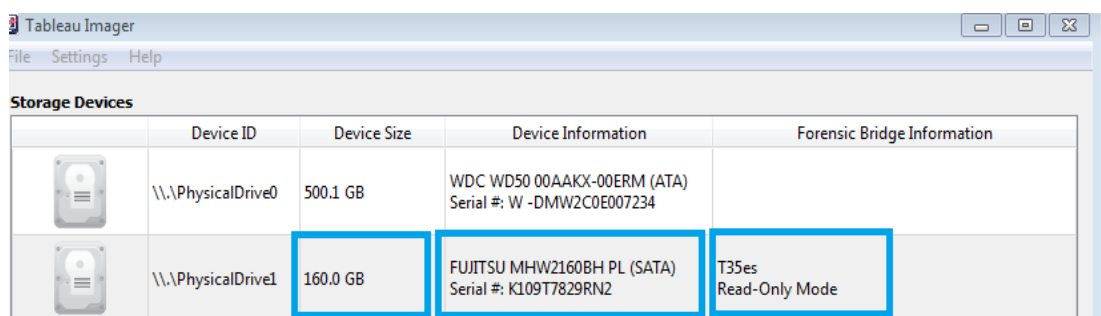
After setting up the environment for the suspect's computer, and the controlled data is posted on the three OSNSs as discussed in Section 4.2.7. Developing test plans for the first case scenario, and setting up the forensic investigation environment is discussed in Section 4.3.1. Phase 3 and 4 of the proposed research phases is conducted using the adopted computer forensic guidelines methodology by Noureldin, Hashem and Abdalla (2011). This methodology has six stages as discussed in Section 3.1.1 which are: Evaluation and Assessment, Acquisition of Evidence, Survey of digital scene, Examination of digital evidence, data reconstruction, and conclusion. The following sub sections analyse each of these phases conducted for the first case scenario.

4.3.2.1 Evaluation and Assessment

The suspect's laptop was powered on when the investigator arrived at the scene for seizure. Then the memory was dumped and pagefile.sys was acquired using FTK Imager Lite, and saved as Pagefile.sys, memdump.mem. After the acquisition of RAM and pagefile.sys, the laptop then was seized by pulling the power cord from the running laptop, and sent to forensic laboratory. The suspect's HD then was taken out of the seized laptop for acquisition, with the use of an Antistatic Wrist Strap to prevent electrostatic discharge (ESD).

4.3.2.2 Acquisition of Evidence

The suspect's HD was acquired using Tableau Imager, and Tableau eSATA forensic bridge. The hard drive is a Fujitsu SATA hard disk drive, Model: MHW2160BH PL. The hard drive Serial Number is: K109T7829RN2, with a storage space of: 160 gigabytes (GB). The RAM memory dump file was acquired using FTK imager lite by the forensic investigator is imaged in order to verify the integrity of the evidence. FTK imager is used to image the acquired RAM bit by bit. The results of this process produces an image type Raw (dd) file which is saved as test1_Livememory_suspect.001. The RAM image is an exact duplicate copy of the acquired memdump.mem initially acquired, the integrity of this image is verified with MD5 Checksum and SHA1 hash values (Appendix 3). The suspect's HD was connected with Tableau eSATA forensic bridge before performing the acquisition. This practice is crucial for the digital forensic investigation in order to prevent any miss handling, or alteration to the data stored in the HD. The tableau Imager is used to acquire the HD in read only mode which confirms that the HD is connected through the use of a write blocker as shown in Figure 4.6.





	Device ID	Device Size	Device Information	Forensic Bridge Information
	\\.\PhysicalDrive0	500.1 GB	WDC WD50 00AAKX-00ERM (ATA) Serial #: W -DMW2C0E007234	
	\\.\PhysicalDrive1	160.0 GB	FUJITSU MHW2160BH PL (SATA) Serial #: K109T7829RN2	T35es Read-Only Mode

Figure 4.6: HD Acquisition Using Tableau Imager & eSATA Forensic Bridge

The connection of eSATA forensic bridge with HD, and with the forensic investigator's PC is performed by applying the guidelines given in the Ultra block user guide. After a successful acquisition of the suspect's HD, it was imaged using FTK imager for the purpose of integrity validation, the image is validated by verifying MD5 and SHA hash values (Appendix 4), and saved as IMAGE-suspect1-harddrive.E01. The hard drive acquisition, and verification is depicted in Figure 4.7. The original files of the suspect's RAM and HD were kept in a safe place along with the physical hard drive.

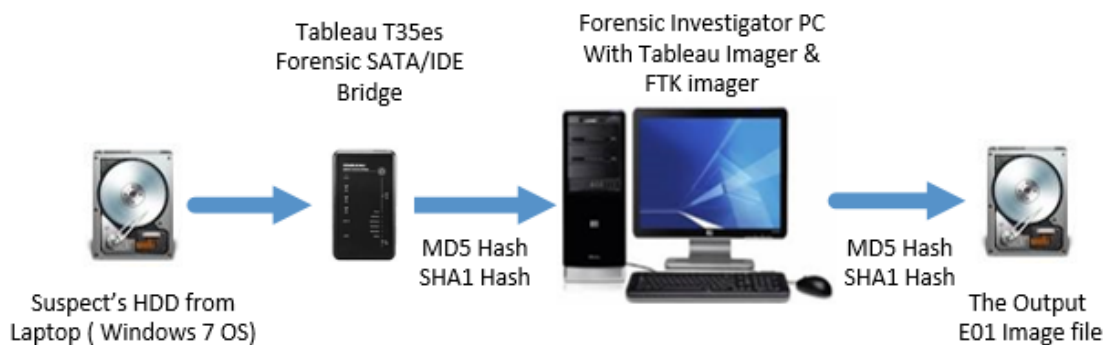


Figure 4.7: HD Acquisition & Verification Process

4.3.2.3 Survey of Digital Scene

This step is crucial in order to evaluate the suspect's skill level in technology. The imaged HD in the previous section is mounted in AccessData FTK imager via performing Mount Image to drive, with Block Device / Read only method mode. Examinations of obvious locations for evidence was conducted, and searching for passwords if stored, completed. Browser files indicated the types of browsers the suspect was using which were IE, Firefox, and Chrome. According to the evaluation, there were no indications that a destructive process was performed on the computer data storage, and encryption of contents to secure data had not been performed on any files. For Users accounts, there was an account named (admin) which was confirmed to be the username that was used for posting threats on the three OSNSs. I:\Users\admin\AppData was found during examination and it was not deleted by the suspect. The recorded date modified on the files is 15/6/2015, which is the same date the simulation of data was performed for this case scenario (Appendix 1).

4.3.2.4 Digital Evidence Examination

Once the suspect's skill is evaluated, the evidence files (RAM, pagefile.sys, and HD) were entered to the three digital forensic tools for evidence processing and data

extractions. Two cases have been created in each of the three digital forensic tools. The first case examines RAM, and pagefile.sys, and the second case examines the HD evidence file. This process is important in order to evaluate the source of evidence, as some evidence may be found on both cases (from RAM & HD), otherwise it may not be found at all. After adding the evidence files to each case they were checked using Belkasoft Evidence Center, and validated that the image hash value calculated by Belkasoft matches the hash value of the image verified by FTK imager. Figure 4.8 Shows the MD5 calculation of the RAM image, which is exactly the same MD5 hash created by FTK imager in Appendix 3. Note: Belkasoft does not support SHA1 for hash calculations.

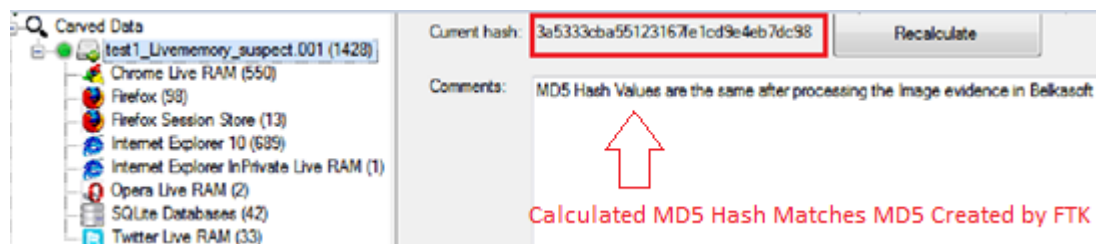


Figure 4.8: RAM Processed and MD5 Calculation & Verification

Since all of the three tools were installed as trial versions with time limitation (30 days trial), the analysis has been made tool by tool. This means that the Belkasoft examination is conducted on this case scenario, and the second case scenario (LinkedIn and Bayt) which will be discussed in Section 4.4. The second digital forensic tool IXTK is installed and the exact process is made for both case scenarios, and then IEF. The remaining of this section is the examination of each tools capabilities in finding evidence from different sources (RAM, Pagefile.sys, and HD).

Once the hash values has been verified, and data carving has been performed, by selecting the data type to be carved (i.e. P2P, Browsers, Instant Messengers Live RAM, Twitter, Facebook etc.), the examination and searching for evidence has been conducted on test plan one for RAM analysis (Appendix 7), and test plan two for hard drive analysis (Appendix 8). When a particular evidence is found, then it is recorded in the test scenario that belongs to. For example, when finding an image posted on Facebook using Firefox, then it is recorded in a Firefox table in Appendix 7, if the source was from RAM or pagefile.sys. Otherwise in Appendix 8 if it's from HD, and it identifies each evidence in test scenario if it is Pass or Fail. Figure 4.9 illustrates the percentage number of evidence extracted using Belkasoft Evidence Center from the suspect's RAM, pagefile.sys and hard drive.

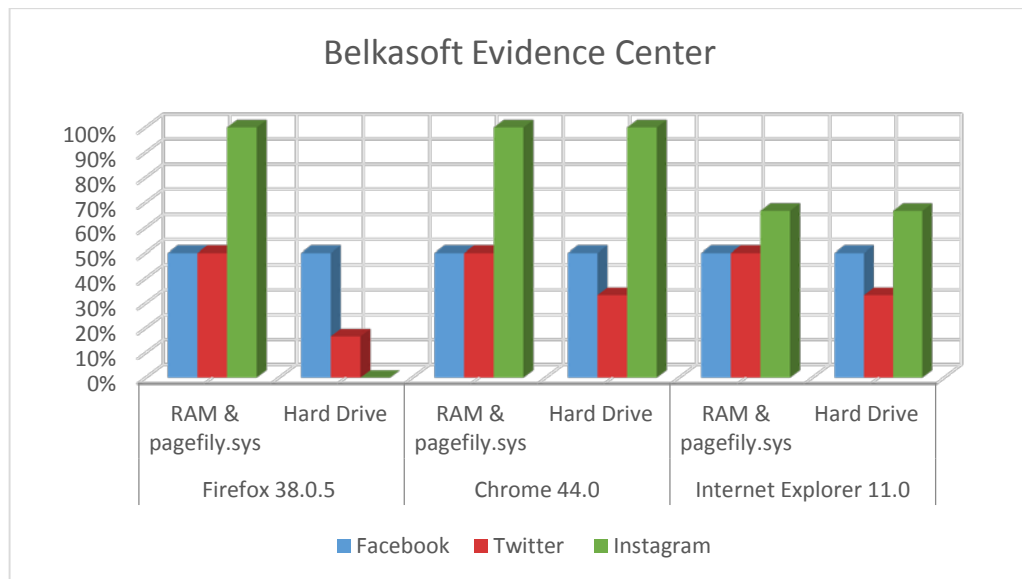


Figure 4.9: Evidence Extracted Using Belkasoft Evidence Center

The total percentage listed above is the total number of evidence items found for each OSNS on the three selected browsers. Belkasoft is powerful in finding most of the shared and viewed Instagram links with an average of 72% of the performed activities, and exactly half of the performed activities in Facebook were recovered from both RAM and HD. However, Twitter was the least number of items with an average of 39% of the performed activities recovered. When comparing the three browsers, the average number of evidence items recovered from Facebook, Twitter, and Instagram using Firefox is 44%, and 64% of average the number of evidence items using Chrome, and 53% for IE.

Internet Examiner Toolkit (IXTK) cannot run directly on the acquired forensic images format .001 for RAM and .E01 for the HD. These image files have to be mounted as a virtual drive, and no additional software was needed to mount the images, as there is a built-in disk options which enabled the investigator to mount the image in forensic manner. Internet Examiner Toolkit has the lowest percentage recovered from both RAM and HD for all the three OSNSs. For IXTK the same image was analysed for RAM is presented in test plan 5 (Appendix 19), and for the HD analysis is in test plan 6 (Appendix 20). The following Figure 4.10 shows the percentage of forensic evidence extracted using IXTK from the suspect's RAM, Pagefile.sys, and HD.

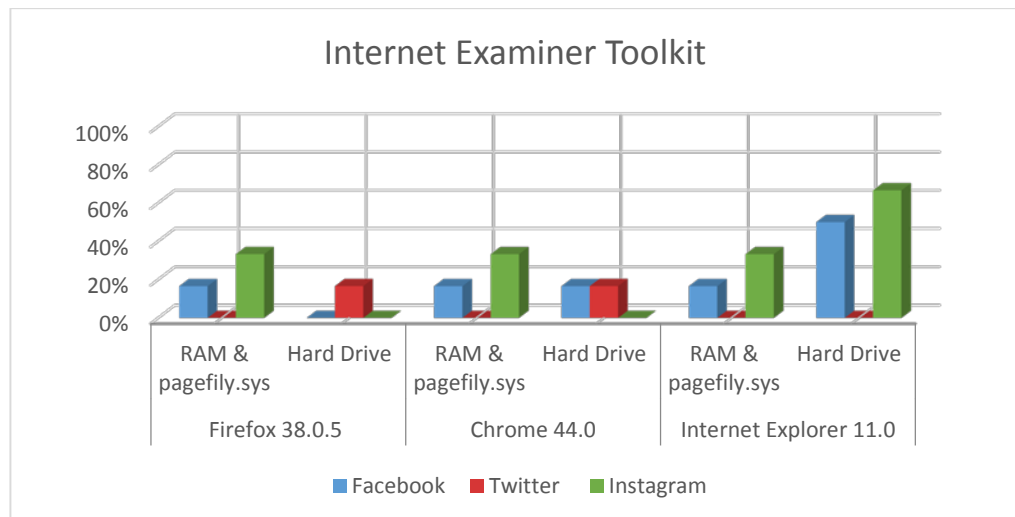


Figure 4.10: Evidence Extracted Using Internet Examiner Toolkit

Figure 4.10 shows that most of the activities performed on all three OSNs were not recovered. Especially for Firefox and Chrome. This is due the fact that IXTK does not intend to recover “trace artefacts” (fragments) and “keyword artefacts from Firefox and Chrome. According to Siquet Technical support, “this is because Firefox and Chrome use proprietary binary layouts to manage “cache” and SQLite databases for their history, and it is unwise to attempt to carve Chrome or Firefox artefacts from Unallocated Space (or disk sectors). Internet Explorer on the other hand has succinct “blocks” of data that can be accurately recovered as a trace artefact”. However, in the actual experiment, some of the Firefox, and Chrome activities were recovered, but the source of evidence was incorrectly presented in IE Temporary Internet Files, or WebCacheV01.dat which is an IE file to store cached activities.

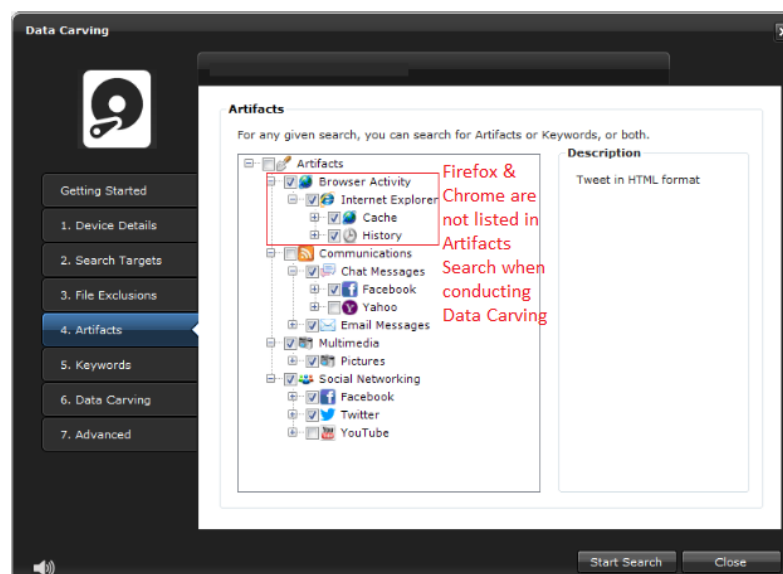


Figure 4.11: Data Carving in IXTK

Figure 4.11 shows that IE is the only browser activity that can be selected to be searched via data carving, and reading in a desk sector level. On average, only 19% of Facebook activities performed were recovered by IXTK and 6% of Twitter activities, and 28% for Instagram activieis which are the lowest compared to the other two forensic tools. When comparing browsers, the average number of evidence extracted from all three OSNSs using Firefox is 11%, and 14% for Chrome. Internet explorer artefacts can be recovered more easily than the other two browsers in IXTK, as the average of recovered evidence from all the three OSNSs is 28%.

The RAM and HD evidence files processed in the previous two tools are also entered on the third tool Internet Evidence Finder (IEF). Figure 4.12 shows the percentage of forensic evidence extracted from the three OSNSs, using IEF from the suspect's RAM, Pagefile.sys, and hard drive.

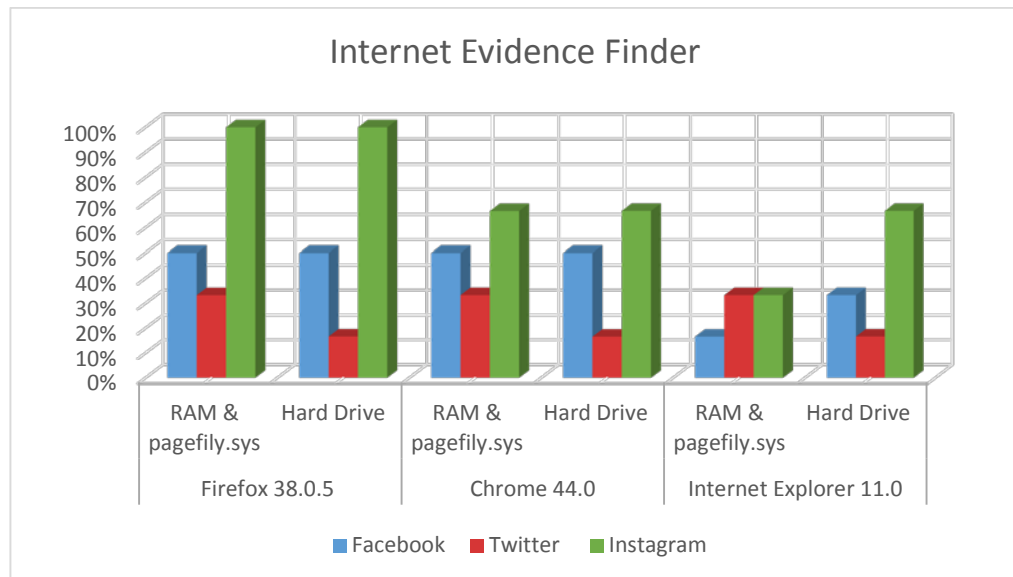


Figure 4.12: Evidence Extracted Using Internet Evidence Finder

Internet Evidence Finder RAM analysis is presented in test plan 9 (Appendix 25), and for hard drive analysis is presented in Test plan 10 (Appendix 26). Figure 4.12 shows that IEF and Belkasoft Evidence Center has the same average percentage of finding evidence on Instagram. IEF recovered an average of 42% of the activities performed on Facebook and 25% for Twitter activities. When comparing browsers, the average number of evidence collected from all the OSNSs when Firefox was used is 58%, and for Chrome is 47%, and 33% is the average of collected evidence items when IE is used.

This section has reported the number of evidence (controlled data) items recovered from each OSNS when using three digital forensic tools. The following

section will discuss the types of recovered evidence (i.e. texts posts, pictures, private message, videos) from each digital forensic tool, along with the source of which they were stored in (e.g. web History, browsers cache, sessions), in order to understand what sort of evidence each tool is capable of recovering, and to finally conduct a comparative analysis as proposed in Chapter 3.

4.3.2.5 Reconstruction of Extracted Data

The extracted data from each digital forensic tool in the previous section is reconstructed in order to draw a conclusion on whether the suspect Smith Volkov committed the threat crime using the laptop or not. For Facebook activities, it is confirmed that none of the three tools is able to extract Facebook wall posts made using the three browsers, and none of the posts on friend's wall were recovered. Uploading Pictures on Facebook however were one of the most recovered evidence items from the three tools. Belkasoft recovered all the posted pictures using three browsers from both RAM & HD. The Facebook uploaded picture URL looks as follow:

“<https://www.facebook.com/photo.php?fbid=107389486266838&set=a.106187259720394.1073741827.100009873604315&type=1&theate>”

A Facebook user ID is noticed at the end of the link (100009873604315), and fbid=107389486266838 is the unique ID of the uploaded picture. Internet Examiner on the other hand only recovered the uploaded picture using Internet Explorer from the suspect's HD, the picture is stored in the Temporary Internet Files. Internet Evidence finder recovered all the uploaded pictures from RAM and HD, except the uploaded picture using IE which is only recovered from the Temporary Internet Files. Belkasoft Evidence Center, IXTK, and IEF partially recovered instant messages conducted on Firefox and Chrome from the pagefile.sys. Figure 4.13 shows the recovered messages from Belkasoft. There were only two Facebook chats recovered in Belkasoft, The first line is the message received when the suspect's was using Firefox, the message was the last message received to the suspect's before closing Firefox, and it shows the time the message was received which is exactly the same time and date recorded in controlled data in Appendix 1. The second message was received by the suspect when using Chrome and it also shows the exact date and time which is recorded in the controlled data. Belkasoft enable the investigator to review message metadata from Hex Viewer, it includes Sender ID, Receiver ID, The message

being sent/Received in plaintext, timestamp of the message including Date/Time. Additional Information were also presented in the Hex which identifies a relationship between the two users as shown in the following hex code the full name, employment status, Vanity URL name, and gender which is classified male =1, female=2.

```

"__=1445656050_d4b2ad43d4d123f92b26d1e22512d297", "name": "Hanan
Alsalem", "short_name": "Hanan", "employee": false, "is_employee_away": false,
"networks": [], "type": "user", "vanity": "hanan.alsalem.58", "is_friend": true, "social_snippets": [], "is_messenger_user": true, { "fbid": 100009873604315, "gender": 2, "href": "https://www.facebook.com/profile.php?id=100009873604"

```

There were other messages sent and received using the three browsers, but they were not found. Thus, in the test plan 1 it is marked as (Fail).

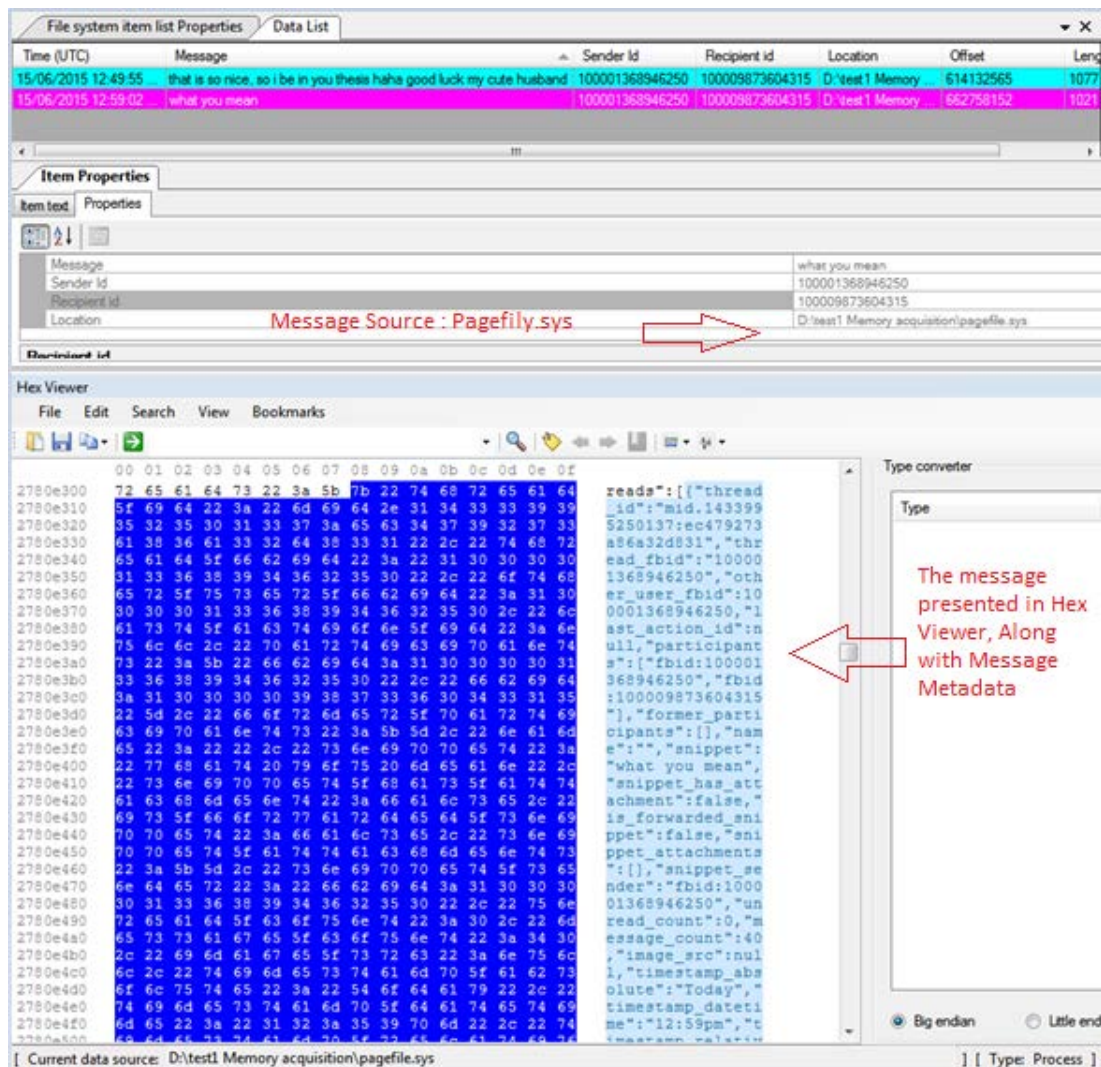


Figure 4.13: Evidence for Facebook Chats Extracted in Belkasoft

Similarly to IXTK which extracted the same messages recovered in Belkasoft. Figure 4.14 and Figure 4.15 show the messages received when the suspect was using Firefox,

and Chrome. IXTK also displays the message metadata in Hex Viewer, this includes the message in plaintext, Data/Time, Facebook ID, attachments to the message.

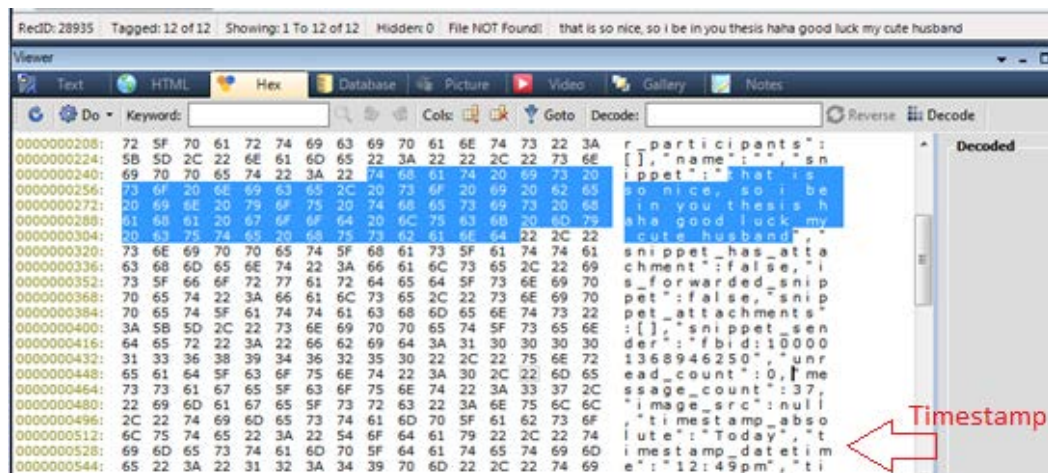


Figure 4.14: Facebook Chats Extracted in IXTK Received Using Firefox

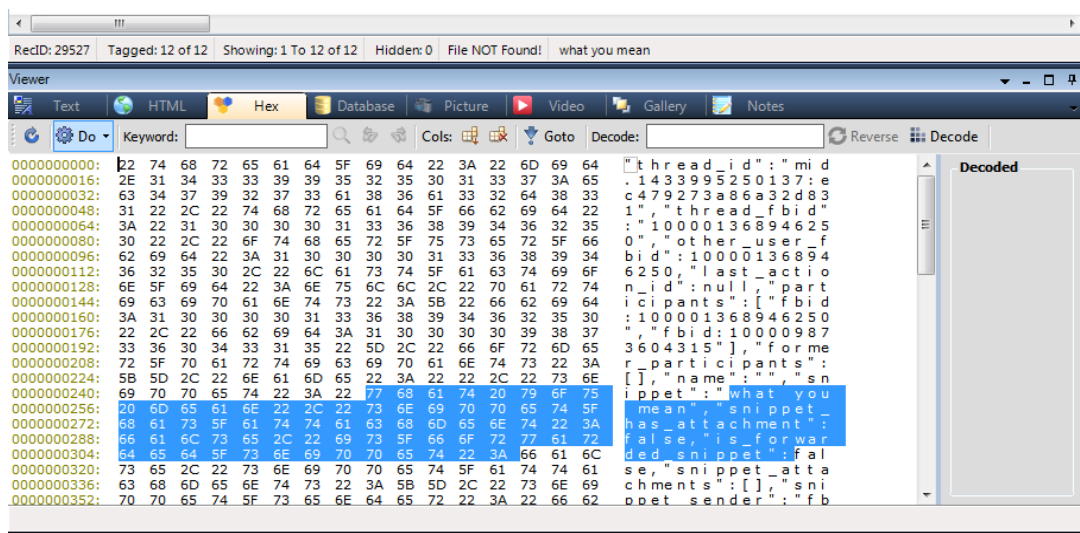


Figure 4.15: Facebook Chats Extracted in IXTK Received Using Chrome

Internet Evidence Finder has better capabilities in recovering Facebook messages than the other two tools, as it partially recovered the same messages from Chrome, and Firefox, but also recovered all the messages sent and received via Internet Explorer. The following Figure 4.16 illustrates the Sent/Received messages on IEF recovered from pagefile.sys. The uploaded videos using the three browsers were recovered from RAM and hard drive by Belkasoft. However IXTK recovered only two videos uploaded using Chrome and Internet Explorer from the suspect's HD. The two videos were stored in:

"I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files."

As discussed in Section 4.3.2.4, IXTK does not carve Chrome or Firefox artefacts, but when it recovers activities performed on these browsers, then it is stored in an IE cache, or history files. This issue may affect the admissibility of the evidence since the extracted evidence were not presented in the correct place by the digital forensic tool. Similar to Belkasoft, IEF recovered all the uploaded videos from RAM and HD, except the video uploaded using Internet Explorer was only recovered from the suspect's HD and found in:

“AppData\Local\Microsoft\Internet Explorer\Recovery\LastActive\{8871C2AB-12FD-11E5-B649-001B2498D131}.dat”

The Videos posted using Chrome were recovered from:

“AppData\Local\Google\Chrome\UserData\Default\Current Session”

Which is a more accurate source of evidence than the source presented in IXTK.

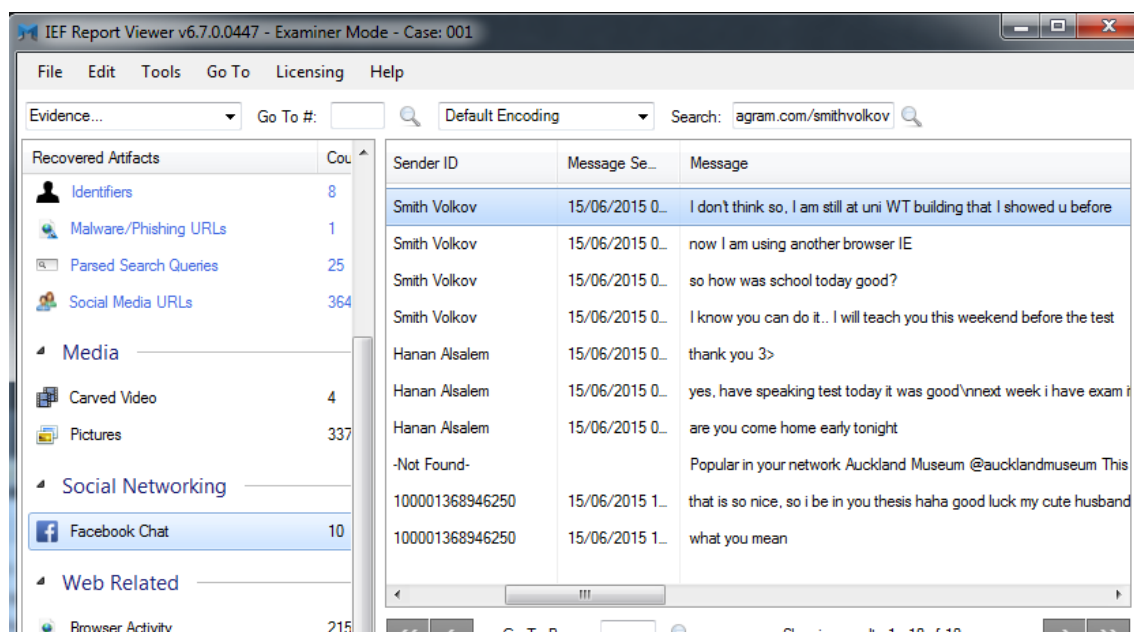


Figure 4.16: Facebook Chats Extracted by IEF

The shared Instagram pictures on Facebook were recovered by Belkasoft on all browsers and from both RAM and HD. IXTK recovered the shared links from the suspect's RAM for the three browsers, and only the shared link using Internet Explorer was recovered from the suspect's HD and it is stored in:

“I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files”

IEF was able to recover the shared links accessed using Firefox and Chrome from both sources RAM and HD. There were no evidence items of the shared links accessed using Internet Explorer.

4.18 shows the evidence found from the second case in Belkasoft for examining the suspect's HD. The Belkasoft report is generated in Appendix 13 which comprehensively illustrates where each evidence item is found and the times and date of accessed which match the time and date each data posted on the controlled data in Appendix 1.

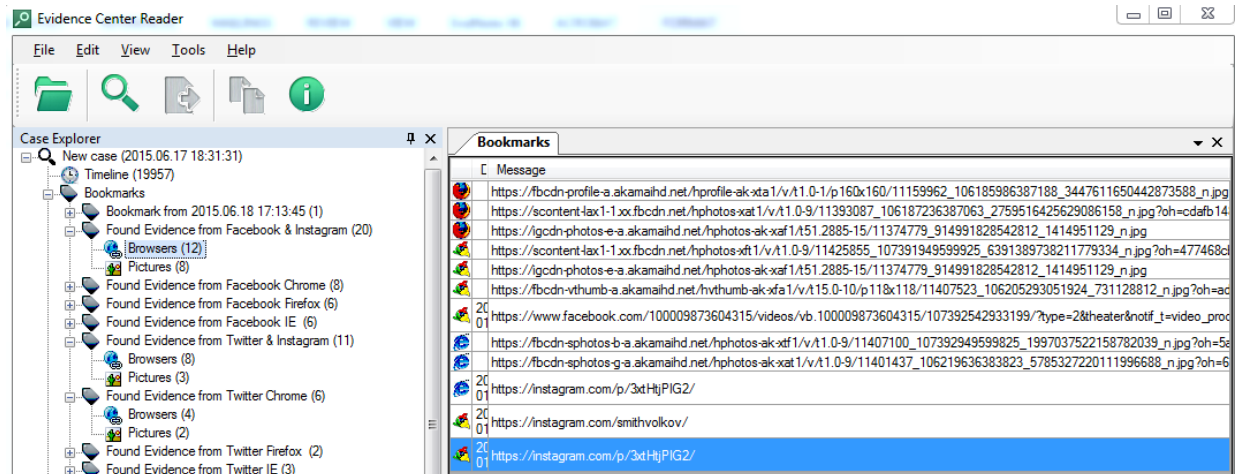


Figure 4.18: Evidence Found on Belkasoft for Facebook & Instagram (HD)

Belkasoft enables the investigator to search for data by typing a word or phrase; or words from a file, once the search for a word is executed. All the search results are listed in a form of data list. IXTK allows an investigator to write and apply SQL custom query statements in order to search artefacts from the carved records presented in the data pane. Appendix 35 summarizes the queries applied to IXTK. IEF has better searching capabilities than the other two tools, as a keyword searching is entered prior to data carving. During searching, the investigator is alerted when data matches a word entered in the keyword searching, by opening a (search alerts) popup interface.

For the evidence recovered using Internet Examiner Toolkit, the following Figure 4.19 illustrates all the evidence found when RAM is examined. In order to generate a report in IXTK an SQL query has to be executed. The following SQL query is executed in order to generate all the bookmarked data into one report:

```
SELECT Records.*, Bookmarks.BookmarkFolder_ID FROM Records INNER JOIN Bookmarks ON
Records.Record_ID = Bookmarks.Record_ID WHERE HideRecord = 0 AND
Bookmarks.BookmarkFolder_ID = 2
```

The generated report of the evidence is presented in Appendix 22.

Tag	Row	RecID	Located At	Url	Activity	Rec	File Category
<input checked="" type="checkbox"/>	6	517035	2,345,721	https://igcdn-photos-g-a.akamaihd.net/hphotos-ak-xaf1/1512885-15/11312502_845459245541990_1704121739_n.jpg	Recovered	URL	Pictures, Multime...
<input checked="" type="checkbox"/>	5	185348	2,620,449	https://igcdn-photos-g-a.akamaihd.net/hphotos-ak-xaf1/1512885-15/11312502_845459245541990_1704121739_n.jpg	Recovered	URL	Pictures, Multime...
<input checked="" type="checkbox"/>	4	176903	3,100,656	https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/1512885-15/11374779_914991828542812_1414951129_n.jpg	Recovered	URL	Pictures, Multime...
<input checked="" type="checkbox"/>	3	162335	3,906,566	https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/1512885-15/11374779_914991828542812_1414951129_n.jpg	Recovered	URL	Pictures, Multime...
<input checked="" type="checkbox"/>	2	146372	2,345,721	https://igcdn-photos-g-a.akamaihd.net/hphotos-ak-xaf1/1512885-15/11312502_845459245541990_1704121739_n.jpg	Recovered	URL	Pictures, Multime...
<input checked="" type="checkbox"/>	1	140779	3,964,507	https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/1512885-15/11374779_914991828542812_1414951129_n.jpg	Recovered	URL	Pictures, Multime...

Figure 4.19: Evidence Found for Facebook & Instagram & Twitter from RAM

The second case created in IXTK to examine the suspect's HD found lists of evidence as discussed previously for Facebook, and will be discussed next for Twitter. The following Figure 4.20 is the evidence reconstructed from the HD and the full report of evidence is listed in Appendix 23.

edID	Row	Artifact Icon	VIC	ParentID	Visi	Artifact Type	Subject	Uri
4893	01		5	0	0		I:\Users\admin\AppData\Local\Micro...	file:///I:\Users\admin\AppData\Local\Microsoft\Wind
7796	02		5	0	0	Cache	https://instagram.com/p/3xtHtjPIG2/	https://instagram.com/p/3xtHtjPIG2/
7771	03		5	0	0	Cache	https://twitter.com/smithvolko1/stat...	https://twitter.com/smithvolko1/status/61025512414
6001	04		5	0	0	History	https://instagram.com/p/3xtNkYPIHN/	https://instagram.com/p/3xtNkYPIHN/
6026	05		5	0	0	History	https://twitter.com/smithvolko1	https://twitter.com/smithvolko1
4838	06		5	0	0		I:\Users\admin\AppData\Local\Micro...	file:///I:\Users\admin\AppData\Local\Microsoft\Wind
4866	07		5	0	0		I:\Users\admin\AppData\Local\Micro...	file:///I:\Users\admin\AppData\Local\Microsoft\Wind
4867	08		5	0	0		I:\Users\admin\AppData\Local\Micro...	file:///I:\Users\admin\AppData\Local\Microsoft\Wind
4939	09		5	0	0		I:\Users\admin\AppData\Local\Micro...	file:///I:\Users\admin\AppData\Local\Microsoft\Wind
4946	10		5	0	0		I:\Users\admin\AppData\Local\Micro...	file:///I:\Users\admin\AppData\Local\Microsoft\Wind
28935	11		5	0	1	Message Snippet	that is so nice, so i be in you thesis h...	
29527	12		5	0	1	Message Snippet	what you mean	

Figure 4.20: Evidence Found for Facebook & Instagram & Twitter from HD

Internet Evidence Finder bookmarking process is slightly different to the previous two tools. The investigator cannot create a bookmark folder, but can directly add evidence to a bookmark list that is built based on the type of evidence. The following Figure 4.21 shows evidence reconstructed from the RAM. The evidence report is generated and listed in Appendix 29.

Facebook URLs:

★ #	URL
★ 5	https://www.facebook.com/photo.php?fbid=107391609599959&set=a.106225223049931.1073741828.100009873604315&type=1&theater
★ 8	https://www.facebook.com/profile.php?id=100009873604315
★ 11	https://www.facebook.com/photo.php?fbid=107389486266838&set=a.106187259720394.1073741827.100009873604315&type=1&theater
★ 18	https://www.facebook.com/100009873604315/videos/vb.100009873604315/107391359599984/?type=2&theater¬if_t=video_processed
★ 22	https://www.facebook.com/hanan.alsalem.58?fref=tl_fr_box&pnref=hc.friends
★ 43	https://www.facebook.com/messages/hanan.alsalem.58WdtR
★ 94	https://www.facebook.com/100009873604315/videos/vb.100009873604315/107392542933199/?type=2&theater¬if_t=video_processed
★ 98	https://www.facebook.com/photo.php?fbid=107391949599925&set=a.106187259720394.1073741827.100009873604315&type=1&theater
★ 1...	https://www.facebook.com/photo.php?fbid=106225229716597&set=a.106225223049931.1073741828.100009873604315&type=1&theater

Web Related: Chrome History:

★	#	URL	Last Visited Date/Ti...
★	29	https://instagram.com/p/3xtHtjPIG2/?taken-by=smithvolkov	15/06/2015 01:01:47 ..
★	30	https://instagram.com/smithvolkov/	15/06/2015 01:02:12 ..

Web Related Firefox Session Artefacts:

★	#	Title	URL
★	2	smithvolkov on Twitter: \"http://t.co/gXjQoLdhWq\"	https://twitter.com/smithvolko1/status/610253537465925632/photo/1
★	7	Instagram photo by Smith Volkov " Invalid date at Invalid date	https://instagram.com/p/3xtNkYPIHN/
★	10	Instagram	https://instagram.com/smithvolkov/
★	11	Instagram	https://instagram.com/p/3xtHtjPIG2/?taken-by=smithvolkov

Internet Explorer 10-11 Daily/Weekly History:

★	#	User	URL	Last Visited Date/Ti...	Source
★	9	admin	https://instagram.com/p/3xtHtjPIG2/	2015-06-15 13:09:25	test1_livememory_suspect1.001

Figure 4.21: Facebook & Instagram Evidence Reconstructed from RAM & pagefile.sys on IEF

The second Case Created in IEF is to examine the suspect's HD as performed in the previous two tools. The following Figure 4.22 is the evidence reconstructed, and the generated report is illustrated in Appendix 30.

Firefox Web History:

★	#	URL	Title	Last Visited ...	Source
★	33	https://instagram.com/p/3xtHtjPIG2/	Smith Volkov o...	15/06/2015 ..	IMAGE-suspect1-harddrive.E01
★	34	https://instagram.com/accounts/login/	Smith Volkov o...	15/06/2015 ..	IMAGE-suspect1-harddrive.E01
★	45	https://instagram.com/p/3xtNkYPIHN/	Instagram photo...	15/06/2015 ..	IMAGE-suspect1-harddrive.E01

Facebook Pictures:

Search:

Bookmarked Artefacts
Count

IEF Refined Results

Facebook URLs 7

Social Media URLs 2

Media

Facebook Pictures 1

Web Related

Chrome Cache Records 1

Chrome Web History 2

Firefox Web History 3

Internet Explorer 10-11 Main History 2

Details
Hex
Text

Potential Profile ID or Picture ID 107392949599825

Image

Browser: IE
website: Facebook
Picture Evidence

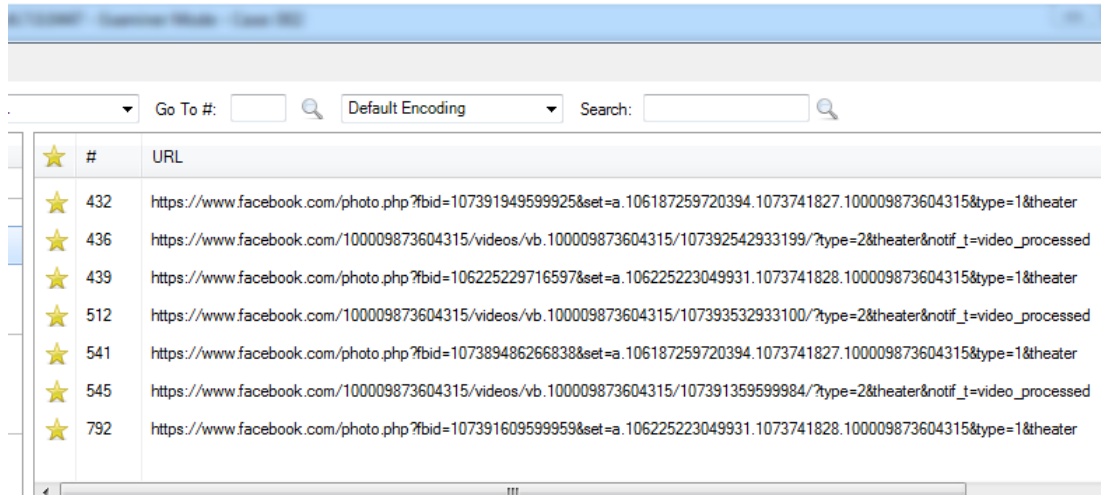
Chrome Web History:

★	#	URL	Last Visited Date/Ti...	Located At	Source
★	35	https://instagram.com/smithvolkov/	15/06/2015 01:02:12 ..	Table: urls(id: 35)	IMAGE-suspect1-hard...
★	36	https://instagram.com/p/3xtHtjPIG2/?taken-by=smithvolkov	15/06/2015 01:01:47 ..	Table: urls(id: 36)	IMAGE-suspect1-hard...

Internet Explorer History:

★	#	User	URL	Source
★	143	admin	https://instagram.com/p/3xtNkYPIHN/	IMAGE-suspect1-harddrive.E01 - _
★	212	admin	https://instagram.com/p/3xtHtjPIG2/	IMAGE-suspect1-harddrive.E01 - _

Facebook URLs:



The screenshot shows the Internet Explorer History window with a search bar at the top. Below the search bar, a list of history items is displayed. The first item is selected, showing a Facebook URL. The list includes several Facebook URLs, some of which are truncated.

★	#	URL
★	432	https://www.facebook.com/photo.php?fbid=107391949599925&set=a.106187259720394.1073741827.100009873604315&type=1&theater
★	436	https://www.facebook.com/100009873604315/videos/vb.100009873604315/107392542933199/?type=2&theater&notif_t=video_processed
★	439	https://www.facebook.com/photo.php?fbid=106225229716597&set=a.106225223049931.1073741828.100009873604315&type=1&theater
★	512	https://www.facebook.com/100009873604315/videos/vb.100009873604315/107393532933100/?type=2&theater&notif_t=video_processed
★	541	https://www.facebook.com/photo.php?fbid=107389486266838&set=a.106187259720394.1073741827.100009873604315&type=1&theater
★	545	https://www.facebook.com/100009873604315/videos/vb.100009873604315/107391359599984/?type=2&theater&notif_t=video_processed
★	792	https://www.facebook.com/photo.php?fbid=107391609599959&set=a.106225223049931.1073741828.100009873604315&type=1&theater

Figure 4.22: Facebook & Instagram Evidence Reconstructed from HD on IEF

For Twitter activities it is confirmed that none of the three digital forensic tools were able to extract any direct messages performed using the three browsers, nor find tweets on friend's wall. Belkasoft was able to extract all the status updates posted on Twitter (Tweets), from the three browsers. The source of the reconstructed tweets was the pagefile.sys. There were no encryption items in the links to the reconstructed tweets as it appeared in plain text in (Twitter Live RAM) in the data pane. The following Evidence is an example of the recovered Tweet performed by the suspect using Firefox.

*"lang="en" data-aria-label-part="0">Generate Ev. using Firefox, Tweeting in
Twitter is very nice; {Hint:Ev. Means Evidence}"*

Internet Evidence Finder was able to recover all the tweets performed on the three browsers from the suspect's RAM. The difference between Belkasoft and IEF is that IEF recovered the link to the tweet which can be accessed by clicking on the links, so it was not in plaintext like the recovered evidence in Belkasoft, The other difference is that Belkasoft was able to construct all the date/Time of each Tweet performed which is exactly same as the Date/Time performed listed in controlled data. IEF was not able to recover the times for the performed tweets. The following Evidence is an example of the recovered Tweets performed using Firefox. It is recovered from Social Media URLs: <https://twitter.com/smithvolko1/status/610253303985745920>

Both Belkasoft and IEF were able to extract all the uploaded pictures on Twitter from both sources: RAM, and HD. Internet Examiner was only able to extract the pictures uploaded using Firefox, and Chrome from the suspect's HD. The reconstructed pictures were incorrectly presented in IE Internet history file and cache, which is the same issue encountered during the reconstruction of Facebook Videos.

The shared Instagram picture on Twitter were only found by Belkasoft from the suspect's HD, and only the links accessed using Chrome, and Internet Explorer. The source of the accessed shared link on Chrome is stored in:

I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\f_000053

And source of the accessed shared link on IE is stored in:

I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T6GT6XA0\11312502_845459245541990_1704121739_n[1].jpg

Belkasoft was able to recover the viewed Instagram picture in Instagram website from RAM, and it was able to recover the viewed Instagram using Chrome and IE from the suspect's HD. Similarly IXTK recovered all the evidence from the RAM, but only the viewed pictures using Internet explorer were recovered from the suspect's HD, which was located at:

I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

Internet Evidence Finder was only able to recover the viewed picture using Firefox from both RAM and HD, and the viewed picture using IE from WebCacheV01.dat.

The last activity performed on Twitter was Retweet someone else's Tweet. This activity was only recovered by Belkasoft Evidence Center. The retweet was made using Firefox and extracted from the suspect's RAM. The retweets performed using Chrome and Internet Explorer were recovered from the pagefile.sys. IXTK and IEF failed to recover the suspect's Retweets. The Figure 4.23 shows the recovered Tweets, Retweets, and shared Instagram links, and the uploaded pictures on Twitter, from the suspect's RAM & Pagefile.sys when using Belkasoft. A detailed report of the evidence found from Twitter and Instagram from the suspect's RAM and pagefile.sys is generated from Belkasoft and presented in Appendix 12.

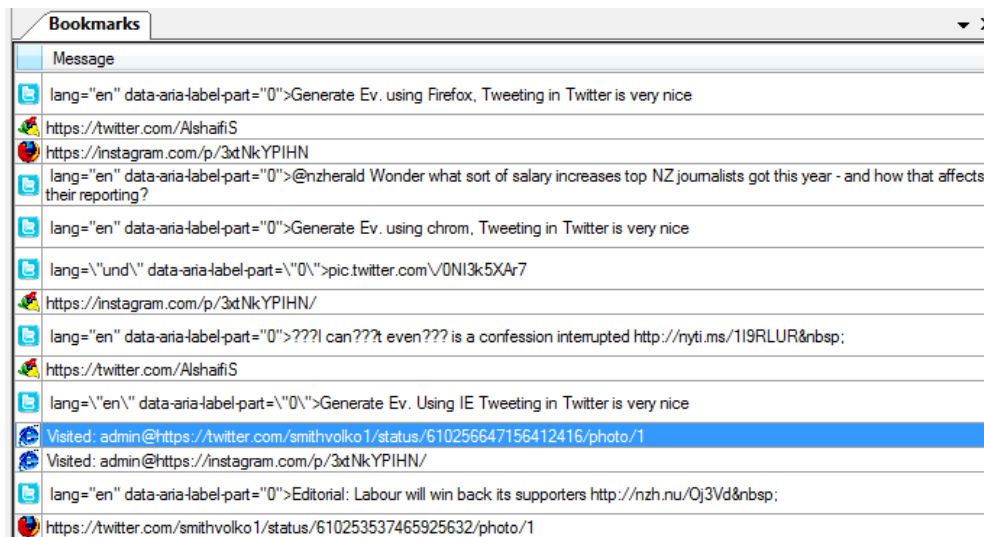


Figure 4.23: Evidence Found on Belkasoft for Twitter & Instagram (RAM & pagefile.sys)

Figure 4.24 shows Twitter and Instagram activities performed by the suspect, which was extracted from the hard drive.

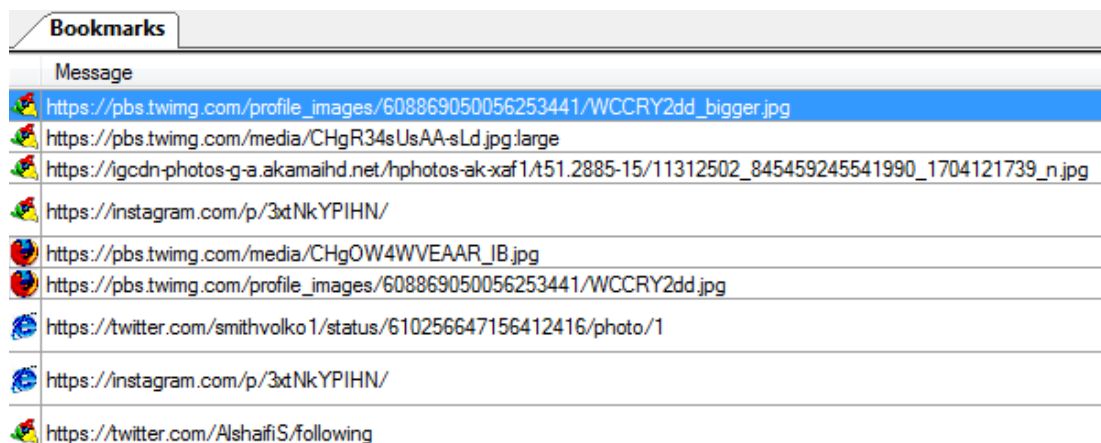


Figure 4.24: Evidence Found on Belkasoft for Twitter & Instagram (HD)

Since Belkasoft has better capabilities in bookmarking and reporting features, Reports of Evidence found from Twitter are separated from the report of Evidence found from Facebook. This is to ensure that there is no clashes or confusion during the analysis. The detailed evidence reconstructed in Figure 4.24 is presented in Appendix 14. The reconstructed Twitter Activities on IXTK are included in Figure 4.19 for RAM, and Figure 4.20 for HD. The following Figure 4.25 shows the reconstructed activities using IEF when examining the suspect's RAM, and a detailed report is presented in Appendix 29.

★	#	Site Name	URL
★	4	Twitter	https://twitter.com/smithvolko1/status/610253303985745920
★	47	Twitter	https://twitter.com/smithvolko1/status/610257403028738050/photo/1
★	255	Twitter	https://twitter.com/smithvolko1/status/608872265522909185
★	258	Twitter	https://twitter.com/smithvolko1/status/608876981673807873
★	167	Twitter	https://twitter.com/smithvolko1/status/610256647156412416/photo/1

Figure 4.26 present the Twitter and Instagram Evidence activities reconstructed from the suspect's HD, detailed Evidence information is presented in Appendix 30.

★	#	Site ...	URL	Artifact
★	240	Twitter	https://twitter.com/smithvolko1/status/610256647156412416/photo/1	Internet Explorer 10-11...
★	381	Twitter	https://twitter.com/smithvolko1/status/610253537465925632/photo/1	Firefox Web History

★ #	URL	File Type	Content Size	Source
★ 46	https://pbs.twimg.com/media/CHgR34sUsAA-sLd.jpg	jpeg	15133	IMAGE-suspect1-harddrive.E01

Showing results 1 - 1 of 1

Details	Hex	Text
File Type	jpeg	
Content Size	15133	



4.3.2.6 Conclusion

99

performed using Firefox, and Chrome but they were incorrectly presented in the Internet Explorer history files.

Findings show that a wide variety of evidence can be found from different sources, RAM and pagefile.sys are crucial sources of evidence to be examined in order to reconstruct Facebook Chats, Tweets, and Retweets. For Facebook Chats, IEF has better capabilities than the other two in terms of finding messages, as it recovered exactly the same messages recovered using Belkasoft and IXTK, but it also recovered all the messages sent and received using Internet Explorer.

4.3.3 Comparative Analysis

The main objective of performing comparative analysis is to compare the activities documented in Appendix1 (controlled data) with the data reconstructed from each digital forensic tool. Regardless of the source of evidence (RAM, pagefile.sys, and HD), the comparative analysis will be crucial to answer the research questions and hypotheses.

Tables 4.5 and 4.6 summarize the activities performed using the three browsers, and identifies the abilities of each forensic tool for findings these activities.

Table 4.5: Comparative Analysis for Facebook & Instagram Activities

<i>Facebook & Instagram</i>		<i>Reconstructed Data</i>		
Controlled Data	Browser Tool	Belkasoft	IXTK	IEF
Wall Posts	Firefox	Not Found	Not Found	Not Found
	Chrome	Not Found	Not Found	Not Found
	IE	Not Found	Not Found	Not Found
Uploaded Pictures	Firefox	Found	Not Found	Found
	Chrome	Found	Not Found	Found
	IE	Found	Found	Found
Posts on Friend's Wall	Firefox	Not Found	Not Found	Not Found
	Chrome	Not Found	Not Found	Not Found
	IE	Not Found	Not Found	Not Found
Instant Messaging	Firefox	Partially Found	Partially Found	Partially Found
	Chrome	Partially Found	Partially Found	Partially Found
	IE	Not Found	Not Found	Found
Uploaded Videos	Firefox	Found	Not Found	Found
	Chrome	Found	Found	Found
	IE	Found	Found	Found
Shared Instagram Picture on Facebook	Firefox	Found	Found	Found
	Chrome	Found	Found	Found
	IE	Found	Found	Not Found
Suspect Account Logged in in Instagram	Firefox	Found	Not Found	Found
	Chrome	Found	Not Found	Found
	IE	Not Found	Not Found	Not Found
Viewed Instagram picture in Instagram Website	Firefox	Found	Not Found	Found
	Chrome	Found	Not Found	Found
	IE	Found	Found	Found

Table 4.6: Comparative Analysis for Twitter & Instagram Activities

<i>Twitter & Instagram</i>		<i>Reconstructed Data</i>		
Controlled Data	Browser Tool	Belkasoft	IXTK	IEF
Wall Post (Tweets)	Firefox	Found	Not Found	Found
	Chrome	Found	Not Found	Found
	IE	Found	Not Found	Found
Uploaded Pictures	Firefox	Found	Found	Found
	Chrome	Found	Found	Found
	IE	Found	Not Found	Found
Tweets on Friend's Wall	Firefox	Not Found	Not Found	Not Found
	Chrome	Not Found	Not Found	Not Found
	IE	Not Found	Not Found	Not Found
Direct Messaging	Firefox	Not Found	Not Found	Not Found
	Chrome	Not Found	Not Found	Not Found
	IE	Not Found	Not Found	Not Found
Shared Instagram Picture on Twitter	Firefox	Not Found	Not Found	Not Found
	Chrome	Found	Not Found	Not Found
	IE	Found	Not Found	Not Found
Viewed Instagram picture on Instagram Website	Firefox	Found	Found	Found
	Chrome	Found	Found	Not Found
	IE	Found	Found	Found
Suspect's Retweets	Firefox	Found	Not Found	Not Found
	Chrome	Found	Not Found	Not Found
	IE	Found	Not Found	Not Found

4.4 SECOND CASE SCENARIO – POLICY BREACH

The second Case Scenario involves a breach of policy implemented by the oil company Gold-Star. The employee Jason Lopiz was using LinkedIn and Bayt using the company's network. The performed activities on LinkedIn and Bayt is listed in table 4.2, and documented in the controlled data in Appendix 2. The objective of this investigation is to find evidence if Jason was using OSNSs during working hours using the company's network, by examining RAM, pagefile.sys, and the hard drive. Three digital forensic tools are used in this investigation which are Belkasoft Evidence Center, Internet Examiner Toolkit, and Internet Evidence Finder.

Similar to the first case scenario, test plans are developed for each digital forensic tool, and each source of evidence whether RAM & pagefile.sys, or HD. For Belkasoft analysis, the first test plan in Appendix 9 (Test plan 3) is analysis of RAM using Belkasoft. Appendix 10 (test plan 4) is analysis of the HD using the same tool. In Appendix 21 is the test plan for analysing the suspect's HD (Test plan 8). Test plan 7 is not listed in the Appendices as IXTK was not able to find any evidence from RAM and pagefile.sys. For Internet Evidence Finder, Appendix 27 (Test plan 11) is the analysis of RAM, and Appendix 28 (Test plan 12) is analysis of the suspect's HD. Each of these test plans have 6 test scenarios, which are presented in the form of tables.

The first three tables are for activities performed on LinkedIn on Firefox, Chrome, and IE, The other three tables are the activities performed on Bayt with the three browsers.

4.4.1 Forensic Investigation Environment Setup

The environment setup for the suspect's computer has been described in Section 4.2.7. The same steps and procedures have been performed on the second case scenario, starting from Wiping the hard drive with Darik's Boot and Nuke tool wiping utility, to installing the three selected browsers. It's important to note that exactly the same operating system, and browsers' version were installed. For the investigator machine, the same Software/Hardware presented in Section 4.3.1, is also used in this case scenario.

4.4.2 Digital Forensics

The adopted digital forensic investigation phases in the first case scenario, is also adopted in the second case scenario, which is based on the computer forensic guidelines methodology proposed by Noureldin, Hashem, and Abdalla (2011). The six phases are: Evaluation and Assessment, Acquisition of Evidence, Survey of digital scene, Examination of digital evidence, data reconstruction, and conclusion.

4.4.2.1 Evaluation and Assessment

Jason's Laptop was powered on when the forensic team arrived to Jason's office for seizure. The forensic team have acquired the RAM, and pagefile.sys using FTK Imager Lite before pulling the power cord off the laptop. Then, Jason's Laptop was sent to the laboratory after pulling the power cord from the laptop. The HD was then taken off the seized laptop for acquisition, and examination.

4.4.2.2 Acquisition of Evidence

The forensic team used Tableau Imager, and Tableau eSATA forensic bridge to acquire Jason's HD. The Hard disk drive is a Fujitsu SATA hard disk drive, Model: MHW2160BH PL, the Hard disk Serial Number is: K109T7829RN2, and has storage space of: 160 gigabytes (GB). For integrity verification, both RAM and hard drive images were verified with MD5 checksum and SHA1 using FTK imager. The RAM image evidence verification is saved as test2_Livememory_suspect2.001 (Appendix 5). The hard drive image is also verified and saved as IMAGE_suspect2_harddrive.E01 (Appendix 6). The process of connecting the HD

with the forensic bridge to the investigator PC for acquisition and verification was depicted in Figure 4.7. The original files of Jason's RAM, and HD were kept in safe place along with the physical HD.

4.4.2.3 Survey of Digital Scene

The imaged HD is mounted as physical drive in AccessData FTK image by performing Mount Image to drive. The method mode used was Block Device/ Read only, this is crucial step in order to prevent any alteration or modification to files structure, or contents of the files. Obvious locations such as searching for user metadata, browsers types used by Jason, finding the browser file location, and so on were employed. According to the evaluation, Jason was using three browsers (Internet Explorer, Firefox, and Chrome), and there were no destructive process performed recently, and there are no encrypted data files. Smith is logged into his laptop with a username name (admin). Browser files were noted, along with I:\Users\admin\AppData. The last date modified on browser files is 23/6/2015, which is exactly the same date the controlled data were simulated in Appendix 2 (Controlled Data for the second case scenario).

4.4.2.4 Digital Evidence Examination

The evidence files (RAM, pagefile.sys, and HD) were entered to the three digital forensic tools for evidence processing and extraction. Similar to case scenario one, there were two cases created in each digital forensic tool, in order to properly evaluate the source of evidence. The first case scenario is for RAM and pagefile.sys analysis, the second case is for hard drive analysis. Once the images were entered in Belkasoft, the MD5 hash values are calculated in order to ensure that the images were not altered, by verifying that the MD5 hash calculated using Belkasoft is exactly same as the MD5 values verified in FTK imager. Once verification has been confirmed using Belkasoft, evidence search is conducted after data carving, with the use of search for word or phrase in Belkasoft. The tool was able to recover valuable evidence from both RAM and HD. Figure 4.27 illustrates the percentage number of evidence items found from LinkedIn and Bayt, using Belkasoft Evidence Center. Figure 4.27 shows that most of the evidence found from LinkedIn and Bayt are stored on the hard drive. Belkasoft was able to recover an average of 20% of all activities performed on LinkedIn, and an average of 29% of all evidence simulated on Bayt. When comparing the three browsers, the average number of evidence items recovered from LinkedIn and Bayt

using Firefox is 34%, and 18% of average number of evidence items using Chrome, In Internet Explorer, the average of all the activities recovered is 23%. The examination and searching for evidence has been conducted on Test Plan Three for RAM analysis (Appendix 9), and test plan four for hard drive analysis (Appendix 10).

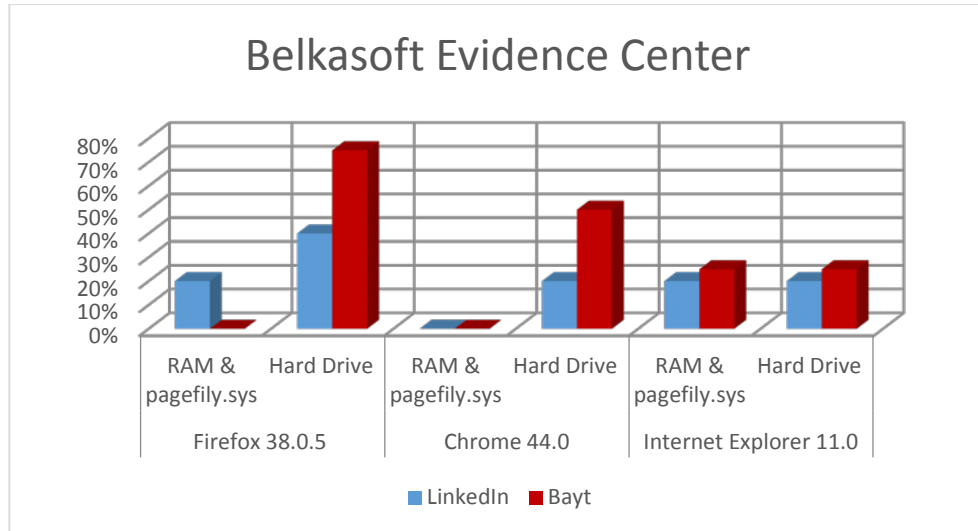


Figure 4.27: Evidence Extracted Using Belkasoft Evidence Center

Internet Examiner Toolkit was not able to recover any evidence from RAM and pagefile.sys. For HD examination, IXTK recovered one evidence from LinkedIn and nothing from Bayt. The Found Evidence is the uploaded picture on LinkedIn using Internet Explorer as shown in Figure 4.28, which was found in Temporary Internet Files. The Evidence is recorded in test plan 8 for IXTK hard drive analysis (Appendix 21), a report generated by Internet Examiner Toolkit is presented in Appendix 24.

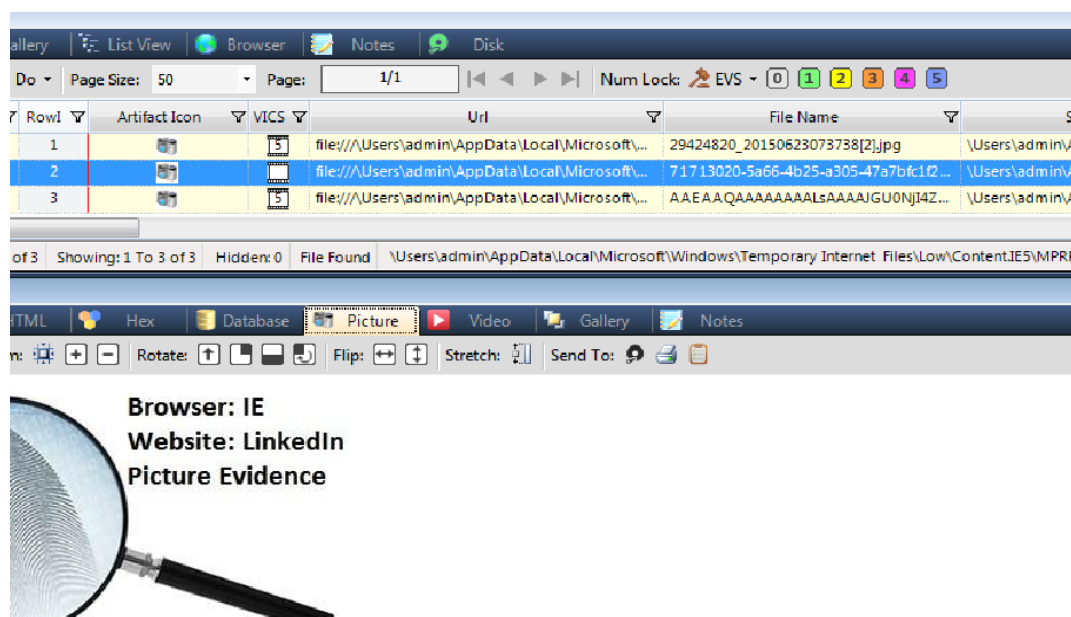


Figure 4.28: The LinkedIn Evidence extracted from IXTK

Internet Evidence Finder has better capabilities for finding evidence from LinkedIn and Bayt. Figure 4.29 demonstrates the percentage of activities recovered using IEF. The overall average of evidence items found from LinkedIn is 20%, and an average of 54% of the simulated evidence in Bayt were recovered. When comparing the evidence recovered from each browsers, IEF was able to recover an average of 29% of the posted data on LinkedIn and Bayt when the suspect was using Firefox. Activities performed on the two OSNSs were recovered with a total average of 60% when the suspect was using Chrome, which is the best average percentage recovered from all tools. For IE, an average of 23% of the evidence items were recovered. For IEF examination, the findings of RAM analysis is documented in Test plan 11 (Appendix 27), for the Hard drive analysis it is presented in Test plan 12 (Appendix 28). The reports generated by Internet Evidence Finder are presented in Appendix 31 & Appendix 32.

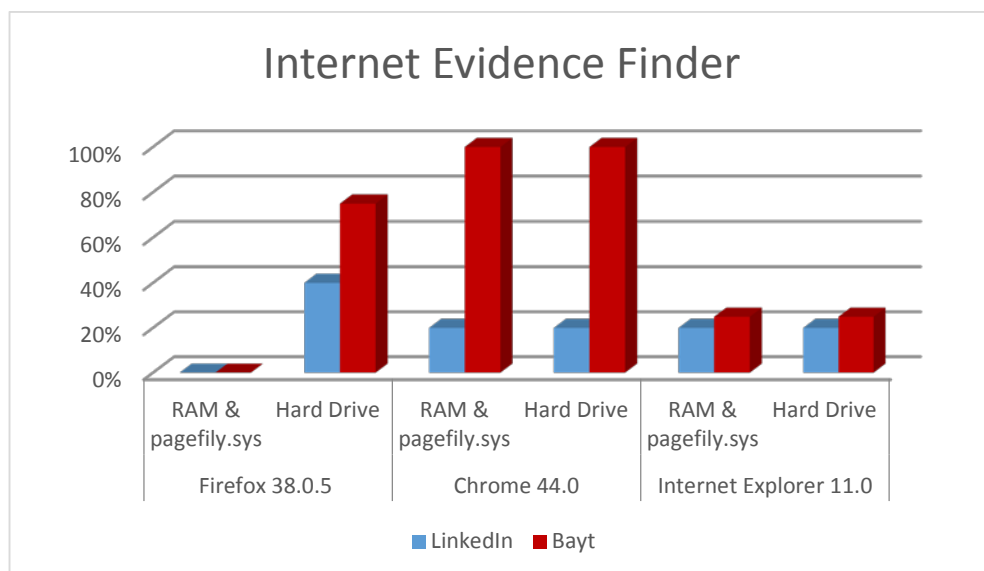


Figure 4.29: Evidence Extracted Using Internet Evidence Finder

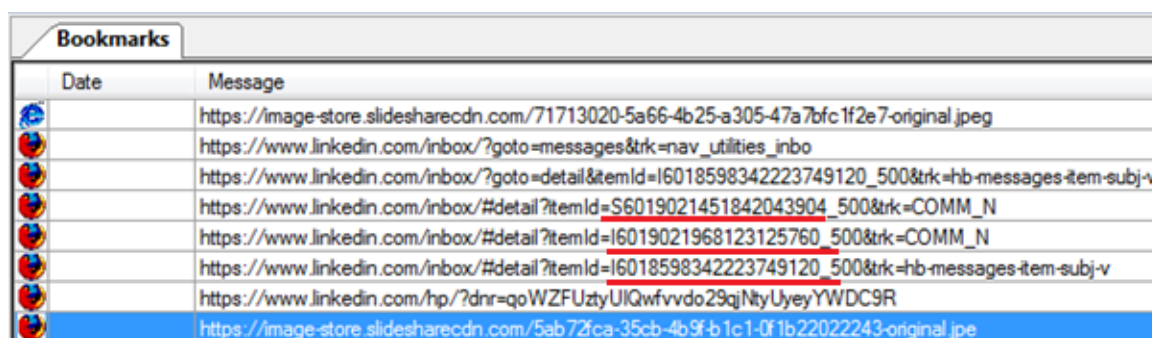
This section has shown the number of evidence items found from LinkedIn and Bayt on each digital forensic tool. It is noticeable that Internet Examiner Toolkit failed in finding most of the forensic evidence from the two OSNSs. This may be due to the fact that they have not included LinkedIn and Bayt on their supported Artefacts. The only OSNSs artefacts supported by IXTK as presented in their Manual are Facebook, Twitter, and YouTube (Siquet, 2015). The following Section discusses the types of findings that were recovered by each digital forensic tools.

4.4.2.5 Reconstruction of Extracted Data

For LinkedIn Activities:

It is confirmed that none of the three digital forensic tools are able to extract posted evidence on suspect's wall, posted comments on pictures, and picture likes. In Belkasoft, the posted pictures using Firefox and IE were found on both RAM (Figure 4.30) and HD (Figure 4.32), while the posted pictures using Chrome were only found from the target's HD, stored in the Chrome cache in K:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3. The uploaded pictures on LinkedIn are normally stored as image-store, or media.licdn.com. The LinkedIn uploaded picture URL looks as follow:

<https://image-store.slidesharecdn.com/5ab72fca-35cb-4b9f-b1c1-0f1b22022243-original.jpeg>



Date	Message
	https://image-store.slidesharecdn.com/71713020-5a66-4b25-a305-47a7bfc1f2e7-original.jpeg
	https://www.linkedin.com/inbox/?goto=messages&trk=nav_utilities_inbo
	https://www.linkedin.com/inbox/?goto=detail&itemId=I6018598342223749120_500&trk=hb-messages-item-subj-v
	https://www.linkedin.com/inbox/#detail?itemId=S6019021451842043904_500&trk=COMM_N
	https://www.linkedin.com/inbox/#detail?itemId=I6019021968123125760_500&trk=COMM_N
	https://www.linkedin.com/inbox/#detail?itemId=I6018598342223749120_500&trk=hb-messages-item-subj-v
	https://www.linkedin.com/hp/?dnr=qoWZFUztyUIQwfvvdo29qjNtyUyeyYWDc9R
	https://image-store.slidesharecdn.com/5ab72fca-35cb-4b9f-b1c1-0f1b22022243-original.jpe

Figure 4.30: LinkedIn Evidence Found from RAM on Belkasoft

Internet Evidence Finder was able to recover all the posted pictures from RAM and HD, except the picture uploaded using Firefox which was only extracted from the target's HD and stored in Firefox Cache records (Appendix 34). Figure 4.31 shows the two pictures uploaded using Chrome, and IE which were recovered from RAM.

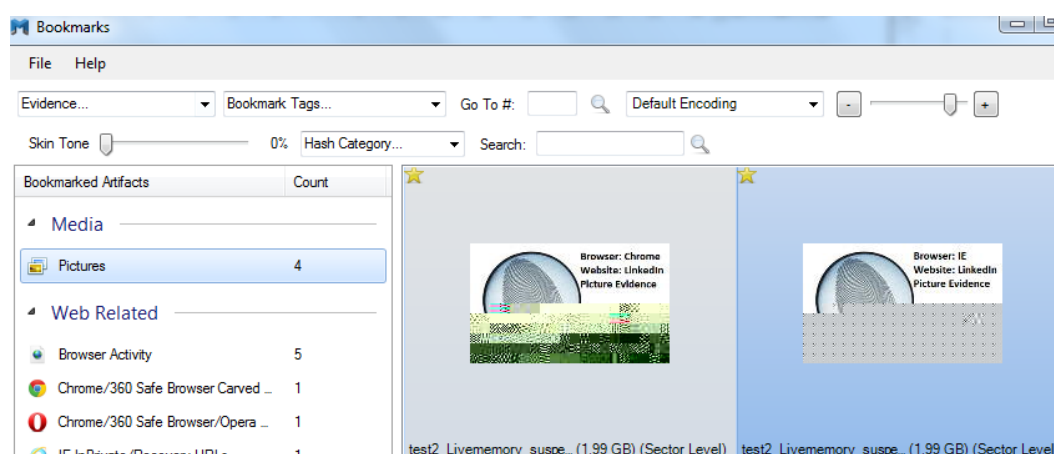


Figure 4.31: LinkedIn Evidence Pictures from RAM on IEF

Both Belkasoft and Internet Evidence Finder were successful in extracting the sent message using Firefox browser. The sent message were only extracted from the target's HD in:

\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\zjhbp3me.default\formhistory.sqlite.

The message was presented in plaintext in both tools as follow:

Subject; Generate message to friend evidence in LinkedIn using Firefox test post 3.

As shown in the following Figure 4.32, Belkasoft was able to extract posted pictures using chrome, Firefox, and IE, and it successfully extracted the message sent to a friend using Firefox. The recovered message using IEF is presented in Appendix 34. The other messages sent using Chrome and IE were not extracted, and IXTK was not successful in extracting any of the messages.

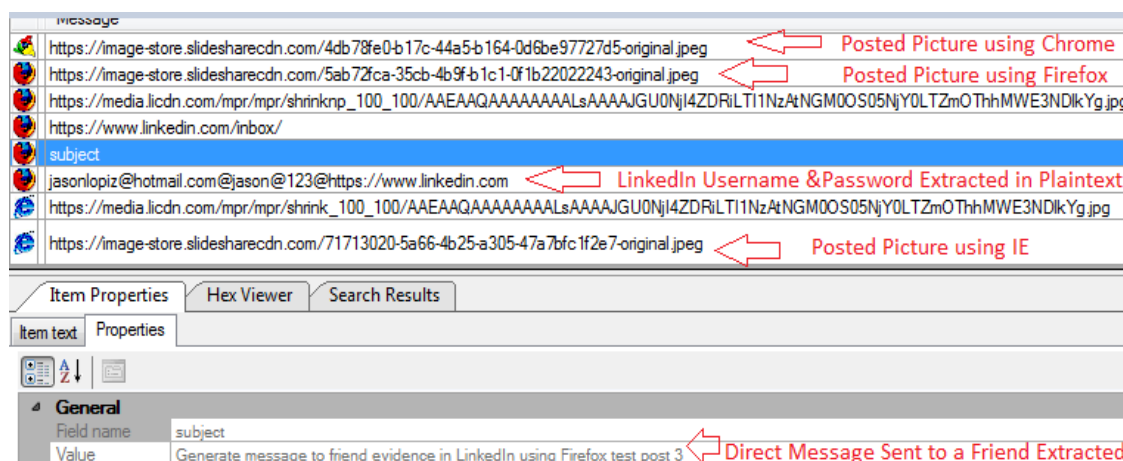


Figure 4.32: LinkedIn Evidence Found from HD on Belkasoft

Belkasoft Evidence Center was the only tool that was able to extract the LinkedIn Username and Password in plaintext for the suspect's account, which was stored in: K:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\zjhbp3me.default. Reports of LinkedIn evidence findings have been generated by Belkasoft and listed in Appendix 15 and Appendix 17.

For Bayt activities:

Belkasoft, and Internet Evidence Finder were able to extract all the posted questions from the target's HD for all the browsers, however, when examining RAM, only the questions posted using IE were recovered by Belkasoft (Figure 4.33), and the two questions posted using Chrome and Internet Explorer were recovered by IEF (Appendix 33). IXTK failed to extract any questions posted on Bayt.

Date	Message
	http://people.bayt.com/saud-elshafi/#submit-alert-message ← Only Friend's ID, Not the Message
	http://www.bayt.com/en/specialties/q/205292/generate-question-as-evidence-in-bayt-using-ie/?first_p=1&b_share=0
	http://www.bayt.com/en/specialties/dashboard/ ↑ Only Question posted using IE
	http://www.bayt.com/en/mymailbox-j/
	http://people.bayt.com/saud-elshafi/ ← Friend's URL Profile, No Message Extracted in IE
	http://www.bayt.com/en/mymailbox-j/#inbox/p1/12686714/
	https://www.bayt.com/en/login/
	http://people.bayt.com/saud-elshafi/

Figure 4.33: Bayt Evidence Recovered from RAM on Belkasoft

IEF successfully recovered the recommendation made to a friend when the suspect was using Chrome. The evidence was recovered from RAM (Appendix 33), and also from the hard drive (Appendix 34). The evidence was notable from the Hex viewer in IEF. The other recommendations sent to a friend using Firefox and Internet Explorer were not recovered. Belkasoft and IXTK were not successful in extracting any of the recommendations made using all the browsers.

The questions are answered from the same browsers they were posted from during RAM examination. They only answer link found is when the suspect was using Chrome, and it was found by IEF (Appendix 33). RAM analysis for the other two tools were not successful in finding any links to the answers made using all browsers. However, when examining the target's HD, both Belkasoft and IEF successfully extracted the links of the answers posted using Firefox and Chrome, and nothing was extracted for Internet Explorer. IXTK was not successful in extracting any of the performed answer evidence.

The direct messages sent to a friend in Bayt were only recovered by Belkasoft from the target's HD (Figure 4.34) when the suspect was using Firefox. IXTK was not able to extract any of the direct messages sent. On the other hand, IEF was able to extract the message sent using Chrome from both RAM (Appendix 33) and HD. The direct message sent using Firefox from only HD is in (Appendix 34). Detailed reports of Bayt evidence found from RAM, pagefile.sys, and HD using Belkasoft is listed in Appendix 16 and Appendix 18.

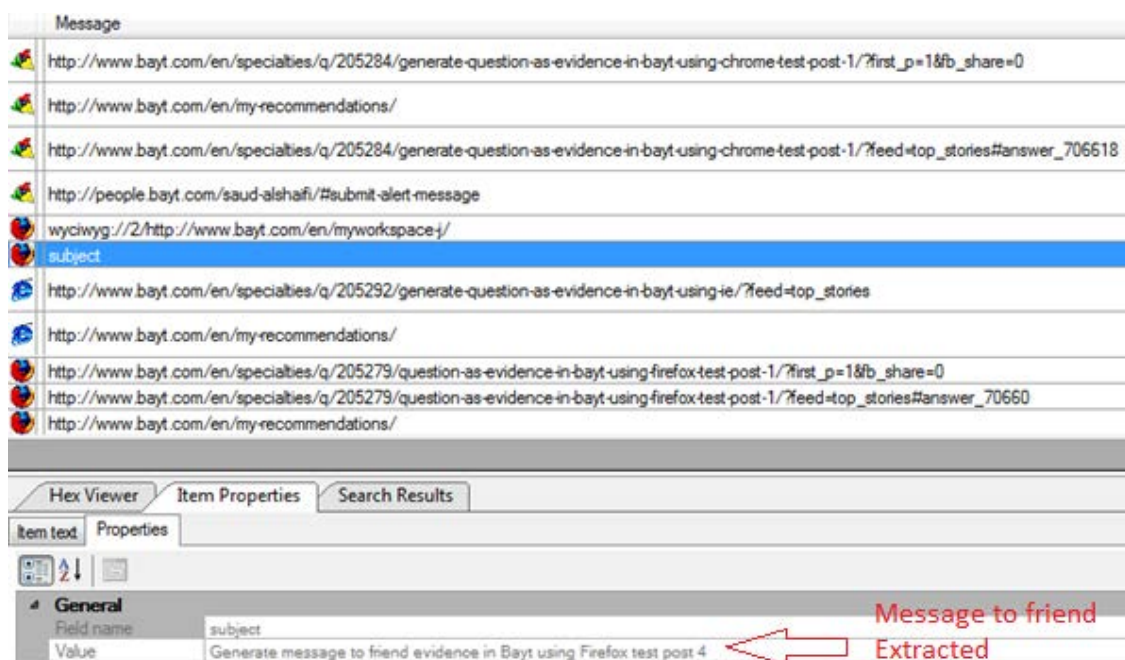


Figure 4.34: Bayt Evidence Recovered from HD on Belkasoft

4.4.2.6 Conclusion

Based on digital evidence examinations, and reconstruction of extracted data, it's evident that Jason Lopiz was using LinkedIn and Bayt during business hours. When the investigation was conducted using Belkasoft and Internet Evidence Finder, these two tools were able to extract a lot more evidence than Internet Examiner Toolkit. Some of the evidence extracted from Belkasoft and IEF were recovered at an exact time that these data were performed. On the other hand, IXTK was only able to trace a picture artefact that was posted on LinkedIn using Internet Explorer, but no additional metadata were extracted such as date and time, which is insufficient to prove that Jason was using OSNSs on that day.

The findings show that some of the LinkedIn and Bayt private messages are recoverable by using Belkasoft and IEF, and by examining the target's HD. Evidence Recommendations made by the suspect in Bayt are also recoverable when using IEF.

4.4.3 Comparative Analysis

The following tables are the comparative analysis between the activities (Controlled data) posted and documented in Appendix 2, and the reconstructed data from the three digital forensic tools. This comparative analysis summarizes the capabilities of each digital forensic tool in finding each evidence item that has been posted using three browsers. Regardless of the source of evidence, if a certain evidence item is recovered

from one source (i.e.: RAM) and not recovered from other sources (i.e.: HD), then the overall result is (Found). Table 4.7 is the overall results of LinkedIn activities found from three digital forensic tools, and Table 4.8 is the overall results of Bayt activities found from each selected digital forensic tool.

Table 4.7: Comparative Analysis for LinkedIn Activities

<i>LinkedIn</i>		<i>Reconstructed Data</i>		
Controlled Data	Browser Tool	Belkasoft	IXTK	IEF
Status Updates (Wall Posts)	Firefox	Not Found	Not Found	Not Found
	Chrome	Not Found	Not Found	Not Found
	IE	Not Found	Not Found	Not Found
Uploaded Pictures	Firefox	Found	Not Found	Found
	Chrome	Found	Not Found	Found
	IE	Found	Found	Found
Posted Comments on Uploaded Pictures	Firefox	Not Found	Not Found	Not Found
	Chrome	Not Found	Not Found	Not Found
	IE	Not Found	Not Found	Not Found
Liked Pictures	Firefox	Not Found	Not Found	Not Found
	Chrome	Not Found	Not Found	Not Found
	IE	Not Found	Not Found	Not Found
Private Messages sent to a Friend	Firefox	Found	Not Found	Found
	Chrome	Not Found	Not Found	Not Found
	IE	Not Found	Not Found	Not Found

Table 4.8: Comparative Analysis for Bayt Activities

<i>Bayt</i>		<i>Reconstructed Data</i>		
Controlled Data	Browser Tool	Belkasoft	IXTK	IEF
Posted Questions	Firefox	Found	Not Found	Found
	Chrome	Found	Not Found	Found
	IE	Found	Not Found	Found
Sent Recommendations	Firefox	Not Found	Not Found	Not Found
	Chrome	Not Found	Not Found	Found
	IE	Not Found	Not Found	Not Found
Answered to the posted Questions	Firefox	Found	Not Found	Found
	Chrome	Found	Not Found	Found
	IE	Not Found	Not Found	Not Found
Direct Messages Sent to a Friend	Firefox	Found	Not Found	Found
	Chrome	Not Found	Not Found	Found
	IE	Not Found	Not Found	Not Found

4.5 CONCLUSION

This Chapter has reported the findings, and analysis of three digital forensic tools that were used to find a wide variety of evidence from five online social networking sites. The experiment has confirmed that the types of data can be found in OSNSs is impressive, including the person's credentials. However, due to the dynamic structure of OSNSs it is still challenging to extract every piece of posted data. In this experiment

some of the posted data was not found at all. It was not found from RAM, pagefile.sys, or HD, and neither found from the three browser cache files. This experiment has confirmed that private messages (to a friend) on Facebook, LinkedIn, and Bayt are recoverable. Twitter messaging on the other hand was not able to be recovered. The research findings will be discussed further in Chapter 5 in order to answer the research question, sub-questions, and the research hypotheses.

Chapter 5

Discussion of Findings

5.0 INTRODUCTION

Chapter 4 reported the findings of the research investigations conducted according to research methodology described in Chapter 3. The changes encountered to data requirements during the testing experiment, are reported in Section 4.1. The results of the investigation are presented in both descriptive and visual ways. The findings enabled the researcher to ascertain the recoverable types of online social networks activities, and their crucial locations when conducting a forensic investigation using the three selected digital forensic tools. Based on the research findings, a comprehensive review will be made in order to define each tool capabilities, strengths, and weaknesses. The main objective of Chapter 5 is to answer the research question, sub-questions and research hypotheses (Section 3.2.3). Also the findings are discussed in relation to evidence evaluation from each digital forensic tool and the Chapter 2 literature expectations that were set at the beginning of the research process.

Chapter 5 consists of 3 sections, Section 5.1 aims to answer the research sub-questions, research hypotheses developed in Chapter 3, and concludes with answering the main research question. Section 5.2 provides a comprehensive discussion of the experiment findings from each digital forensic tool, and an evaluation of results for each tool's capabilities, strengths, and weaknesses, and presents method recommendation for forensic investigators. Lastly Section 5.3 concludes this Chapter.

5.1 RESEARCH QUESTIONS AND HYPOTHESES

This section starts with answering the research sub-questions based on the collected evidence, and the digital forensic investigation conducted in Chapter 4. The answers of each sub-question is presented in Section 5.1.1. Section 5.1.2 is to test the research hypotheses which are checked against the experiment findings. The hypotheses testing with arguments for and against are presented in table format. Ultimately, the main research question will be answered in Section 5.1.3.

5.1.1 Sub-Questions

In order to answer the main research question, six associated sub-questions outlined in Section 3.2.3 were used during the digital forensic testing and analysis. The following tables present each sub-question, their associated answers, and summary, in Table 5.1 to Table 5.6.

Table 5.1: Sub-Question 1 and Answer

Sub-Question 1 (SQ1): What are the types of data that can be found for each online social networking site?
Answer: It varies from each online social networking site. Facebook provides more types of collectable evidence than any other OSNSs.
Summary: Based on preliminary tests on Section 4.2, the collectable forensic evidence from Facebook include: Images, videos, status and wall posts, shared links ,comments, replies, likes, private messages, user locations, Usernames, Facebook profile ID used to send, and received private messages, Facebook profile picture, Joined group pages, events, friend lists , Date/ Time of each performed activity. The collectable Twitter activities are Tweets which can be in text format, pictures, or short videos. Private messages sent and received, Twitter profile picture, username ID, shared links, hashtag names, usernames, unique post ID, following users and the followers, Retweets, and Date/Time of each activity. The types of data can be found from Instagram consists of username account information, shared pictures and videos, Direct pictures/Videos sent to another user, Unique URL ID of each posts. The types of data that can be found from LinkedIn consists of: update status, pictures, comments, likes, professional user information, LinkedIn profile picture ,private messages sent and received, User ID, Date/ Time of each posted data. The types of data can be collected from Bayt consists of: posted questions, recommendations, private messages, posted answers to questions. No videos/Pictures were allowed to be posted apart from users' profile picture.

Table 5.2: Sub-Question 2 and Answer

Sub-Question 2 (SQ2): Can the selected tools perform a successful acquisition without the need for other tools?
Answer: No, the investigation shows that all the three selected digital forensic tools require additional software for acquiring evidence from the target machine.
Summary: Although none of the selected digital forensic tools were able to acquire the target's HD, the vendors provided separate volatile memory acquisition tools: <ol style="list-style-type: none">1. Belkasoft RAM Capture: Dumps memory of all versions of Windows Operating systems, the dumped memory created in file type .mem2. SiQuest Memory Imager: capture memory (RAM) into one or more contiguous RAW (DD) image file format. (Windows OS).3. Magnet RAM Capture: capture physical memory (RAM) of the target's PC into RAW (.DMP) image file format. (Windows OS). However, all the three digital forensic tools lack in acquisition functionality, therefore additional tools were needed for acquiring the target's HD, and pagefile.sys.

Table 5.3: Sub-Question 3 and Answer

Sub-Question 3 (SQ3): What are the hardware and software applications used for extraction and acquisition of OSNSs data which best suits the three selected forensic tools for examination?
Answer: A list of hardware and software specifications are identified in Section 4.3.1. The additional software used is FTK imager lite for RAM, pagefile.sys acquisition. Tableau Imager, Tableau eSATA forensic bridge for HD acquisition.
Summary: Since all the tool vendors provide a separate software for RAM dumps, and each of these tools have different image file formats (.mem, DD, DMP.), additional tool was needed to acquire RAM and pagefile.sys, in order to use the same acquired image in all of the three selected digital forensic tools for analysis.

Table 5.4: Sub-Question 4 and Answer

<p>Sub-Question 4 (SQ4):</p> <p>How are the collected data validated?</p>
<p>Answer:</p> <p>As shown in Sections 4.3.2 and Section 4.4.2, the dumped memory using FTK imager lite, and the acquired HD using Tableau Imager, were verified using AccessData® FTK Imager, by calculating MD5 & SHA1 hash values. Further validation of the images were performed by Belkasoft Evidence Center, in order to ensure that the image MD5 hash value calculated by Belkasoft matches the MD5 hash value of the image verified by FTK imager. (Note: Belkasoft doesn't calculate SHA1).</p>
<p>Summary:</p> <p>The following hashes present the RAM and HD hash images acquired in the first case scenario:</p> <p>RAM Verifications:</p> <p>[Computed Hashes]</p> <p>MD5 checksum: 3a5333cba55123167fe1cd9e4eb7dc98</p> <p>SHA1 checksum: 0c7031ae82a9d72ecdba04f487c63d7d5056eb6e</p> <p>Image Verification Results:</p> <p>MD5 checksum: 3a5333cba55123167fe1cd9e4eb7dc98 : verified</p> <p>SHA1 checksum: 0c7031ae82a9d72ecdba04f487c63d7d5056eb6e : verified</p> <p>Belkasoft hash validation:</p> <p>MD5 hash: 3a5333cba55123167fe1cd9e4eb7dc98 (Validated)</p> <p>HD Verifications:</p> <p>[Computed Hashes]</p> <p>MD5 checksum: abeddbf96de0e20747b3cc32e75dbace</p> <p>SHA1 checksum: 4a3a569616a70371a5cc1d0a0fa56f3350838bab</p> <p>Image Verification Results:</p> <p>MD5 checksum: abeddbf96de0e20747b3cc32e75dbace : verified</p> <p>SHA1 checksum: 4a3a569616a70371a5cc1d0a0fa56f3350838bab : verified</p> <p>Belkasoft hash validation:</p> <p>MD5 hash: abeddbf96de0e20747b3cc32e75dbace (Validated)</p> <p>The following hashes present the RAM and HD hash images acquired in the second case scenario:</p> <p>RAM Verifications:</p> <p>[Computed Hashes]</p> <p>MD5 checksum: c0024b656b4fa49683852e51281cca4a</p> <p>SHA1 checksum: 98b865fb18a95d8525d34bb93c895dca0d6ccc4b</p> <p>Image Verification Results:</p> <p>MD5 checksum: c0024b656b4fa49683852e51281cca4a : verified</p> <p>SHA1 checksum: 98b865fb18a95d8525d34bb93c895dca0d6ccc4b : verified</p> <p>Belkasoft hash validation:</p>

MD5 hash: c0024b656b4fa49683852e51281cca4a (Validated)
 HD Verifications:
 [Computed Hashes]
 MD5 checksum: c4649a4654466e0b777974bdd1e281fa
 SHA1 checksum: ffe81ffe1c48e876509394f2e5251775ed98d024
 Image Verification Results:
 MD5 checksum: c4649a4654466e0b777974bdd1e281fa : verified
 SHA1 checksum: ffe81ffe1c48e876509394f2e5251775ed98d024 : verified
 Belkasoft hash validation:
 MD5 hash: c4649a4654466e0b777974bdd1e281fa (Validated)

Table 5.5: Sub-Question 5 and Answer

Sub-Question 5 (SQ5):

What types of data are within the scope for each digital forensic tool?

Answer:

Based on reconstruction of extracted data in sub sections 4.3.2.5 and 4.4.2.5, the data that are within the scope for each digital forensic tool varies depending on several factors: the source of evidence, the web browser, and the social networking site used by the suspect.

Summary:

Regardless of the source of evidence, and the browser used by the suspect, it is confirmed that all of the three selected tools are able to recover the following activities:

1. Facebook: Uploaded pictures and videos, private (Instant) messages, shared Instagram picture links, and viewed Instagram pictures on Instagram website.
2. Twitter: Uploaded Pictures, Viewed shared Instagram picture on Instagram website.
3. LinkedIn: Uploaded Pictures.

It is confirmed that only Belkasoft Evidence Center and Internet Evidence Finder are able to recover the following activities:

1. Instagram: Suspect account logged into Instagram.
2. Twitter: Wall posts (Tweets).
3. LinkedIn: Private Messages
4. Bayt: Posted questions, posted answers, and direct messages.

It is confirmed that only Belkasoft Evidence Center is able to recover the following activities:

<ol style="list-style-type: none"> 1. Twitter: Shared Instagram pictures on Twitter, Suspect's Retweets. 2. LinkedIn: login name, email address and password of the suspect account. <p>It is confirmed that only Internet Evidence Finder is able to recover the following activities:</p> <ol style="list-style-type: none"> 1. Bayt: recommendations made. <p>Field-findings also confirmed that none of the three selected digital forensic tools are able to find the following activities:</p> <ol style="list-style-type: none"> 1. Facebook: Wall posts (Status updates), and posts made on friend's wall. 2. Twitter: Tweets on friend's wall, and direct messages. 3. LinkedIn: Status updates, posted comments on pictures, and liked pictures.

Table 5.6: Sub-Question 6 and Answer

<p>Sub-Question 6 (SQ6):</p> <p>What is the ranking of the selected digital forensic tools in terms of accuracy and capability of extraction OSNSs data?</p>
<p>Answer:</p> <p>In terms of location of each evidence recovered:</p> <p>Belkasoft scored 1st for identifying and presenting the right evidence location sources, IEF is the 2nd and IXTK is the 3rd.</p> <p>In terms of recovering evidence date/time:</p> <p>Internet Evidence Finder scored 1st for recovering date/time of evidence (activities) posted by the suspect, Belkasoft scored 2nd highest number of recovered date/time for some evidence, IXTK was the 3rd.</p>
<p>Summary:</p> <p>There are two factors that identify the accuracy of the recovered evidence from each tool which are: the location of the evidence extracted, and the recovered evidence has its metadata including date/time.</p> <p>Belkasoft was able to identity evidence and their sources accurately from each browser, whereas the same evidence recovered in IEF were presented in a form of links which means that it need to be accessed by the investigator in order to see what has been posted. For example, the recovered Tweets in Belkasoft were presented within the tool in plaintext, which saves the investigator the time to click every link, (See Twitter Live RAM in Appendix 12). The same recovered evidence by IEF were presented in the form of links. This too might affect the forensic investigation, as a</p>

particular tweet may be deleted by the suspect during the investigation, or a suspect's assistant may remove all twitter posts with intention of destroying evidence. Belkasoft was also able to identify visit page names/ page titles (Appendix 11, 12, 13, 14, 15, 17, and 18), but IEF did not include visit page names in most of the recovered evidence. IXTK scored 3rd as some of OSNSs activities posted using Firefox and Chrome were inaccurately presented in Internet Explorer temporary internet files, and the WebCacheV01.dat cache file (Appendix 23).

IEF was better than Belkasoft and IXTK in identifying most of the evidence metadata including Facebook messages ID, and date/time. In IEF the number of recovered evidence with the date/time of the activities performed by the suspect. There were 37 evidence items, whereas in Belkasoft the number of evidence items recovered with their date/time was 32, and 6 evidence items in IXTK.

5.1.2 Hypotheses Testing

This section tests and evaluates the four hypotheses developed and outlined in Section 3.2.3. The main objective of hypotheses testing is to verify the validity of the reported findings reported in Chapter 4, and to assist in answering the main research question. The research findings and evidence collected from all the selected digital forensic tools during the digital forensics phases, are checked against the developed hypotheses, with arguments made for and against in order to draw a conclusion on whether each hypothesis is accepted, rejected, or indeterminate. The hypothesis tested are presented in Table 5.7 to Table 5.10.

Table 5.7: Hypothesis Testing 1

Hypothesis 1 (H1): It is expected that all of the chosen forensic tools will not recover everything posted on each OSNS. However, the chosen tools will be successful in acquiring sufficient information and from different locations that could be suitable for the digital forensic investigation.	
Argument For: None of the three digital forensic tools were able to recover all the posted data on the selected OSNSs. Although, some activities were not extracted in both case scenarios, all the	Argument Against: Internet Examiner toolkit was not able to recover sufficient information from LinkedIn in the second case scenario, as the only recovered evidence from LinkedIn was the uploaded picture using

<p>selected tools performed well in the first case scenario (Facebook, Twitter, and Instagram), and provided sufficient evidence for a prosecution.</p> <p>Belkasoft Evidence Center and Internet Evidence Finder were able to provide sufficient data in the second case scenario (LinkedIn and Bayt).</p>	<p>IE (Figure 4.28 and Appendix 24). The picture's metadata does not indicate that the picture was uploaded on LinkedIn by the suspect, also neither presenting the date/time of this activity. IXTK was also not able to extract any information from Bayt. Therefore, Internet Examiner Toolkit is not successful at recovering sufficient forensic evidence from both LinkedIn and Bayt.</p>
<p>Summary:</p> <p>The selected digital forensic tools were not able to recover all the data posted on OSNSs. Nevertheless, sufficient evidence can still be gathered in order to confirm the likelihood of criminal activities, as each tool was able to recover a large portion of the evidence posted on OSNSs. Furthermore, the recovered evidence from the selected tools are the same as the data previously documented in the controlled data (Appendix 1 and Appendix 2), which confirms the relevancy of each evidence item extracted by the selected tools. Thus, the argument made "For" is sufficient to confirm that the hypothesis is to be accepted.</p>	

Table 5.8: Hypothesis Testing 2

<p>Hypothesis 2 (H2): When conducting a forensic investigation on different OSNSs, evidence collected from each OSNS will vary depending on the tool that is used to examine and search for evidence, and depending on the complexity of how each site is operated.</p>	
<p>Argument For:</p> <p>Variations of the types and amount of evidence extracted from the three digital forensic tools have been encountered.</p> <p>Belkasoft for example is the only tool that was able to recover the Retweets made from all the browsers (Figure 4.23 and Appendix 12).</p>	<p>Argument Against:</p> <p>Although evidence variation encountered because of the forensic tool used and the functionality of each OSNS, they are not the only factors that caused variation on the collected evidence, as some of the evidence recovered also varied because of the type of browser the suspect was using. As shown in the findings that private</p>

<p>Furthermore, it depends on the functionalities of each OSNS, and how each activity or post was generated on each OSNS, as shown from the findings that when a suspect posts a question on Bayt, the site creates a unique URL, within this URL the question is shown in plaintext (Figure 4.33, Figure 4.34, and Appendix 16, 18, 31, 32, 33, and 34). Uploading pictures on OSNSs also supports this argument, as each posted picture on OSNSs have its unique ID that represent the picture ID, and lead to the suspect profile.</p>	<p>messages in LinkedIn were recovered using Belkasoft and IEF, but only when the suspect was using Firefox (Figure 4.32. Appendix 17, 32, and 34), and no messages were extracted from Chrome or Internet Explorer.</p> <p>The selected browsers were used in their default configurations, meaning that they were installed in their own native format and file storage locations. The activities performed on OSNSs were conducted on normal browsing mode, and there were other features such as InPrivate browsing mode that would prevent the browser from storing data about browsing sessions. InPrivate browsing mode was not used in this experiment, but it may make the forensic investigation on OSNSs even harder.</p> <p>The condition of the system at seizure is another crucial factor that directly affects the collected evidence. The suspect's machine in both case scenarios was powered on when seizure occurred, meaning that the PC was forensically powered off in a manner that does not corrupt the integrity of stored files.</p>
<p>Summary:</p> <p>Collecting evidence from OSNSs is difficult because there are many factors that need careful handling. The types of digital forensic processes used is crucial for the forensic investigation, along with knowing the types of expected evidence from each OSNS. The forensic investigator has to be aware of what browser was used by the suspect. The field findings confirmed that a particular post or activity can be found</p>	

from a particular browser used by the suspect, but may not be found on others. It is crucial to determine the condition of the PC, and how to handle evidence seizure and acquisition, Thus, the argument made for and against show that the hypothesis is rejected.

Table 5.9: Hypothesis Testing 3

<p>Hypothesis 3 (H3): The chosen forensic tools will share common capabilities and functionalities. However, it is expected that Belkasoft will perform better in extracting private messages in all OSNSs, and by contrast IEF and IXTK will perform better in searching for evidence.</p>	
<p>Argument For:</p> <p>Field testing results show that the selected digital forensic tools share common capabilities and functionalities such as web browser cache extraction, partial extraction of Facebook private messages using Firefox and Chrome, the ability of extracting posted pictures and videos. The selected tools also share built-in reporting functionality.</p>	<p>Argument Against:</p> <p>According to the experiment findings, IEF performed better in extracting private messages in OSNSs, as it extracted more Facebook (Figure 4.16), and Bayt private messages than the other two tools (Appendix 33 and 34).</p> <p>Keyword search was one of the methods used on the selected tools to find evidence. Belkasoft and IEF have better keyword searching features than IXTK.</p>
<p>Summary:</p> <p>Although the selected tools have certain capabilities and functionally in common, the findings indicate that Belkasoft is not always able to perform better in extracting private messages than the other two tools. The findings also show that each tool has its own strength and limitations in extracting forensic evidence from OSNSs. Thus, the hypothesis is rejected.</p>	

Table 5.10: Hypothesis Testing 4

<p>Hypothesis 4 (H4): The collected evidence from each digital forensic tool will vary depending on the source of evidence RAM, Pagefile.sys, or HD, and it is expected that RAM and pagefile.sys analysis will add more value to the collected evidence during OSNSs forensic investigation.</p>	
<p>Argument For:</p>	<p>Argument Against:</p>

<p>The findings show that Facebook messages were no longer cached in the browser cache file, neither the performed wall posts, nor Retweets in Twitter. Some of these viable activities have been recovered from RAM, some other evidence have been swapped to the pagefile.sys in the file system and were only recovered from the pagefile.sys. So, from the field-testing results, it was discovered that some artefacts can only be recovered from RAM and pagefile.sys and cannot be found from the hard drive.</p>	<p>Some other evidence can be extracted from RAM, pagefile.sys and also from the HD. Based on file-testing results, some of the uploaded pictures on Facebook, Twitter, and LinkedIn, and some of the shared Instagram pictures were found from the three sources. Moreover, private messages sent on LinkedIn were not recovered from RAM neither pagefile.sys. However they were recovered from the target's HD in: AppData\Roaming\Mozilla\Firefox\Profiles\zjhbp3me.default\formhistory.sqlite</p>
<p>Summary:</p> <p>It is essential to understand that the activities performed on OSNSs are not stored in a specific location, and that is why OSNSs forensic investigation is challenging. The hard drive examination, and Internet Temporary files, and web browser files were vital source of evidence. If RAM and pagefile.sys analysis were not examined in both scenarios, there would be less evidence to be collected, and it would be even harder to extract different types of evidence such as private message and Tweets. Thus, RAM and pagefile.sys analysis certainly added value to the collected evidence in both case scenarios. The argument made for and against prove that the hypothesis is to be accepted.</p>	

5.1.3 The Research Question

This section aims to answer the main research question developed in Section 3.2.3. The main research question is: What evidence can be extracted from online social networking sites when using different forensic extraction tools? The aim of this research is to examine and compare the capabilities of each digital forensic tool in terms of finding forensic evidence from the five selected OSNSs.

In Chapter 2, the researcher gained an understanding of how OSNSs are used for criminal activities, and how these OSNSs contain a wide verity of forensic evidence. In Chapter 3, a number of approaches were reviewed for evaluating digital

forensic tools, and methods that are applicable for OSNSs investigations. These approaches assisted in developing the methodology for this research. Two case scenarios have been played to populate the sites with potential evidence, and also to identify the amount and type of data for discovery. In this way the tools could be assessed against the potential evidence presented and benchmarked. The first phase was identifying IT artefacts and the controlled data was posted on each OSNS. The second phase was to document each tool performance against the SWGDE validation schema that had 12 test plans (4 for each tool). Each test plan has the following: purpose of the test, its scope, requirement specifications, methodology used for testing, and test scenarios. The third phase was to perform acquisition and extraction of evidence from the computer forensics guideline methodology proposed by Noureldin, Hashem and Abdalla (2011). The fourth phase was data analysis. This phase analysed the extracted evidence in the previous phase in order to reconstruct and conduct a comparative analyses between the controlled data generated, and the evidence reconstructed from each tool.

To answer the main research question, the testing results indicate that the forensic evidence that can be extracted from the selected OSNSs using the three digital tools are as follows:

- For Facebook activities, the recoverable activities are: pictures and videos uploaded by suspect, instant messages with other individuals, shared Instagram links on Facebook.
- For Twitter activities the recoverable evidence includes: wall posts (Tweets), Uploaded pictures, shared Instagram links on Twitter, Retweets.
- For Instagram activities the recovered evidence includes: suspect's account logged on Instagram, viewed Instagram pictures that are previously shared on Facebook and Twitter on Instagram website.
- For LinkedIn activities the evidence that can be recovered are: uploaded pictures, and private messages sent to another individuals,
- For Bayt activities the recoverable evidence are: posted questions, written answers, recommendations made by the suspect, and direct messages sent to another individual.

Based on comparative analysis in Table 4.5 to Table 4.8, sub-questions, and research hypotheses, Belkasoft Evidence Center performed better than the other two digital

forensic tools in findings forensic evidence from Twitter, and Instagram. Internet Evidence Finder performed better than the other two digital forensic tools in finding evidence from Facebook, and Bayt. Belkasoft and IEF have similar capabilities in extracting evidence from LinkedIn. However, as shown in Figure 4.23 that Belkasoft was the only tool that was capable of extracting the username, email, and password of the suspect's LinkedIn account. Thus, Belkasoft performed better than the other two tools for finding evidence from LinkedIn. Although Internet Examiner Toolkit was able to recover some of the artefacts from Facebook, Twitter, and Instagram, it was not sufficient on LinkedIn and Bayt forensic investigation. Thus, it performed the worst among three tools. IXTK also had several other concerns which will be discussed in the following section.

5.2 DISCUSSION

The investigations and testing conducted for this research revealed significant findings. The process started by setting up the testing environment for the two case scenarios, and then to the reconstructed evidence from each digital forensic tool. Some significant strengths and weaknesses of each tool were also identified. Section 5.2.1 discusses how the environment setup effected the forensic investigation, and reflects on the literature reviewed in Section 2.3.7. Section 5.2.2 discusses each of the selected digital forensic tool's capabilities, strengths, and weaknesses, and deliberates on how the recovered data from each tool can be considered admissible evidence in courts. Section 5.2.3 gives method recommendations, and advice for the digital forensic investigator.

5.2.1 Discussion of the Case Scenarios Environment

The case scenarios presented in Section 4.2.7.1 and Section 4.2.7.2 were developed to be similar to real world scenarios as possible. The first phase was to learn how each OSNS operated, and the possible data that can be extracted from each site; which then can be used as forensic evidence. An appropriate testing environment was setup to simulate the data recorded in the controlled data. In both case scenarios, the target machine was initially zeroed, and then Windows 7 operating system was installed, along with the three browsers identified in Table 4.3. The controlled data posted on each OSNS, and on each browser were recorded at the time of performing each post, along with the exact date and time. Although this phase was not part of answering the

main research question, it is crucial to have a proper environment setup. It was also crucial to know what exactly has been posted, and on which browser. Thus, the investigator is aware of what is expected to be recovered by the three extraction tools. For example, when the documented Facebook chats performed on the three browsers, all the tools recovered some of the messages on Firefox and Chrome, but not all the expected messages were extracted. Thus, they were considered as a fail in the test plans. On the other hand, IEF was the only tool that extracted messages sent using IE. Thus, it is considered better than the other in terms of extracting Facebook messages.

The literature reviewed in Chapter 2 discussed the viable sources that lead to crucial evidence in OSNSs. In Section 2.3.7, Mulazzani, Huber and Weippl (2012) grouped these sources into five social footprints with other users, for example, friend lists, connected groups, communication methods between individuals such as private messages, comments, likes, pictures and videos posted online, along with people tagged with the posts, date and times of the activities. Based on the conducted investigation, these sources were proven to be viable, as they assisted in the forensic investigation to identify the suspects, the activities, and times of activities. Moreover, the authors stated that these social artefacts cannot be recovered from the target's HD, and the information is only stored at the OSNS's provider. However, testing results show that OSNSs forensic evidence can still be found without the need of the OSNS's provider, and some activities and social artefacts such as photos, and videos can be recovered from target's HD. Mutawa, Awadhi, Baggili and Marrington, (2011) stated that most often, some information may be stored in RAM, which may be difficult to recover depending on the computer status when seized. Based on the conducted investigation, it has been proven that viable forensic evidence were only recovered from RAM and pagefile.sys. However, the target machine in both case scenarios was not turned off during seizure, meaning that an acquisition of RAM and pagefile.sys were performed in forensic manner. It is not established if the recovered evidence from RAM and pagefile.sys can still be recovered if the machine was powered off during seizure. Mutawa, Awadhi, Baggili and Marrington, (2011) also stated that web browser files are potential sources of forensic evidence, since they are used to connect with OSNSs. Social artefacts can be located from different places including browsing history, cookies, cache files, depending on the type of browser, and the version used. Based on the findings, crucial information were recovered from both case scenarios from the browser files. Moreover, it has been shown that browser type and version

affect the possibility of extracting forensic evidence from OSNSs. For example, the only extracted LinkedIn messages were when the suspect was using Firefox. The following section discusses the capabilities, strengths, and weaknesses of the three selected digital forensic tools, based on the testing reported in Chapter 4.

5.2.2 Discussion of the Findings for Tool Evaluation

The selected digital forensic tools share some common capabilities, and features. However, each of the selected tool has its own strengths, and weaknesses. This section discusses these capabilities, strengths, and weaknesses for each tool, how each tool performed, and describes the challenges encountered with using the three tools during the testing. This section also discusses how the forensic evidence recovered from each tool can be used as admissible evidence in courts.

5.2.2.1 Belkasoft Evidence Center

The official webpage for Belkasoft states that Belkasof Evidence Center can search, analyse, store and share digital evidence found inside computers, and mobile phones, and it has the ability to work with different OS including Windows, Mac OS X, and Unix-based systems. The supported forensic images that can be examined includes E01, L01/Lx01, FTK, DD, SMART, Virtual machines, RAM memory dumps, Hibernation files, and pagefile.sys.

In Belkasoft, when a new case is created by including the case name, and investigator's name. To add evidence to the case, the user specifies the data source the investigator wants to analyse. The data sources are categorized into 6 types: Drive image file or virtual machine disk, logical drive, physical drive, mobile backup files, Live RAM image file (pagefile.sys, hibernation file, memory dump), and a specific folder to scan it for evidence such as users folder. After adding the source, Belksoft lists the artefacts, and types of data that the investigator wants to search for, which includes social networks, instant messengers, and various types of browsers. Once the user clicks finish, the tool will start searching and extracting data. The software then completes the analysis and presents the findings in the date tree pane, which is also categorized into the artefacts selected for searching. The time that Belkasoft takes to extract and analyse the data deepens on the size of the forensic image created for examination. For the RAM image, test1_Livememory_suspect.001, it took about 8 minutes to finish, while for HD image: IMAGE-suspect1-harddrive.E01, it took 50

minutes, which is considered efficient comparing to IXTK. However, IEF was the fastest in terms of processing the evidence and presenting the results.

Data carving was indispensable technique while searching for volatile data and destroyed evidence. The word ‘Carving’ refers to a specific approach to locate forensic evidence. The carving method is based on a signature search analysis, which means that it doesn’t only rely on the image file systems to locate the evidence, but it also reads the content of the image in much lower level approach. The data blocks in the image are reviewed and compared against a database of known artefacts format. If the algorithm finds a match, then it assumes that a specific data block holds a file header. Based on the testing results, Belkasoft was able to recover evidence by searching within a particular sequence of bytes, and characteristics signatures. Belkasoft Hex Viewer window allowed the investigator to look for binary data, for example in Figure 4.13, the chat message was already presented in the item properties. However, additional metadata were only presented in the Hex Viewer window. It included the relationship between the suspect and the other user, gender, timestamp, and attachments status. There was no complication, nor major challenges during the interaction with Belkasoft, as most of the features were clearly described in the Belkasoft user manual. For example, searching for keywords or phrases, built-in SQLite database viewer, and Registry viewer.

Bookmarking evidence was easy as the investigator can first create a new bookmark folder, and then select one or more items to be bookmarked. Similarly, the advanced reporting features was effective. Belkasoft offers various reporting formats such as HTML, XCML, PDF, DOCX, and CSV. It also offers advanced options of how the report should look like. Thus, Bookmarking and reporting features offered by Belkasoft are better than the other two tools.

A fascinating feature called “Export for Evidence Reader“, which permits the investigator to export a particular case that contains forensic evidence to a separate portable evidence file, allows the case to be accessed from any PC even if Belkasoft is not installed on that machine. The evidence reader provides a read-only access to the information, in order to preserve the integrity of the case, and the items within the case. In addition bookmarking and reporting features can be performed on the Evidence Reader.

As can be seen from the comparative analysis, and sub-questions that Belkasoft was the most powerful tool in finding evidence from Twitter, and Instagram.

It is the only tool that extracted Twitter posts (Tweets) in plaintext without the need to click the link of the tweets. In the real life scenario, a particular post may be deleted, or even the suspect's account may be removed by a suspect's assistant. Thus, the evidence will not be recovered or known if it was only presented as a URL link. Moreover, admissibility of evidence can be rejected if the evidence was not presented with its source reference. Belkasoft was better than the other tools in locating and presented the evidence references.

Although the ability to extract forensic evidence from OSNSs was satisfactory, there is scope to improve. For example, there is no built-in acquisition features within the tool. Instead the vendors offer another separate tools, namely Belkasoft RAM Capture, and Belkasoft Computer Acquisition Module, which enable the forensic investigator to acquire HD, and it supports SATA/IDE/SSD/USB storage media. It would be very helpful if RAM and HD acquisition are built-in features in Belkasoft Evidence Center instead of buying more software from the vendor.

5.2.2.2 Internet Examiner Toolkit

IXTK is an offline digital forensic tool that gathers evidence from a wide range of artefacts. In Section 2.5.3, it is reported that IXTK is able to recover browser activities artefacts, multimedia files, keyword artefacts, and OSNSs activities. According to SiQuest (2015), IXTK is able to locate and analyse browser cache, history, cookies for several browsers including Internet Explorer, Safari, Firefox, Opera, and Google Chrome.

The investigations conducted and reported in Chapter 4 show that IXTK has several powerful features, for example the investigator was able to locate and view picture evidence as a thumbnail using the built-in Gallery viewer. Facebook Messages extracted from IXTK can be viewed from the fully featured integrated Hex viewer.

IXTK provides another feature called Evidentiary Value Scoring (EVS) system, with EVS and its 6-point scale, it made it possible for the researcher to associate a weight or value of importance to individual items and records within case files. This approach provides yet another method of organizing internet based evidence.

Similar to Belkasoft, IXTK was able to perform data carving. However, before performing carving, IXTK has to take an additional step to proceed with searching and analysis. IXTK is the only tool that required disk image mounting. Both RAM and HD

images for this research had to be mounted as a virtual drive. IXTK already has a built-in mounting capabilities for common disk image files types E01, .Ex01, .Lx01, .L01, SMART, and Raw.

As shown in Chapter 4, Figure 4.11, IXTK doesn't include Firefox and Chrome browser activity artefacts, as the browser to be selected for carving is IE. Although, some activities performed using Firefox and Chrome were recovered, the source of the evidence were incorrectly presented in the IE browser files. This indeed affects the admissibility of the recovered evidence.

The relevant artefacts were selected to be searched such as browser artefacts, and social networking artefacts. IXTK took too much time to process, search, and present the evidence. For example, the first case created to test a RAM image, test1_Livememory_suspect.001, it took 26 minutes to finish, while for HD image: IMAGE-suspect1-harddrive.E01, it took about 18 hours to finish. In real life scenarios, the forensic investigator will have no clue of what type of evidence they are looking for, and which artefacts should be selected. Thus, they will select all the possible artefacts to be searched, due to this, the time to process would be much longer than 18 hours. This is one of the most challenging issues the investigator has to encounter during IXTK examination.

Another issue encountered is creating a bookmark folder. When the investigator creates a new bookmark folder, then adds a record to the created folder, an alert message popups and displays the following message:

(Exception of type 'system.outofMemoryException' was thrown)

Then the tool freezes, and has to be restarted. Once restarted, the bookmark folder with the record is already presented in the data pane. This bug has been sent to the software's technical support, and they confirmed the bug. The vendor has issued an update after fixing this issue. The other problem which needs to be improved is moving from one record to another. Sometimes the tool loads records slowly, with the popup loading message taking 1 to 2 minutes then the selected records are presented. This issue was also challenging for the investigator, because there are vast amounts of evidence that the investigator is looking through, and it takes too much time to find the evidence from the records. The slow loading issue has increased the time use of the forensic investigation in both case scenarios.

5.2.2.3 Internet Evidence Finder

Similar to previous two tools, Internet Evidence Finder (IEF) can recover OSNSs artefacts, and various web browsing activities. According to the vendor's website, IEF is also able to examine and search for evidence from various types of mobile phones including iOS, Android, and Windows-powered smartphones and tablets. There are more than 165 types of mobile artefacts that can be discovered using IEF. This research was based on computer based investigation and hence, the ability that IEF can offer for mobile forensic investigation is out of scope.

When opening IEF, the tool presents several icons indicating the different sources of evidence that IEF accepts for analysis, which are; 1) Drives, 2) Files & Folders, 3) Images, 4) Volume Shadow copies, and 5) Mobile. This research used the Images option. The search option provided by the tool also consists of five options which are Quick search, Unallocated Clusters Only, Full Search, Files and Folders Search, and Full Search on Sector Level. The search options used for this research are Full Search, and Full Search on Sector Level. After adding the image, and selecting the search type, the investigator has to select artefacts that need to be searched, which is similar to the previous tools. Then the last step is to setup a case folder which includes destination path, case folder name, case number, examiner's name, and configuration of the keyword search.

Keyword searching alert is one of the most fascinating features that helped the investigator during analysis. This feature is based on writing one or more keywords before the tool starts to search for evidence. During searching, the tool alerts the investigator via (Email, or audible options) about the found matches. For example, in the first case scenario the keywords lists are Smith, Volkov, Message, Instant, Twitter, Facebook, Tweets, Photo, and Video and so on, were written to the search alerts. This feature was working well, and saved a lot of time as the recovered evidence from search alert can be viewed and examined while the tool is still searching for evidence from the entered image.

IEF is much faster than the other two tools in terms of processing, and searching evidence from the entered images. For example, in the first case scenario the image test1_Livememory_suspect.001, took about 3 minutes to finish. For the second case created for HD examination, IMAGE-suspect1-harddrive.E01, took about 34 minutes to finish.

Like the other two tools, IEF provides a user-friendly interface, even for non-technical person. The tool can be understood easily without complication. The help feature provides straightforward information that can be followed. IEF is also very fast in terms of viewing items in the data pane, and moving from one category to another in the main tree pane.

IEF was the most sufficient tool among the three in terms of finding Facebook messages sent and received by the suspect. All the messages were extracted from the Swap file. IEF extracted some of the messages sent using Firefox and Chrome which was previously extracted by Belkasoft and IXTK. However, it is the only tool that was able to extract all the messages sent and received using Internet Explorer, along with the exact date and time of the messages. All artefacts locations found on IEF were mapped to either a physical sector offset or file offset. IEF was also the best tool in terms of findings the times of posted/performed activities, which matches the date/time recorded in the controlled data. This is a crucial capability, as in a real life scenario, the exact date and time are important to understand a particular case. Sometimes, if the date and time of the recovered evidence were not identified, the evidence may not be helpful, as the investigator will not have a clue on when a particular activity was performed by the suspect. Similar to Belkasoft, IEF enables the investigator to create an IEF portable case which can be shared with other investigators. The IEF portable case is simply a copy of the case file containing the recovered evidence from the image, the portable case can be viewed without the need of IEF licence. Thus, it can be viewed from any PC. Similar to the previous two tools, IEF provides a Hex and Text Viewer capabilities, which are essential parts of the forensic examination that assist in conducting additional analysis beyond the refined results provided by IEF.

There were some weaknesses encountered when using IEF. The first weakness is the bookmarking procedure. The investigator cannot create a bookmark folder (like in Belkasoft and IXTK). Instead, when a particular record need to be bookmarked, the investigation should select that record and click on bookmark, then the record will go directly to a bookmark list. However, this may cause a complication during a forensic investigation. As some investigators may want to bookmark particular records to a separate folder, for example bookmark folder named (Evidence Found from Firefox) and so on. Another weakness is IEF reporting capabilities. Although there were a choice of reporting formats that can be generated, the tool cannot create one report file containing all the artefacts. For example, if the bookmarked records are Facebook

Chats, Facebook URLs, Social Media URLs artefacts. When selecting all of the three artefacts to be exported into a report, IEF creates three different reports, one for each artefact. Thus, the investigator had to put them together into one report manually.

5.2.3 Method Recommendations

The research findings from the research phases showed that common functionalities and features are shared on the three digital forensic tools. The findings have also revealed the different capabilities from each tool. The testing was conducted with the five phases defined earlier in Figure 3.8. Based on testing and findings, the proposed research phases were proven to be practicable for digital forensic tools evaluation associated with the investigation of online social networking sites.

The second phase of the research phases has adapted the recommended guidelines for tool validation testing developed by SWGDE. The main objective of this approach, is to test and evaluate the selected tools, in order to determine their capabilities, techniques, and features function correctly and as intended. This approach has been discussed in Section 3.1.3. During developing this phase, the researcher has precisely described the purpose and scope of each test plan, the requirements that need to be fulfilled, a description of methodology, and the expected results, and finally developing the test scenarios. This method has guided the researcher during the testing experimentation, as there were 12 test plans, 3 digital forensic tools, 3 browsers, and examination of different sources which are RAM, Pagefile.sys, and HD. It would be much more difficult to control if this approach was not adapted. During reconstruction and analysis, there was not any difficulty handling big data, nor complications. This is because each test plan has its own case created on each digital forensic tool, and each test plan is described before the testing begins. Based on research findings, the SWGDE approach for validation testing works effectively with online social networks investigation.

The forensic guideline model by Nouredin, Hashem and Abdalla (2011) also has been adapted in order to ensure that the forensic investigation and the research findings presented in Chapter 4 proceeded in a forensically trusted manner. The six phases of the digital forensics are discussed in Section 3.1.1. According to Nouredin, Hashem and Abdalla (2011), the goal of this phase is to find, collect, and examine different digital sources, and artefacts in order to reconstruct forensic evidence, and draw a conclusion of determining criminal activities. Although criminal activity can

possibly be identified, the reconstructed evidence can also assist in determining what happened, how it happened, what was the time and date, where the evidence was collected from, and possibly who has done it (Noureldin, Hashem and Abdalla (2011). Based on digital forensics examination on Sections 4.3.2 and 4.4.2, this method is suitable for online social networks investigation.

Comparative analysis method has assisted the researcher in understanding the types of evidence that can be collected from the selected OSNSs when using the selected digital forensic tools. This method has certainly assist the researcher in realizing each tool's capability, the four tables presented in Tables 4.5 to 4.8 can be used as scope for developments by the tools' vendors.

Although browser forensic technique can be used to recover a large portion of forensic evidence on a user's HD. RAM and pagefile.sys could be the only source of some potential evidence found from OSNSs. However, it depends on the system status once found, and also it depends on how the collection, acquisition, analysis were performed. SWGDE have recommended computer forensics best practices which includes handling of powered-on systems, acquisitions of evidence, evidence packing and transportation, forensic analysis and examination, and documentation. These phases should be followed precisely in order to maintain the admissibility of the evidence. Thus digital forensic investigators have to be aware of these matters.

5.3 CONCLUSION

In this Chapter, a comprehensive discussion was made based on the research findings presented in Chapter 4. This Chapter has answered the sub-questions formulated in Chapter 3, and also tested the hypotheses with arguments made for and against to draw a conclusion on whether each hypothesis is accepted, rejected, or indeterminate. Based on all the above, the research main question was answered and discussed. The difficulties encountered during using the three digital forensic tools, and the tool's strengths and weaknesses were also discussed, and a method recommended for digital forensic investigators was delivered.

Online Social Networks forensics is a still a relatively new to the field of digital forensics. There are currently no tools designed and specified for OSNSs forensic investigation. Some of the current digital forensic tools can still extract the OSNSs artefacts, and recover admissible forensic evidence. In this research, the selected

digital forensic tools share some of the capabilities, and features. However, each tool has its own ability in extracting forensic evidence from the selected OSNSs. Moreover, the research findings have confirmed that OSNSs artefacts can be recovered without the need of OSNSs' providers, and the recoverable evidence is not always stored on the target's HD. This can be seen from the findings that crucial evidence such as Facebook Messages, Tweets, and Wall posts, can be recovered only from RAM and pagefile.sys. Furthermore, the research has confirmed that the web browser type used by the suspect has influenced the scope of evidence extracted from OSNSs. Some evidence could be found from one browser, but the same evidence may not be found when it is posted using other browsers. Although, the ability to extract forensic evidence from OSNSs was satisfactory, the selected digital forensic tools cannot extract the entire evidence posted on each OSNS. Thus, collecting evidence from online social networks is still a developmental challenge for the digital forensic field.

Chapter 6 concludes this thesis by summarising the research findings. The limitations of this research will be discussed, and recommendations for future research will be presented, in order to provide a link for further research in the field of online social networks forensics.

Chapter 6

Conclusion

6.0 INTRODUCTION

This Chapter is to conclude the entire thesis project based on the research findings presented in Chapter 4, and the discussion conducted in Chapter 5. There were several limitations and difficulties encountered, which are presented in this Chapter in order to identify the gaps in the OSNSs forensic research. These gaps can be essential opportunities for future research that can assist in developing the fields of online social network forensics, and digital forensic tools.

In Chapter 6, a summary of research and research findings is presented in Section 6.1. Followed by the limitation of testing and research in Section 6.2. Recommendations for future research based on the testing environment, investigation findings, and discussion made in Chapter 5 will be delivered in Section 6.3, in order to provide further research focus in this area.

6.1 SUMMARY OF RESEARCH

In this research, the five OSNSs selected for the investigation were based on their popularity. Three most popular browsers were installed in order to simulate data on different browsers, and to find whether the scope of the recovered evidence may vary depending on the type of browser used. The digital forensic tools were selected based on literature reviewed in Chapter 2. The main objective of this research is to examine, and compare the capabilities of the selected digital forensic tools when extracting forensic evidence from the selected OSNSs. Through background research conducted in Chapter 2, and similar studies reviewed in Chapter 3, a comprehension was gained of how to conduct a forensic investigation for online social networks, and how to evaluate digital forensic tools in a forensically trusted manner. The research phases in Figure 3.8, and data requirements in Section 3.3 were developed in order to be followed during the investigation, and to answer the research questions, and research hypotheses. A method of tool validation testing proposed by SWGDE was adopted, in order to evaluate the selected digital forensic tools. Based on SWGDE guidelines, test

plans have been developed, which include the purpose, scope, requirements, methodology and test scenarios for each test plan. The forensic guideline methodology proposed by Noureldin, Hashem and Abdalla (2011) was adopted in order to ensure that the OSNSs forensic investigation will be conducted in a forensically trusted manner.

A comparative analysis was the last approach performed, which compared the control data posted on each OSNSs using each browser, with the evidence reconstructed by each digital forensic tool. The objective of the comparative analysis was to identify and recognize the similarities, differences, performance, and scope of each of the selected tools in terms of extracting forensic evidence from OSNSs. The evidence was to be admissible to a court of law, and to assist in answering the research questions and hypotheses. There were some changes and modifications encountered during the testing which are discussed in Section 4.1. RAM, and pagefile.sys acquisition, examinations, and analysis have been added to the investigation in both case scenarios. Thus, more test plans were developed in order to maintain control, to prevent complexity of big data, and to accurately determine the source of the recovered evidence.

The findings showed that all the three digital forensic tools have succeeded in recovering some of OSNSs artefacts, which can be used as forensic evidence against the suspects Smith in first case scenario, and Jason in the second case scenario. The findings show that forensic evidence recovered from OSNSs can vary depending on the several factors which are; the browser used by the suspect, the source of evidence to be examined (RAM, pagefile.sys, HD), and the digital forensic tool used for examination. Findings show that some volatile data cannot be found from the hard drive, and can only be found from the acquired RAM, or pagefile.sys such as Facebook messages. Examination and analysis has been conducted, and the findings showed that the selected digital forensic tools cannot recover the entire amount of data posted on each OSNS. The artefacts that cannot be recovered from Facebook are status updates (wall posts), and posts on a friend's wall. The artefacts that could not be recovered from Twitter are Tweets on friend's wall, and direct messages. The artefacts that could not be recovered from LinkedIn are status updates, comments made on pictures, and likes. Although these activities could not be recovered, there are other crucial activities recovered from each OSNS. This research found that private messages (to a friend) on

Facebook, LinkedIn, and Bayt are possible to be recovered, unlike private messages sent on Twitter which was not possible to be recovered.

Research found that Belkasoft Evidence Center is better than the other two tools when conducting a forensic investigation on Twitter and Instagram. Although IEF and IXTK succeeded in recovering the uploaded pictures on twitter, and viewed Instagram pictures on the Instagram website. Belkasoft is the only tool that was able to recover the retweets made by the suspect, and the shared Instagram pictures on Twitter. Moreover, Belkasoft and IEF both were able to extract wall posts made on Twitter (Tweets). However, Belkasoft reconstructed these tweets in forms of plaintext (see Figure 4.23), on the other hand, IEF did not reconstruct the tweets in plaintext, and instead gave a URL link to the tweets which need to be accessed by the investigator in order to view what has been written by the suspect. This may cause a loss of evidence as it can be deleted or removed by anyone who intends to help the suspect by destroying forensic evidence.

Although the average of recovered Facebook evidence is 50% using Belkasoft, and 19% using IXTK, and 42% using IEF, this does not mean that Belkasoft is better than the other two tools. IEF is the only tool that was able to recover all the private messages sent using Internet Explorer. Moreover, the only advantage that Belkasoft has over IEF on Facebook investigation, is that it was able to recover the Video and Picture posted using Internet Explorer, and the shared Instagram picture from both RAM and HD sources. IEF recovered the posted Video and the Picture only from the hard drive, and only private messages from RAM. This has made Belkasoft better in terms of the average number of evidence items extracted but not the type of evidence extracted from Facebook. Thus, research found that Internet Evidence Finder is better than the other two tools when conducting a forensic investigation on Facebook.

Both Belkasoft and Internet Evidence Finder has the same average percentage of recovered evidence from LinkedIn which is 20%, and both tools were able to recover the private message sent using Firefox, and no private messages were recovered from the other browsers. Moreover, Belkasoft had the ability to extract the suspect's account credentials which are Username, password of the LinkedIn account. Thus, Belkasoft is more preferable and better than the other two tools when conducting a forensic Investigation on LinkedIn.

The average number of evidence recovered from Bayt using Belkasoft was 29%, and 0% using IXTK, and 54% using IEF. Although, both IEF and Belkasoft were

able to recover posted questions, posted answers, and direct messages. IEF is the only tool that was able to reconstruct the recommendations made by the suspect. Thus, IEF is better than Belkasoft for Bayt forensic investigation.

Internet Examiner Toolkit has reconstructed vital forensic evidence from the first case scenario (Facebook, Twitter, and Instagram). The reconstructed evidence were incorrectly presented in different locations, as some of the posted data using Firefox, and Chrome were recovered, but were presented in IE history files. This is due to the fact that IXTK did not include Firefox and Chrome artefacts to be searched when conducting data carving (See Figure 4.11). In the Second case scenario (LinkedIn, Bayt), IXTK could not recover any evidence from RAM and pagefile.sys, and was able to recover one evidence item from the target's HD, which is the uploaded picture on LinkedIn using IE. Thus, the IXTK ability to extract forensic evidence from LinkedIn and Bayt was unsatisfactory

6.2 LIMITATION OF RESEARCH

In Chapter 3, Section 3.4 there were several limitations discussed, which presented the areas that are out of the scope for the conducted research. These limitations were addressed based on research methodology and data requirements. The testing procedures, and findings show that the predicted limitations in Section 3.4 are still apparent and significant during and after the investigations. This section will discuss and summarize these limitations, the limitations encountered during the testing, and limitations that were found from the findings of this research will also be presented in this Section 6.2.

Firstly, as discussed in the literature that there is still a lack of evidence extraction tools designed only for online social network investigations. In this research, the selected digital forensic tools have a wide verity of features, capabilities, and functionalities which were not tested because they were not relevant to the proposed research. These features include cloud storage, mobile forensic analysis, other browsers, peer-to-peer software, and encrypted files and volumes. Thus, the results of this research are limited to the investigation of the selected OSNSs (Facebook, Twitter, Instagram, Bayt, and LinkedIn), and is limited to the selected browsers listed in Table 4.3. Although, this research focused on three digital forensic tools, the other tools such as Encase were not evaluated due to the time constraints. It

was not possible to test all digital forensic tools within the specified time frame for this research.

The scope of this research was to test 5 selected online social networks. There were many other social networks, which are widely used, such as Google Plus, YouTube, Bebo, and Orkut and so on. The selected digital forensic tool documentation stated that they can recover artefacts from these social networks. However, due to each social network site's functionality, and architecture, the scope of recovered evidence varied. Another limitation is that most of the popular OSNSs currently can be accessed via devices such as smartphones, and PDAs, and many users may access their online account from different digital devices. In a real live scenario, if the digital investigation was only applied on a suspect's PC, some evidence might not be recovered because it was not posted or performed using the PC, but using another digital device such as a mobile phone. Moreover, the conducted experiments, and findings are only limited to the Windows 7 operating system. Tools and techniques for extracting forensic evidence from different platforms will vary, because of the variation in file structure of each system.

During testing-setup, the laptop used for the experimentation is equipped with only 2 GB of installed memory (RAM), which is considered very small comparing to newer technology. The size of RAM may have affected the amount of recovered evidence during the forensic investigation, moreover, when RAM is full the data is swapped to the pagefile.sys which was also examined, and it was the only source of crucial evidence such as Facebook chat. On the other hand, it can be argued that, although RAM was small in size, the selected digital forensic tools were still satisfactory in extracting some of the forensic evidence. However, if the RAM size was bigger, the scope of evidence recovered from RAM and pagefile.sys would have been more. The limitations provided in this section present directions for further research which will be summarized in the following section.

6.3 FUTURE RESEARCH

In this research, three digital forensic tools have been evaluated for extracting forensic evidence from five OSNSs, by analysing different artefacts, and different sources of evidence. Forensic analysis for each tool and comparisons have been performed. For further research other digital forensic tools should proceed by tests using the same

proposed methodology, in order to compare the findings with this research. Future research could also focus on other browsers such as Safari and Tor, and different operating systems such as Linux and Mac platforms to test the different file structures.

The dynamic nature of OSNSs is one of the main challenges in the forensic investigation, as the posts and activities can be easily deleted. In this research, all the posts and activities performed and documented in the controlled data, are not deleted or removed (Appendix 1 & Appendix 2). It is vital to determine whether the selected tools can still recover the deleted data from OSNSs. Thus, future research could focus on recovering the deleted activities from the selected OSNSs. Assuming a suspect has posted data on Facebook, Twitter, Instagram, LinkedIn, and Bayt for example, then all the posted data including the types of data used for this research on each OSNS in Table 4.2 can be deleted and a forensic recovery attempted. This would cover the scenario that the forensic team arrives for seizure but the suspect has deleted or found ways of deleting potential evidence. Based on these research findings, it is expected that the selected digital forensic tools can still recover some of the artefacts and activities, even if they are deleted by the suspect from their OSNSs accounts. This is because some of the data will have already been swapped into the pagefile.sys, and may not be removed from the pagefile.sys, even if they are deleted data from the website. Likewise, browser files may store artefacts when performing the posts, and may be recovered even if the posts are deleted. Although, OSNSs forensic investigation is challenging, using digital forensic tools to recover the deleted activities is worth researching.

Future research can also focus on live memory examination and analysis, since RAM and pagefile.sys analysis can recover valuable artefacts that may not be recovered from the system's hard disk drive. Although, in this research, the environment setup for the target's machine contains only 2 GB of installed memory (RAM), the selected forensic evidence extraction tools recovered vital evidence that can be used for prosecutions. The researcher expects that the type and amount of evidence recovered from RAM and pagefile.sys can be effected by the size of RAM installed on the system. So, future research can be focused on the relationship between the size of RAM used on the target's system, and the recovered evidence from each tool. It is suggested to use 2 laptops, one is equipped with 2GB RAM, and the other one is equipped with 16GB of RAM or more, then the activities are to be posted on each OSNS. Memory dump and acquisition of pagefile.sys are then performed, and

images are entered to the three digital forensic tools for examination and analysis. The outcome of this research should assist in determining how OSNSs volatile data is stored on RAM, and when they are swapped into pagefile.sys, and to determine the significance of the RAM size when conducting a live investigation on online social networks.

Furthermore, evidence legitimacy and standardization of social networks forensic investigation are crucial areas that need to be addressed for future research. Although, some standards have been proposed for OSNSs forensic investigation there is still no international standard model that can be followed. Future research should focus on reviewing all of the previously proposed standards, and to develop a comprehensive standard that can be applied on forensic investigation of any online social network. This standard should prevent major ethical issues during the investigation such as invasion of privacy, dishonest or immoral investigations of OSNSs. The standard should also minimize the number of legislation and OSNSs forensic investigations laws over the world in order to resolve jurisdictional issues across borders. This can be achieved by making the developed standards available for reviews by the digital forensic community, allowing continuous development in order to come up with a final standard which should be internationally accepted, and applied.

REFERENCES

- Abbas, N. (2015). 'Gang rape' goes viral, three youths arrested - *The Times of India*. Retrieved 24 March 2015, from <http://timesofindia.indiatimes.com/city/bareilly/Gang-rape-goes-viral-three-youths-arrested/articleshow/46088226.cms>
- Abdalla, A., & Yayilgan, S. (2014). A Review of Using Online Social Networks for Investigative Activities. In G. Meiselwitz (Ed.), *Social Computing and Social Media* (Vol. 8531, pp. 3-12): Springer International Publishing. Retrieved from http://dx.doi.org/10.1007/978-3-319-07632-4_1. doi:10.1007/978-3-319-07632-4_1
- AccessData. (2015). Forensic Toolkit (FTK) Computer Forensics Software. Retrieved 26 March 2015, from <http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk>
- Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, 5(1), 118-131.
- Alothman, A. B. (2013). *A survey of social media users in Saudi Arabia to explore the roles, motivations and expectations toward using social media for social and political purposes* (Order No. 1541900). Available from ProQuest Dissertations & Theses Global. (1419422776). Retrieved from <http://ezproxy.aut.ac.nz/login?url=http://search.proquest.com/docview/1419422776?accountid=8440>
- Alwagait, E., Shahzad, B., & Alim, S. (2014). Impact of social media usage on students academic performance in Saudi Arabia. *Computers in Human Behavior*. doi:<http://dx.doi.org/10.1016/j.chb.2014.09.028>
- Al-Zaidy, R., Fung, B. C. M., Youssef, A. M., & Fortin, F. (2012). Mining criminal networks from unstructured text documents. *Digital Investigation*, 8(3-4), 147-160. doi:<http://dx.doi.org/10.1016/j.diin.2011.12.001>
- Ashbaugh, D. Ridgeology: Modern evaluation friction ridge identification, *Journal of Forensic Identification* (1991) 41:16-64.
- Athanasopoulos, E., Makridakis, A., Antonatos, S., Antoniadis, D., Ioannidis, S., Anagnostakis, K. G., & Markatos, E. (2008). Antisocial Networks: Turning a Social Network into a Botnet. In T.-C. Wu, C.-L. Lei, V. Rijmen, & D.-T. Lee (Eds.), *Information Security* (Vol. 5222, pp. 146-160): Springer Berlin Heidelberg. Retrieved from http://dx.doi.org/10.1007/978-3-540-85886-7_10. doi:10.1007/978-3-540-85886-7_10

- Attia, A. M., Aziz, N., Friedman, B., & Elhusseiny, M. F. (2011). Commentary: The impact of social networking tools on political change in Egypt's "Revolution 2.0". *Electronic Commerce Research and Applications*, 10(4), 369-374. doi:<http://dx.doi.org/10.1016/j.elerap.2011.05.003>
- Bachrach, Y., Kosinski, M., Graepel, T., Kohli, P., & Stillwell, D. (2012). Personality and patterns of Facebook usage. *Proceedings of the 4th Annual ACM Web Science Conference*, Evanston, Illinois. doi:10.1145/2380718.2380722
- Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, 2(2), 147-167. doi:10.1016/j.diin.2005.04.002
- Beebe, N. L., & Clark, J. G. (2007). Digital forensic text string searching: Improving information retrieval effectiveness by thematically clustering search results. *Digital Investigation: The International Journal of Digital Forensics & Incident Response*, 4, 49-54. doi:10.1016/j.diin.2007.06.005
- Belkasoft. (2015). Leading Digital Evidence Extraction Software for Computer Forensic Investigations. *Belkasoft.com*. Retrieved 26 March 2015, from <http://belkasoft.com/en/ram-capturer>
- Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210-230. doi: 10.1111/j.1083-6101.2007.00393.x
- Broillet, A., Kampf, C., & Emad, S. (2014, 13-15 Oct. 2014). What and how do we learn from LinkedIn forums? An exploratory investigation, in *Professional Communication Conference (IPCC), 2014 IEEE International*, 1-14. doi:10.1109/IPCC.2014.7020339
- Caloyannides, M. A., Memon, N., & Venema, W. (2009). Digital Forensics. *Security & Privacy, IEEE*, 7(2), 16-17. doi:10.1109/MSP.2009.34
- Carrier, B. D. (2009). Digital Forensics Works. *IEEE Security & Privacy*, 7(2), 26-29. doi:10.1109/MSP.2009.35
- Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, 2(2), 1-20.
- Carrier, B., & Spafford, E. H. (2005). Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence. In *Proceedings of the 2005 Digital Forensics Research Workshop*.

- Carter, H. L., Foulger, T. S., & Ewbank, A. D. (2008). Have You Googled Your Teacher Lately? Teachers' Use of Social Networking Sites. *Phi Delta Kappan*, 89(9), 681-685. doi:10.1177/003172170808900916
- Casey, E. (2004). *Digital Evidence and Computer Crime* (2nd Ed). Forensics Science, Computers and the Internet, 2nd ed., Elsevier, Amsterdam.
- Casey, E. (2010). *Digital evidence and computer crime: forensic science, computers and the Internet*. London: Academic Press.
- Casey, E. (2011). *Digital evidence and computer crime: forensic science, computers and the internet* (3rd Ed.). Waltham, MA: Academic press.
- Cassa, C. A., Chunara, R., Mandl, K., & Brownstein, J. S. (2013). Twitter as a Sentinel in Emergency Situations: Lessons from the Boston Marathon Explosions. *Public library of science, Currents Disasters*, 5, doi:10.1371/currents.dis.ad70cd1c8bc585e9470046cde334ee4b
- Chen, L., Xu, L., Yuan, X., & Shashidhar, N. (2015). Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges. *Computing, Networking and Communications (ICNC), 2015 IEEE International Conference*, 1132-1136. doi:10.1109/ICCNC.2015.7069509
- Cheung, C. M. K., & Lee, M. K. O. (2010). A theoretical model of intentional social action in online social networks. *Decision Support Systems*, 49(1), 24-30. doi:10.1016/j.dss.2009.12.006
- Civie, V., & Civie, R. (1998). Future technologies from trends in computer forensic science. *Information Technology Conference, 1998 IEEE*, 105-108, doi:10.1109/IT.1998.713392
- Cohen, F. B. (2010). Fundamentals of Digital Forensic Evidence. In *Handbook of Information and Communication Security* (pp. 789-808). Berlin Heidelberg: Springer.
- Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
- Duggan, M., Ellison, N.B., Lampe, C., Lenhart, A, and Madden, M. (2015). Social Media Update 2014, *Pew Research Center, January 2015*. Available at: <http://www.pewinternet.org/2015/01/09/social-media-Update-2014/>
- Dwyer, C. (2007). Digital Relationships in the "MySpace" Generation: Results from a Qualitative Study. *System Sciences, 2007, HICSS 2007. 40th Annual Hawaii International Conference*. doi:10.1109/HICSS.2007.176

- Evans, M. (2015). Police facing rising tide of social media crimes. *The Telegraph*. Retrieved November 25, 2015, from <http://www.telegraph.co.uk/news/uknews/crime/11653092/Police-facing-rising-tide-of-social-media-crimes.html>
- Facebook, 2014, *Facebook Reports Fourth Quarter and Full Year 2014 Results*. Retrieved from <http://investor.fb.com/releasedetail.cfm?ReleaseID=893395>
- Forensic.belkasoft.com. (2015). *Belkasoft - Leading Digital Evidence Extraction Software for Computer Forensic Investigations*. Retrieved 30 March 2015, from http://forensic.belkasoft.com/en/bec/en/evidence_center.asp
- Gao, Y., Wang, F., Luan, H., & Chua, T.-S. (2014). Brand Data Gathering From Live Social Media Streams. *Proceedings of International Conference on Multimedia Retrieval, Glasgow, United Kingdom*. doi:10.1145/2578726.2578748
- Gibson, A., Miller, M., Smith, P., Bell, A., Crothers, C. (2013). The Internet in New Zealand 2013. *Auckland, New Zealand: Institute of Culture, Discourse & Communication, AUT University*
- Guidancesoftware.com, (2015). *Computer Forensic Software - Encase Forensic*. Retrieved 30 March 2015, from <https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx>
- Hattingh, F., Buitendag, A., & Thompson, W. (2014, 7-9 May 2014). User willingness to accept friend requests on SNS: A Facebook experiment. *In IST-Africa Conference Proceedings, 2014*. doi:10.1109/ISTAFRICA.2014.6880610
- Hayes, G. (2011). Social media used for criminal investigations. *The Record*. Retrieved January 13, 2016, from http://therecordlive.com/article/Orange_County_News/Orange_County_News/Social_media_used_for_criminal_investigations/64391
- Ho, S. China blocks some Internet reports on Egypt protests. *Voice of America News* (January 30, 2011). Available at www.voanews.com/english/news/China-Blocks-Some-Internet-Reports-on-Egypt-Protests-114925514.html
- Ieong, R. S. C. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, 3, 29-36. doi:<http://dx.doi.org/10.1016/j.diin.2006.06.004>
- Instagram Press Centre, *accessed March 16, 2015*, <http://blog.instagram.com/post/104847837897/141210-300million>

- Itakura, K. Y., & Sonehara, N. (2013, 2-6 Sept. 2013). Using Twitter's Mentions for Efficient Emergency Message Propagation. *Availability, Reliability and Security (ARES), 2013 Eighth International Conference*, 530-537. doi:10.1109/ARES.2013.70
- Jang, Y.-J., & Kwak, J. (2014). Digital forensics investigation methodology applicable for social network services. *Multimedia Tools and Applications*, 1-12. doi:10.1007/s11042-014-2061-8
- Kairam, S., Brzozowski, M., Huffaker, D., & Chi, E. (2012). Talking in circles: selective sharing in google+. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, 1065-1074. doi:10.1145/2207676.2208552
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*, 800-886.
- Lau, R. Y. K., Xia, Y., & Ye, Y. (2014). A Probabilistic Generative Model for Mining Cybercriminal Networks from Online Social Media. *Computational Intelligence Magazine, IEEE*, 9(1), 31-43. doi:10.1109/MCI.2013.2291689
- Lu, H., & Lee, C. (2015). The Topic-Over-Time Mixed Membership Model (TOT-MMM): A Twitter Hashtag Recommendation Model that Accommodates for Temporal Clustering Effects. *Intelligent Systems, IEEE, PP(99)*, 1-1. doi:10.1109/MIS.2
- Maas A (2013) Social oldies means Facebook loses its cool. 27 January. Available at: <http://www.stuff.co.nz/technology/digital-living/8227867/Social-oldies-mean-Facebook-loses-its-cool> .
- Magnet Forensics, (2015). *Internet Evidence Finder*. Retrieved 26 March 2015, from <http://www.magnetforensics.com/mfsoftware/internet-evidence-finder/>
- Marcella, A., & Menendez, D. (2007). *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition*: CRC Press, Boston, MA.
- Mingming, X. (2014, 25-27 June 2014). Analysis of social networking services organizations' profit model based on Web2.0. *Service Systems and Service Management (ICSSSM), 2014 11th International Conference*, 1-4. doi:10.1109/ICSSSM.2014.6943349
- Mostyn, S. (2010). Police stats suggest Facebook becoming hotbed of crime. Retrieved April 25, 2012, from <http://www.thetechherald.com/articles/Police-stats-suggest-Facebook-becoming-hotbed-of-crime>

- Msab.com. (2015). *What is XRY?* Retrieved 26 March 2015, from <https://www.msab.com/xry/what-is-xry?gclid=CJzGscr-xMQCFY8kvQodHGMA9w>
- Muda, A. K., Choo, Y.-H., Abraham, A., & Srihari, S. N. (2014). *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*. Springer International Publishing: Warsaw, Poland.
- Mulazzani, M., Huber, M., & Weippl, E. (2012). Social Network Forensics: Tapping the Data Pool of Social Networks. *Eighth Annual IFIP WG 11.9 International Conference on Digital Forensics*. Retrieved from http://www.sba-research.org/wp-content/uploads/publications/socialForensics_preprint.pdf
- Mumba, E. R. & Venter, H. S. (2014). Testing and Evaluating the Harmonized Digital Forensic Investigation Process in Post Mortem Digital Investigations. *Proceedings of the 2014 ADFSL Conference on Digital Forensics, Security and Law. Richmond, Virginia. May 28-29, 2014.*
- Mutawa, N. Al, Awadhi, I. Al, Baggili, I., & Marrington, A. (2011). Forensic artifacts of Facebook's instant messaging service. *6th International Conference on Internet Technology and Secured Transactions*, 771-776. Abu Dhabi, UAE: IEEE. Retrieved from <http://ieeexplore.ieee.org.ezproxy.aut.ac.nz/stamp/stamp.jsp?tp=&arnumber=6148436&isnumber=6148349>
- Nagarajan, M., Sheth, A., & Velmurugan, S. (2011). Citizen sensor data mining, social media analytics and development centric web applications. *Proceedings of the 20th international conference companion on World Wide Web*, Hyderabad, India. doi:10.1145/1963192.1963315
- Nair, A. S. V., & Ajeena, B. A. S. (2014). *A Log Based Strategy for Fingerprinting and Forensic Investigation of Online Cyber Crimes. Proceedings of the International Conference on Interdisciplinary Advances in Applied Computing*, Amritapuri, India. doi:10.1145/2660859.2660912
- NIJ. (2008). *Electronic crime scene investigation: a guide for first responders*. 2ed. Washington, DC.
- NIST. (2001). General test methodology for computer forensic tools. Retrieved 6 May 2015, from <http://www.cftt.nist.gov/Test%20Methodology%207.doc>
- Noureldin, S. H., Hashem, S., & Abdalla, S. (2011, 4-6 Nov. 2011). Computer Forensics Guidance Model with Cases Study. *Multimedia Information Networking and Security (MINES), 2011 Third International Conference*, 564-571. doi:10.1109/MINES.2011.49

- Palmer, G. (2001). A Road Map for Digital Forensic Research. *First Digital forensic Research Workshop*, Utica, New York. 2001
- Deibert, R. (2014). *DIY Citizenship: Critical Making and Social Media*. (M. Ratto & M. Boler, Eds.). *MIT Press*. Retrieved from <http://www.jstor.org/stable/j.ctt9qf5jb>
- Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, 1(3), 1-12. Retrieved 5 March, 2015 from <https://www.swgde.org/documents/Current%20Documents/2013-04-08%20SWGDE-SWGIT%20Glossary%20v2.7>
- Scellato, S., Mascolo, C., Musolesi, M., & Latora, V. (2010). Distance matters: geo-social metrics for online social networks. *WOSN'10 Proceedings of the 3rd conference on online social networks*, 8-8.
- Schneier, B. (2010). A Taxonomy of Social Networking Data. *Security & Privacy, IEEE*, 8(4), 88-88. doi:10.1109/MSP.2010.118
- Schofield, D. (2007, 14-17 Aug. 2007). Animating and Interacting with Graphical Evidence: Bringing Courtrooms to Life with Virtual Reconstructions. *Computer Graphics, Imaging and Visualisation, 2007. CGIV '07*, 321-328. doi:10.1109/CGIV.2007.18
- Scientific Working Group on Digital Evidence (2014, September 5). *SWGDE Recommended Guidelines for Validation Testing Version 2.0*. Retrieved May 11, 2015, from Scientific Working Group on Digital Evidence: <https://www.swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Recommended%20Guidelines%20for%20Validation%20Testing%20V2-0>
- Shrivastava, G., & Gupta, B. B. (2014, 7-10 Oct. 2014). An Encapsulated Approach of Forensic Model for digital investigation. *Consumer Electronics (GCCE), 2014 IEEE 3rd Global Conference*, 280-284. doi:10.1109/GCCE.2014.7031241
- Silva, T. H., Melo, P. O. S. V. d., Almeida, J. M., Salles, J., & Loureiro, A. A. F. (2013). A comparison of Foursquare and Instagram to the study of city dynamics and urban social behavior. *Presented at the meeting of the Proceedings of the 2nd ACM SIGKDD International Workshop on Urban Computing*, Chicago, Illinois. doi:10.1145/2505821.2505836
- Siquet.com. (2015). *IXTK Supported Artifacts SiQuest Corporation | Home of Internet Examiner Toolkit (IXTK) | Leaders in Internet Forensic Software*.


Retrieved 30 March 2015, from <http://www.siquet.com/index.php/ixtk-supported-artifacts/>


- Sorensen, L. (2009). User managed trust in social networking - Comparing Facebook, MySpace and LinkedIn. *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference*, 427-431. doi:10.1109/WIRELESSVITAE.2009.5172486
- Stringhini, G., Wang, G., Egele, M., Kruegel, C., Vigna, G., Zheng, H., & Zhao, B. Y. (2013). Follow the green: growth and dynamics in twitter follower markets. *Proceedings of the 2013 conference on Internet measurement*, 163-176. doi:10.1145/2504730.2504731
- SWGDE. (2013). SWGDE and SWGIT Digital & Multimedia Evidence Glossary.
- Teoh, K.-K., Pourshafie, T., & Balakrishnan, V. (2014). A gender lens perspective of the use of social network in higher education in Malaysia and Australia. *Proceedings of the 2014 International Conference on Social Computing*, Beijing, China. doi:10.1145/2639968.2640070
- The Icehouse survey, (2013), August 2013 Retrieved from <http://socialmedia.org.nz/2013/12/why-social-media-really-matters-for-kiwi-businesses-in-2014/>
- Tipping, R., Farrell, G., Farrell, V., & Woodward, C. J. (2014). From collection to courtroom: perceptions and realities of how the data flows. *Proceedings of the 26th Australian Computer-Human Interaction Conference on Designing Futures: the Future of Design*, Sydney, New South Wales, Australia. doi:10.1145/2686612.2686626
- Venter, H., Labuschagne, L., & Eloff, M. (2007). New approaches for security, Privacy and Trust in Complex Environments: *Proceedings of the IFIP TC 11 22nd International Information Security Conference (SEC 2007)*, 14-16 May 2007, Sandton, South Africa
- Wang, Q., Woo, H. L., Quek, C. L., Yang, Y., & Liu, M. (2012). Using the Facebook group as a learning management system: An exploratory study. *British Journal of Educational Technology*, 43(3), 428-438. doi:10.1111/j.1467-8535.2011.01195.x
- Whittaker, J. A. (2000). What is software testing? And why is it so hard? *Software, IEEE*, 17(1), 70-79. doi:10.1109/52.819971


- Willassen, S. Y., & Mjølunes, S. F. (2005). Digital forensics research. 30(2007), 92-97.
- Willassen, S., Mjølunes, S. (2005). Digital forensic Research, *Teletronikk*, vol. 2005(1), pp. 92-97
- Wilsdon, T., & Slay, J. (2006). Validation of forensic computing software utilizing black box testing technique. *Proceedings of 4th Australian Digital Forensics Conference*, Perth, Australia
- Wireshark.org, (2015). *Chapter 1. Introduction*. Retrieved 26 March 2015, from https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html
- Zainudin, N. M., Merabti, M., & Llewellyn-Jones, D. (2010, June). A digital forensic investigation model for online social networking. *In Proceedings of the 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting, Liverpool* (pp. 21-22).
- Zainudin, N. M., Merabti, M., & Llewellyn-Jones, D. (2011, 23-24 Nov. 2011). Online social networks as supporting evidence: A digital forensic investigation model and its application design. *Research and Innovation in Information Systems (ICRIIS), 2011 International Conference*, 1-6. doi:10.1109/ICRIIS.2011.6125728
- Zhang, H., Choudhury, M. D., & Grudin, J. (2014). Creepy but inevitable? : The evolution of social networking. *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, Baltimore, Maryland, USA. doi:10.1145/2531602.2531685

APPENDICES


Appendix 1 – First Case Scenario: Smith Volkov's (The Suspect) Simulation of the Controlled Data

The First Scenario-Facebook & Instagram- Firefox - Target's Computer SmithVolkov				
Event #	Date/Time	Browser /method	Action	Clarifications
1	15/6/2015 12:41 PM	Firefox	Login to Facebook	Created account: smith volkov
2	15/6/2015 12:43 PM	Firefox	Post evidence in Facebook	Generate Ev. using Firefox, wall post in Facebook is great (Hint: Ev. = Evidence)
3	15/6/2015 12:45 PM	Firefox	Upload photo to Facebook	
4	15/6/2015 12: 46 PM	Firefox	Post on Friend's wall	Post to Hanan Alsalem: Hello hanan, Generate Ev. Using Firefox posting to friend wall
5	15/6/2015	Firefox	Instant Messages prepared below:	With hanan Alsalem
	15/6/2015 12:46 PM	Firefox	Hanan this is saud This is for my thesis I created this account just now to do the testing	Smith Volkov
	15/6/2015 12:47 PM		Oh that is cool How is your day?	Hanan alsalem
	15/6/2015 12:47 PM		Good busy day	Smith Volkov
	15/6/2015 12:47 PM		Ana bro7 home b3d alma3had	Hanan Alsalem
	15/6/2015 12:48 PM		Ok cool Can you talk more in English, because this will be used for my thesis work lol. As I told you yesterday, I need to generate data, so i can do the examination. this is one of the data	Smith Volkov
	15/6/2015 12:49 PM		that is so nice, so i be in you thesis haha good luck my cute husband	Hanan Alsalem
6	15/6/2015 12:51 PM	Firefox	Post video as evidence	Video-Firefox.flv
7	15/6/2015 12:52 PM	Phone Instagram APP	Posting 2 pictures from Android phone to Instagram application on smithvolkov (Twitter & Facebok)	One for Facebook and another one for Twitter



8	15/6/2015 12:53 PM	Phone Instagram APP	Share the first Instagram picture from phone app to Facebook	 App:Instagram Instagram to facebook share Picture Evidence
9	15/6/2015 12:53 PM	Firefox	View Instagram picture from Facebook account	Wall page of Smith Volkov
10	15/6/2015 12:54 PM	Firefox	Login to Instagram	Username : smithvolkov
11	15/6/2015 12:54 PM	Firefox	View pictures added by Instagram application	


The First Scenario-Facebook & Instagram- Chrome - Target's Computer SmithVolkov				
Event #	Date/Time	Browser /method	Action	Clarifications
1	15/6/2015 12:55 PM	Chrome	Login to Facebook	Created account: smith volkov
2	15/6/2015 12:56 PM	Chrome	Post evidence in Facebook	Generate Ev. using Chrome, wall post in Facebook is awesome (Hint: Ev. = Evidence)
3	15/6/2015 12:56 PM	Chrome	Upload photo to Facebook	 Browser: Chrome website: Facebook Picture Evidence
4	15/6/2015 12:57 PM	Chrome	Post on Friend's wall	Post to Hanan Alsalem: Hello hanan, Generate Ev. Using Chrome posting to friend wall
5	15/6/2015	Chrome	Instant Messages prepared below:	With hanan Alsalem
	15/6/2015 12:58 PM	Chrome	Hanan I need to keep talking because I need to do this from different browsers	Smith Volkov
	15/6/2015 12:59 PM		what you mean	Hanan alsalem
	15/6/2015 12:59 PM		You know there are many browsers people can use to go to web pages right? I need to generate data from three of them so i can examine	Smith Volkov
	15/6/2015 1:00 PM		aha Still English?	Hanan Alsalem
	15/6/2015 1:00 PM		haha yes u need to practice what u learnt at school babe	Smith Volkov
6	15/6/2015 1:01 PM	Chrome	Post video as evidence	Video-Chrome.flv
7	15/6/2015 1:01 PM	Chrome	View Instagram picture from Facebook account	Wall page of Smith Volkov

8	15/6/2015 1:02 PM	chrome	Login to Instagram	Username : smithvolkov
9	15/6/2015 1:02 PM	Chrome	View pictures added by Instagram application	


The First Scenario-Facebook & Instagram- IE - Target's Computer SmithVolkov				
Event #	Date/Time	Browser /method	Action	Clarifications
1	15/6/2015 1:03 PM	IE	Login to Facebook	Created account: smith volkov
2	15/6/2015 1:03 PM	IE	Post evidence in Facebook	Generate Ev. using IE, wall post in Facebook is very nice (Hint: Ev. = Evidence)
3	15/6/2015 1:03 PM	IE	Upload photo to Facebook	 Browser: IE website: Facebook Picture Evidence
4	15/6/2015 1:04 PM	IE	Post Friend's wall	Post to Hanan Alsalem: Hello hanan, Generate Ev. Using IE posting to friend wall
5	15/6/2015	IE	Instant Messages prepared below:	With hanan Alsalem
	15/6/2015 1:06 PM		now I am using another browsers IE	Smith Volkov
	15/6/2015 1:06 PM		are you come home early tonight	hanan Alsalem
	15/6/2015 1:06 PM		I don't think so, I am still at uni in WT building that I showed u before so how was school today good?	Smith Volkov
	15/6/2015 1:07 PM		yes, have speaking test today it was good next week i have exam if i pass i go to upper intermediate	hanan Alsalem
	15/6/2015 1:07 PM		I know you can do it. I will teach u this weekend before the test	Smith Volkov
	15/6/2015 1:07 PM		thank you 3>	hanan Alsalem
6	15/6/2015 1:08 PM	IE	Post video as evidence	Video-IE.flv
7	15/6/2015 1:08 PM	IE	View Instagram picture from Facebook account	Wall page of Smith Volkov
8	15/6/2015 1:09 PM	IE	Login to Instagram	Username : smithvolkov
9	15/6/12015 1:09 PM	IE	View pictures added by Instagram application	

The First Scenario-Twitter & Instagram- Firefox - Target Computer 1 - SmithVolkov				
Event #	Date/Time	Browser /method	Action	Clarifications
1	15/6/2015	Firefox	Login to Twitter	Created account:smithvolko1


	1:10 PM			
2	15/6/2015 1:11 PM	Firefox	Post evidence in Twitter	Generate Ev. using Firefox, Tweeting in Twitter is very nice
3	15/6/2015 1:12 PM	Firefox	Upload photo to Twitter	 Browser: Firefox website: Twitter Picture Evidence
4	15/6/2015 1:13 PM	Firefox	Tweet on Friend's wall	Post to Alshaifi: Generate Ev. Using Firefox Tweeting to friends wall
5	15/6/2015	Firefox	Direct Messages prepared below:	With @AlshaifiS
	15/6/2015 1:14 PM		Direct message from suspect to another person, on Twitter using Firefox	smithvolko1
	15/6/2015 1:14 PM		Reply that's good	AlshaifiS
6	15/6/2015 1:15 PM	Phone Instagram APP	Share the second Instagram picture from phone app to Twitter	 App: Instagram Instagram to Twitter share Picture Evidence
7	15/6/2015 1:15 PM	Firefox	View Instagram picture from Twitter account	Wall page of smithvolko1
8	15/6/2015 1:16 PM	Firefox	Login to Instagram	Username : smithvolkov
9	15/6/2015 1:16 PM	Firefox	View picture shared in Twitter added by Instagram application	
10	15/6/2015 1:17 PM	Firefox	Retweet a post	


The First Scenario-Twitter & Instagram- Chrome - Target Computer 1 - SmithVolkov				
Event #	Date/Time	Browser /method	Action	Clarifications
1	15/6/2015 1:17 PM	Chrome	Login to Twitter	Created account:smithvolko1
2	15/6/2015 1:18 PM	Chrome	Post evidence in Twitter	Generate Ev. using chrom, Tweeting in Twitter is very nice
3	15/6/2015 1:18 PM	Chrome	Upload photo to Twitter	 Browser: Chrome website: Twitter Picture Evidence
4	15/6/2015 1:20 PM	Chrome	Tweet on Friend's wall	Post to Alshaifi: Generate Ev. Using Chrome Tweeting to friends wall


5	15/6/2015	Chrome	Direct Messages prepared below:	With @AlshaifiS
	15/6/2015 1:21 PM		Direct message from suspect to another person, on Twitter using Chrome	smithvolko1
	15/6/2015 1:21 PM		That's nice	AlshaifiS
6	15/6/2015 1:22 PM	Chrome	View Instagram picture from Twitter account	Wall page of smithvolko1
7	15/6/2015 1:22 PM	Chrome	Login to Instagram	Username : smithvolkov
8	15/6/2015 1:23 PM	Chrome	View picture shared in Twitter added by Instagram application	
9	15/6/2015 1:23 PM	Chrome	Retweet a post	

The First Scenario-Twitter & Instagram- IE - Target Computer 1 - SmithVolkov				
Event #	Date/Time	Browser /method	Action	Clarifications
1	15/6/2015 1:24 PM	IE	Login to Twitter	Created account:smithvolko1
2	15/6/2015 1:24 PM	IE	Post evidence in Twitter	Generate Ev. using IE, Tweeting in Twitter is very nice
3	15/6/2015 1:24 PM	IE	Upload photo to Twitter	 <p>Browser: IE website: Twitter Picture Evidence</p>
4	15/6/2015 1:26 PM	IE	Tweet on Friend's wall	Post to Alshaifi: Generate Ev. Using IE Tweeting to friends wall
5	15/6/2015	IE	Direct Messages prepared below:	With @AlshaifiS
	15/6/2015 1:27 PM		Direct message from suspect to another person, on Twitter using Internet Explorer	smithvolko1
	15/6/2015 1:27 PM		That's nice	AlshaifiS
6	15/6/2015 1:28 PM	IE	View Instagram picture from Twitter account	Wall page of smithvolko1
7	15/6/2015 1:28 PM	IE	Login to Instagram	Username : smithvolkov
8	15/6/2015 1:29 PM	IE	View picture shared in Twitter added by Instagram application	
9	15/6/2015 1:29 PM	IE	Retweet a post	

Appendix 2 – Second Case Scenario: Jason Lopiz’s (The Suspect) Simulation of the Controlled Data

The second Scenario-LinkedIn- Firefox - Target Computer 2 - Jason Lopiz				
Event #	Date/Time	Browser /method	Action	Clarifications
1	23/6/2015 7:55 pm	Firefox	Login to LinkedIn	Created account: Jason Lopiz
2	23/6/2015 7:57 pm	Firefox	Post evidence in LinkedIn	Generate Evidence in LinkedIn using Firefox test post 1
3	23/6/2015 7:58 pm	Firefox	Upload photo to LinkedIn	 <p>Browser: Firefox Website: LinkedIn Picture Evidence</p>
4	23/6/2015 8:00 pm	Firefox	Post Comments on picture	Generate Comment evidence in LinkedIn using Firefox test post 2
5	23/6/2015 8:00 pm pm	Firefox	Like picture	Like the picture uploaded in event 3
6	23/6/2015	Firefox	Send message	With saud alshaifi
	23/6/2015 8:02 pm	Firefox	Generate message to friend evidence in LinkedIn using Firefox test post 3	Jason Lopiz
	23/6/2015 8:04 pm	Firefox	Reply from friend received in Firefox LinkedIn test post 4	Saud alshaifi

The second Scenario-LinkedIn- Chrome - Target Computer 2 - JasonLopiz				
Event #	Date/Time	Browser /method	Action	Clarifications
1	23/6/2015 8:06 pm	Chrome	Login to LinkedIn	Created account: Jason Lopiz
2	23/6/2015 8:08 pm	Chrome	Post evidence in LinkedIn	Generate Evidence in LinkedIn using Chrome test post 1
3	23/6/2015 8:08 pm	Chrome	Upload photo to LinkedIn	 <p>Browser: Chrome Website: LinkedIn Picture Evidence</p>
4	23/6/2015 8:09 pm	Chrome	Post Comments on picture	Generate Comment evidence in LinkedIn using Chrome test post 2
5	23/6/2015 8:10 pm	Chrome	Like picture	Like the picture uploaded in event 3
6	23/6/2015	Chrome	Send message	With saud alshaifi
	23/6/2015 8:11 pm	Chrome	Generate message to friend evidence in LinkedIn using Chrome test post 3	Jason Lopiz
	23/6/2015 8:12 pm	Chrome	Reply from friend received in Chrome LinkedIn test post 4	Saud alshaifi

The second Scenario-LinkedIn- IE - Target Computer 2 - Jason Lopiz				
Event #	Date/Time	Browser /method	Action	Clarifications
1	23/6/2015 8:14 pm	IE	Login to LinkedIn	Created account: Jason Lopiz
2	23/6/2015 8:14	IE	Post evidence in LinkedIn	Generate Evidence in LinkedIn using IE test post 1
3	23/6/2015 8:15 pm	IE	Upload photo to LinkedIn	 <p>Browser: IE Website: LinkedIn Picture Evidence</p>
4	23/6/2015 8:16 pm	IE	Post Comments on picture	Generate Comment evidence in LinkedIn using IE test post 2
5	23/6/2015 8:17 pm	IE	Like picture	Like the picture uploaded in event 3
6	23/6/2015	IE	Send message	With saud alshaifi
	23/6/2015 8:18 pm	IE	Generate message to friend evidence in LinkedIn using IE test post 3	Jason Lopiz
	23/6/2015 8:19 pm	IE	Reply from friend received in IE LinkedIn test post 4	Saud alshaifi

The second Scenario-Bayt- Firefox - Target Computer 2 - Jason Lopiz				
Event #	Date/Time	Browser /method	Action	Clarifications
1	23/6/2015 8:22 pm	Firefox	Login to Bayt	Created account: Jason Lopiz
2	23/6/2015 8:24 pm	Firefox	Post question as evidence in Bayt	question as evidence in Bayt using Firefox test post 1
3	23/6/2015 8:25 pm	Firefox	Make a recommendation	Generate recommendation evidence in Bayt using Firefox test post 2
4	23/6/2015 8:28 pm	Firefox	Answer question as evidence	Answering a question as evidence in Bayt using Firefox test post 3
5	23/6/2015	Firefox	Send message	With saud alshaifi
	23/6/2015 8:30 pm	Firefox	Generate message to friend evidence in Bayt using Firefox test post 4	Jason Lopiz
	8:32 pm	Firefox	Reply from friend received in Firefox Bayt test post 5	Saud alshaifi

The second Scenario-Bayt- Chrome - Target Computer 2 - Jason Lopiz				
Event #	Date/Time	Browser /method	Action	Clarifications
1	23/6/2015 8:33 pm	Chrome	Login to Bayt	Created account: Jason Lopiz
2	23/6/2015 8:36 pm	Chrome	Post question as evidence in Bayt	Generate question as evidence in Bayt using Chrome test post 1
3	23/6/2015 8:39 pm	Chrome	Make a recommendation	Generate recommendation evidence in Bayt using Chrome test post 2
4	23/6/2015 8:41 pm	Chrome	Answer question as evidence	Answering a question as evidence in Bayt using Chrome test post 3
5	23/6/2015	Chrome	Send message	With saud alshaifi

	23/6/2015 8:43 pm	Chrome	Generate message to friend evidence in Bayt using Chrome test post 4	Jason Lopiz
	23/6/2015 8:46 pm	chrome	Reply from friend received in Chrome Bayt test post 5	Saud alshaifi

The second Scenario-Bayt- IE - Target Computer 2 - Jason Lopiz				
Event #	Date/Time	Browser /method	Action	Clarifications
1	23/6/2015 8:49 pm	IE	Login to Bayt	Created account: Jason Lopiz
2	23/6/2015 8:50 pm	IE	Post question as evidence in Bayt	Generate question as evidence in Bayt using ie
3	23/6/2015 8:56 pm	IE	Make a recommendation	Generate recommendation as evidence in Bayt using internet explorer test post 2
4	23/6/2015 9:00 pm	IE	Answer question as evidence	Answering a question as evidence in Bayt using IE test post 3
5	23/6/2015	IE	Send message	With saud alshaifi
	23/6/2015 9:06 pm	IE	Generate message to friend evidence in Bayt using IE test post 4	Jason Lopiz
	9:07pm	IE	Reply from friend received in IE Bayt test post 5	Saud alshaifi

Appendix 3 – First Case Scenario: Smith Volkov's RAM Verification Image

Created By AccessData® FTK® Imager 2.9.0.1385 100406

Case Information:

Case Number: casescenario1

Evidence Number: 001

Unique description: forensic image of memory dump

Examiner: saud alshaifi

Notes: Dumping memory from the suspect computer

Information for D:\test1 Memory acquisition\test1_Livememory_suspect:

Physical Evidentiary Item (Source) Information:

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 4,175,488

[Image]

Image Type: Raw (dd)

Source data size: 2038 MB

Sector count: 4175488

[Computed Hashes]

MD5 checksum: 3a5333cba55123167fe1cd9e4eb7dc98

SHA1 checksum: 0c7031ae82a9d72ecdba04f487c63d7d5056eb6e

Image Information:

Acquisition started: Mon Jun 15 14:56:17 2015

Acquisition finished: Mon Jun 15 14:57:49 2015

Segment list:

D:\test1 Memory acquisition\test1_Livememory_suspect.001

Image Verification Results:

Verification started: Mon Jun 15 14:57:50 2015

Verification finished: Mon Jun 15 14:58:17 2015

MD5 checksum: 3a5333cba55123167fe1cd9e4eb7dc98 : verified

SHA1 checksum: 0c7031ae82a9d72ecdba04f487c63d7d5056eb6e : verified

Appendix 4 – First Case Scenario: Smith Volkov's HD Verification Image

Created By AccessData® FTK® Imager 2.9.0.1385 100406

Case Information:

Case Number: casescenario1

Evidence Number: 002

Unique description: create an image of suspect hard disk

Examiner: saud alshaifi

Notes: Imaging suspect 1 hard disk

Information for D:\suspect1 hard disk\IMAGE-suspect1-harddrive:

Physical Evidentiary Item (Source) Information:

[Verification Hashes]

MD5 verification hash: abeddbf96de0e20747b3cc32e75dbace

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 312,581,808

[Image]

Image Type: E01

Case number: 002

Evidence number:

Examiner: saud alshaifi

Notes: Imaging Suspect 1 hard drive

Acquired on OS: Windows 7

Acquired using: 3.22g

Acquire date: 17/06/2015 2:55:00 p.m.

System date: 17/06/2015 2:55:00 p.m.

Unique description:

Source data size: 152627 MB

Sector count: 312581808

[Computed Hashes]

MD5 checksum: abeddbf96de0e20747b3cc32e75dbace

SHA1 checksum: 4a3a569616a70371a5cc1d0a0fa56f3350838bab

Image Information:

Acquisition started: Sun Jun 17 16:57:30 2015

Acquisition finished: Sun Jun 17 17:13:01 2015

Segment list:

D:\suspect1 hard disk\IMAGE-suspect1-harddrive.E01

Image Verification Results:

Verification started: Sun Jun 17 17:13:02 2015

Verification finished: Sun Jun 17 17:27:00 2015

MD5 checksum: abeddbf96de0e20747b3cc32e75dbace : verified

SHA1 checksum: 4a3a569616a70371a5cc1d0a0fa56f3350838bab : verified

Appendix 5 – Second Case Scenario: Jason Lopiz’s RAM Verification Image

Created By AccessData® FTK® Imager 2.9.0.1385 100406

Case Information:

Case Number: cacescenario2

Evidence Number: 001

Unique description: create an image of suspect's computer RAM

Examiner: saud alshaifi

Notes:

Information for D:\test2 Memory Acquisition\test2_Livememory_suspect2:

Physical Evidentiary Item (Source) Information:

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 4,175,488

[Image]

Image Type: Raw (dd)

Source data size: 2038 MB

Sector count: 4175488

[Computed Hashes]

MD5 checksum: c0024b656b4fa49683852e51281cca4a

SHA1 checksum: 98b865fb18a95d8525d34bb93c895dca0d6ccc4b

Image Information:

Acquisition started: Tue Jun 23 22:40:43 2015

Acquisition finished: Tue Jun 23 22:42:30 2015

Segment list:

D:\test2 Memory Acquisition\test2_Livememory_suspect2.001

Image Verification Results:

Verification started: Tue Jun 23 22:42:30 2015

Verification finished: Tue Jun 23 22:42:40 2015

MD5 checksum: c0024b656b4fa49683852e51281cca4a : verified

SHA1 checksum: 98b865fb18a95d8525d34bb93c895dca0d6ccc4b : verified

Appendix 6 – Second Case Scenario: Jason Lopiz’s HD Verification Image

Created By AccessData® FTK® Imager 2.9.0.1385 100406

Case Information:

Case Number: casescenario2

Evidence Number: 002

Unique description: create an image of hard disk image

Examiner: saud alshaifi

Notes:

Information for D:\suspect2 hard disk\IMAGE_suspect2_harddrive:

Physical Evidentiary Item (Source) Information:

[Verification Hashes]

MD5 verification hash: c4649a4654466e0b777974bdd1e281fa

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 312,581,808

[Image]

Image Type: E01

Case number: casescenario2

Evidence number:

Examiner: saud alshaifi

Notes:

Acquired on OS: Windows 7

Acquired using: 3.22g

Acquire date: 24/06/2015 3:19:48 p.m.

System date: 24/06/2015 3:19:48 p.m.

Unique description:

Source data size: 152627 MB

Sector count: 312581808

[Computed Hashes]

MD5 checksum: c4649a4654466e0b777974bdd1e281fa

SHA1 checksum: ffe81ffe1c48e876509394f2e5251775ed98d024

Image Information:

Acquisition started: Thu Jun 25 17:08:10 2015

Acquisition finished: Thu Jun 25 17:24:23 2015

Segment list:

D:\suspect2 hard disk\IMAGE_suspect2_harddrive.E01

Image Verification Results:

Verification started: Thu Jun 25 17:24:24 2015

Verification finished: Thu Jun 25 17:37:53 2015

MD5 checksum: c4649a4654466e0b777974bdd1e281fa : verified

SHA1 checksum: ffe81ffe1c48e876509394f2e5251775ed98d024 : verified

Appendix 7 – First Case Scenario: Analysis of RAM Using Belkasoft Evidence Center (Test Plan 1)

TEST PLAN 1 (Belkasoft Evidence Center)

Test Number: 001

Examiner: Saud Alshaifi

Test Title: Test of Belkasoft Evidence Center for finding evidence from the first Scenario Image RAM

Test start Date: 15/6/2015

Purpose and Scope

The Belkasoft Evidence Center is a digital forensic tool developed by Belkasoft, and used by many law enforcements such as FBI, US army, and police department of Germany. Belkasoft can analyse different OSNSs including Facebook and twitter from several artefacts. The purpose of this test is to determine the ability of Belkasoft Evidence Center to successfully analyse evidence from the acquired RAM in the first Scenario.

Requirements

- 1) Belkasoft Evidence Center should successfully recognize the RAM image created by FTK imager
- 2) An MD5 hash value should be calculated before attempt of analysing the acquired image
- 3) The Belkasoft Evidence Center should successfully block any write-up to the image
- 4) The Belkasoft Evidence Center should successfully analyse the image to extract evidence from the conducted first scenario
- 5) Belkasoft evidence Center should successfully extract all the evidence generated in the first scenario from Twitter, Facebook, and Instagram from three different browsers, through analysing the RAM.

Description of Methodology

Once the data has been posted on OSNSs (Controlled data) and documented, the acquisition of live RAM will be done using FTK imager. The image will be validated and verified with MD5 and SHA1 checksum in order to ensure the integrity of the image. The original image will be stored safely for later needs. The created image will be further verified by Belkasoft by calculating the MD5 hash values and compare it with the previous hash values, this is to ensure that the evidence has not been altered after processing it in Belkasoft Evidence Center. The image then will analysed using Belkasoft Evidence Center to look for Evidence from Facebook, Twitter, and Instagram from several web browsers (Firefox, Chrome, and Internet Explorer)

Expected Results

- 1) Belkasoft will successfully find evidence posted in Facebook via Firefox, Chrome, and Internet explorer.
- 2) Belkasoft will successfully find evidence posted in Twitter via Firefox, Chrome, and Internet explorer.
- 3) Belkasoft will successfully find evidence posted in Instagram via Firefox, Chrome, and Internet explorer.

Test Scenarios - Belkasoft Evidence Center - RAM - Facebook & Instagram on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
01-2	Facebook	Find posted evidence on suspect's wall	No Evidence Found	Fail
01-3	Facebook	Find Uploaded Picture	Found Evidence: https://www.facebook.com/photo.php?fbid=107389486266838&set=a.106187259720394.1073741827.100009873604315&type=1&theate Source : firefox.exe	pass
01-4	Facebook	Find post on friend's wall	Only found Friends ID but the post is not found https://www.facebook.com/hanan.alsalem.58?fref=tl_fr_box&pnref=lhc.friend Source : firefox.exe	Fail
01-5	Facebook	Find Instant messaging with friend	Found Evidence Only found the last message out of 6 done in Firefox Figure 4.13 Source : pagefile.sys	Fail
01-6	Facebook	Find video evidence post	Found Evidence: https://www.facebook.com/100009873604315/videos/vb.100009873604315/107391359599984/?type=2&theater&notif_t=video Source : firefox.exe	Pass
01-9	Facebook	Find shared Instagram picture evidence	Found Evidence: https://www.facebook.com/photo.php?fbid=107391609599959&set=a.106225223049931.1073741828.100009873604315&type= Source : firefox.exe	Pass
01-10	Instagram	Find Instagram account of suspects logged in via Firefox	Found Evidence: https://instagram.com/accounts/login Page title: /Smith Volkov on Instagram Source : firefox.exe	Pass
01-11	Instagram	Find viewed Instagram picture via Firefox	Found Evidence: https://instagram.com/p/3xtHtjPIG2 page title: /Smith Volkov on Instagram: "this is instagram shared in Facebook Source : firefox.exe	Pass

Test Scenarios - Belkasoft Evidence Center - RAM - Facebook & Instagram on Chrome				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
02-2	Facebook	Find posted evidence on suspect's wall	No Evidence Found	Fail
02-3	Facebook	Find Uploaded Picture	Found Evidence: https://www.facebook.com/photo.php?fbid=107391949599925&set=a.106187259720394.1073741827.100009873604315&type=1&theater Source : pagefile.sys	Pass

02-4	Facebook	Find post on friend's wall	Found Evidence: Only found Friends ID but the post is not found https://www.facebook.com/hanan.alsalem.58?fref=tl_fr_box&pnref=lhc.fri Source : pagefile.sys	Fail
02-5	Facebook	Find Instant messaging with friend	Found Evidence: Only found the second message received from a friend out of 5 Figure 4.13 Source : pagefile.sys	Fail
02-6	Facebook	Find video evidence post	Found Evidence: https://www.facebook.com/100009873604315/videos/vb.100009873604315/107392542933199/?type=2&theater&notif_t=video_processed Source : pagefile.sys	Pass
02-7	Facebook	Find shared Instagram picture evidence	Found Evidence: https://www.facebook.com/photo.php?fbid=106225229716597&set=a.106225223049931.1073741828.100009873604315&type=1&theater Source : Chrome.exe	Pass
02-8	Instagram	Find Instagram account of suspects logged in via Chrome	Found Evidence: https://instagram.com/smithvolkov/ Source : pagefile.sys	Pass
02-9	Instagram	Find viewed Instagram picture via Chrome	Found Evidence: https://instagram.com/p/3xtHtjPIG2/?taken-by=smithvolkov Source : pagefile.sys	Pass

Test Scenarios - Belkasoft Evidence Center - RAM - Facebook & Instagram on IE				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
03-2	Facebook	Find posted evidence on suspect's wall	No Evidence Found	Fail
03-3	Facebook	Find Uploaded Picture	Found Evidence: URL not found but Uploaded picture is found: D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\75.jpg Source: pagefile.sys	Pass
03-4	Facebook	Find post on friend's wall	Found Evidence: Only found Friends page https://www.facebook.com/hanan.alsalem.58?fref=tl_fr_box&pnref=lhc.friends&ajaxpipe=1&ajaxpipe_token=AXhV7F_wR5W-0dVz&quickling[version]=1784025;0&user=100009873604315&a=1&dyn=7AmajEyl2lm9o-t2u5bHaEWy6zECiq78hAKGgyi8DCqrWU8popyUWu396y8-bxu3fzob8iUkUyu4kckwychFEGmHQ8yEK_AzE&r	Fail

			Source: pagefile.sys	
03-5	Facebook	Find Instant messaging with friend	Found Evidence: Partially found User ID of messaged friend and message URL https://www.facebook.com/messages/?ajaxpipe=1&ajaxpipe_token=AXhV7F_wR5W-0dVz&quickling[version]=1784025;0;&user=100009873604315&a=1&dyn=7AmajEy12lm9o-t2u5bHaEWy6zECiq78hAKGgyi8DCqrWU8ponUKedWOhEyfyUnwPUS2O4K5e8Dx53588z4qqaBGZ28GbLV8W&req=js_onp Source: pagefile.sys	Fail
03-6	Facebook	Find video evidence post	Found Evidence: URL not found but Uploaded picture is found: D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\122.jpg Source: pagefile.sys	Pass
03-7	Facebook	Find shared Instagram picture evidence	Found Evidence: D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\151.jpg Source: pagefile.sys	Pass
03-8	Instagram	Find Instagram account of suspects logged in via IE	No Evidence Found User smithvolkov Instagram account is not found	Fail
03-9	Instagram	Find viewed Instagram picture via IE	Found Evidence: admin@https://instagram.com/p/3xtHtjPIG2/ Source: svchost.exe	Pass

Test Scenarios - Belkasoft Evidence Center – RAM – Twitter & Instagram on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
04-2	Twitter	Find posted evidence on Twitter	Found Evidence: lang="en" data-aria-label-part="0">Generate Ev. using Firefox, Tweeting in Twitter is very nice; ; Source: pagefile.sys	pass
04-3	Twitter	Find uploaded photo in Twitter	Found Evidence: https://twitter.com/smithvolko1/status/610253537465925632/photo/1 And: D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\389.jpg Source: Firefox session store & pagefile.sys	Pass
04-4	Twitter	Find tweets in friends wall	No evidence found	Fail

04-5	Twitter	Find Direct messaging with friend	Found Evidence: Only found the User ID of friend not the message https://twitter.com/AlshaifiS Source: firefox.exe	Fail
04-7	Twitter	Find shared Instagram picture evidence	No evidence found	Fail
04-9	Instagram	Find viewed picture evidence in Instagram	Found Evidence: https://instagram.com/p/3xtNkYPIHN Source: firefox.exe	Pass
04-10	Twitter	Find suspect's retweets	Found Evidence: lang="en" data-aria-label-part="0">@nzherald Wonder what sort of salary increases top NZ journalists got this year - and how that affects their reporting? Source: firefox.exe	pass

Test Scenarios - Belkasoft Evidence Center – RAM – Twitter & Instagram on Chrome				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
05-2	Twitter	Find posted evidence on Twitter	Found Evidence: lang="en" data-aria-label-part="0">Generate Ev. using chrom, Tweeting in Twitter is very nice Source: pagefile.sys	pass
05-3	Twitter	Find uploaded photo in Twitter	Found Evidence: lang="und" data-aria-label-part="0">pic.twitter.com\0NI3k5XAr7 and: D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\432.jpg Source: Chrome.exe & pagefile.sys	Pass
05-4	Twitter	Find tweets in friends wall	No evidence found	Fail
05-5	Twitter	Find Direct messaging with friend	Found Evidence: Only friends ID found https://twitter.com/AlshaifiS Source: Chrome.exe	Fail
05-6	Twitter	Find shared Instagram picture evidence	No evidence found	Fail
05-8	Instagram	Find viewed picture evidence in Instagram	Found Evidence: https://instagram.com/p/3xtNkYPIHN/ Source: Chrome.exe	Pass
05-9	Twitter	Find suspect's retweets	Found Evidence: lang="en" data-aria-label-part="0">???I can???t even??? is a confession interrupted http://nyti.ms/1I9RLUR&nbsp Source: pagefile.sys	pass

Test Scenarios - Belkasoft Evidence Center – RAM – Twitter & Instagram on IE				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
06-2	Twitter	Find posted evidence on Twitter	Found Evidence: lang=\"en\" data-aria-label-part=\"0\">Generate Ev. Using IE Tweeting in Twitter is very nice Source: SearchProtocol	Pass
06-3	Twitter	Find uploaded photo in Twitter	Found Evidence: admin@https://twitter.com/smithvolko1/status/610256647156412416/photo/1 Source: taskhost.exe	Pass
06-4	Twitter	Find tweets in friends wall	No evidence found	Fail
06-5	Twitter	Find Direct messaging with friend	No evidence found	Fail
06-6	Twitter	Find shared Instagram picture evidence	No evidence found	Fail
06-8	Instagram	Find viewed picture evidence in Instagram	Found Evidence: admin@https://instagram.com/p/3xtNkYPIHN/ Source: taskhost.exe	pass
06-9	Twitter	Find suspect's retweets	Found Evidence: lang="en" data-aria-label-part="0">Editorial: Labour will win back its supporters http://nzh.nu/Oj3Vd&nbsp Source: pagefile.sys	pass

Appendix 8 – First Case Scenario: Analysis of Hard Drive Using Belkasoft Evidence Center (Test Plan2)

TEST PLAN 2 (Belkasoft Evidence Center)

Test Number: 002

Examiner: Saud Alshaifi

Test Title: Test of Belkasoft Evidence Center for finding evidence from the first Scenario suspect's hard disk

Test Date: 17/6/2015

Purpose and Scope

After analysis of suspect' (Smith Volkov) RAM in the first case scenario, and finding the result of evidence found from his Computer's RAM, the investigator is going to conduct another examination in order to find evidence from his hard drive acquired using Tableau eSATA forensic bridge and Tableau Imager 1.11.

Requirements

- 1) The Belkasoft Evidence Center should successfully recognize hard disk image created by Tableau Imager 1.11.
- 2) An MD5 hash value should be calculated before attempt of analysing the acquired image
- 3) The Belkasoft Evidence Center should successfully prevent any write-up to the image.
- 4) The Belkasoft Evidence Center should successfully analyse the image created by Tableau Imager type .E01 to extract evidence from the conducted first scenario
- 5) Belkasoft evidence Center should successfully extract all the evidence generated in the first scenario from Twitter, Facebook, and Instagram from three different browsers, through analysing the suspect's hard disk.

Description of Methodology

The suspect's laptop has been seized for further analysis. The suspect hard disk is taken out from the laptop with forensic manner. The collection of data from the suspect's hard drive was accomplished via using write blocker T35es which is a forensic SATA/IDE bridge in order to ensure the integrity of the image by blocking any write to the hard disk. The software used for acquiring the hard disk is Tableau Imager, image version 1.11. The acquired evidence image is verified using MD5 hash value after processing the image in Belkasoft Evidence Center. The original image will be stored safely for later needs. The created image will be analysed using Belkasoft Evidence Center to look for Evidence from Facebook, Twitter, and Instagram from several web browsers (Firefox, Chrome, and Internet Explorer) from the suspect's hard drive

Expected Results

- 1) Belkasoft will successfully find evidence posted in Facebook via Firefox, Chrome, and Internet explorer.
- 2) Belkasoft will successfully find evidence posted in Twitter via Firefox, Chrome, and Internet explorer.
- 3) Belkasoft will successfully find evidence posted in Instagram via Firefox, Chrome, and Internet explorer.

Test Scenarios - Belkasoft Evidence Center – hard drive – Facebook & Instagram on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
07-2	Facebook	Find posted evidence on suspect's wall	Found Evidence: Only found profile picture of the suspect. On https://fbcdn-profile-a.akamaihd.net/hprofile-ak-xta1/v/t1.0-1/p160x160/11159962_106185986387188_3447611650442873588_n.jpg?oh=d88081d179ae0b0f1c29f34d399c562c&oe=55F64555&gda_1441600379_021ca8ea5a8ace8daed18faca2958262 Source:I:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\8ez4wa3i.default\cache2\entries\6207ece090c815f2b092349f937ef0b2635fb870	Fail
07-3	Facebook	Find Uploaded Picture	Found Evidence: Uploaded picture is found: https://scontent-lax1-1.xx.fbcdn.net/hphotos-xat1/v/t1.0-9/11393087_106187236387063_2759516425629086158_n.jpg?oh=cdafb148a070badd8bc50a696e6d6d39&oe=5629DD79 Source:I:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\8ez4wa3i.default\cache2\entries\4d2357ae5f12be38cf6d6152ab04f8699d3fac12	pass
07-4	Facebook	Find post on friend's wall	No evidence found	Fail
07-5	Facebook	Find Instant messaging with friend	No evidence found	Fail
07-6	Facebook	Find video evidence post	Found Evidence: Posted video is found Source: D:\belkasoft cases\forensics case 2 - suspect1 hard drive\forensics case2 analysis of suspect 1 HD\forensics case2 analysis of suspect 1 HD\23\Jpeg\233.jpg	Pass
07-9	Facebook	Find shared Instagram picture evidence	Found in https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11374779_914991828542812_1414951129_n.jpg Source: I:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\8ez4wa3i.default\cache2\entries\11867d59bda6affbe1e0767b56e08c1f2381db8d	Pass
07-10	Instagram	Find Instagram account of suspects logged in via Firefox	No evidence found	Fail
07-11	Instagram	Find viewed Instagram picture via Firefox	No Evidence Found	Fail

Test Scenarios - Belkasoft Evidence Center – hard drive – Facebook & Instagram on Chrome				
Test Number/event #	Social network	Expected result	Found Evidence	Actual result
08-2	Facebook	Find posted evidence on suspect's wall	No Evidence found	Fail
08-3	Facebook	Find Uploaded Picture	Found Evidence: https://scontent-lax1-1.xx.fbcdn.net/hphotos-xtf1/v/t1.0-9/11425855_107391949599925_6391389738211779334_n.jpg?oh=477468cb2594b99bf21b27d12eeb2575&oe=55F800E3 Source: I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3	Pass
08-4	Facebook	Find post on friend's wall	No Evidence found	Fail
08-5	Facebook	Find Instant messaging with friend	No Evidence found	Fail
08-6	Facebook	Find video evidence post	Found Evidence: https://www.facebook.com/100009873604315/videos/vb.100009873604315/107392542933199/?type=2&theater&notif_t=video_processed Source: I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sites	Pass
08-7	Facebook	Find shared Instagram picture evidence	Found Evidence: https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11374779_914991828542812_1414951129_n.jpg Source: I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\f_00004A	Pass
08-8	Instagram	Find Instagram account of suspects logged in via Chrome	Found Evidence: https://instagram.com/smithvolkov/ Source: I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sites	Pass
08-9	Instagram	Find viewed Instagram picture via Chrome	Found Evidence: https://instagram.com/p/3xtHtjPIG2/ Source: I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sites	Pass

Test Scenarios - Belkasoft Evidence Center – hard drive – Facebook & Instagram on IE				
Test Number/event #	Social network	Expected result	Found Evidence	Actual result
09-2	Facebook	Find posted evidence on suspect's wall	No Evidence found	Fail
09-3	Facebook	Find Uploaded Picture	Found Evidence: https://fbcdn-sphotos-b-a.akamaihd.net/hphotos-ak-xtf1/v/t1.0-	Pass

			9/11407100_107392949599825_1997037522158782039_n.jpg?oh=5a4b48eafe97f229ae2b6de1449e96ba&oe=55F6B044&_gda_=1446151455_501780dacec66e0e34f80f5f14600292 Source: I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE556GGEP5W\11407100_107392949599825_1997037522158782039_n[1].jpg	
09-4	Facebook	Find post on friend's wall	No Evidence Found	Fail
09-5	Facebook	Find Instant messaging with friend	No Evidence Found	Fail
09-6	Facebook	Find video evidence post	Found Evidence: https://fbcdn-sphotos-g-a.akamaihd.net/hphotos-ak-xat1/v/t1.0-9/11401437_106219636383823_5785327220111996688_n.jpg?oh=62b81a63fd2e3b9415f109d4479b6a7c&oe=55E7B2EB&_gda_=1446082612_29171c540e6edacfa26169f4aeb2183b Source: I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE556GGEP5W\11401437_106219636383823_5785327220111996688_n[1].jpg	Pass
09-7	Facebook	Find shared Instagram picture evidence	Found Evidence: Picture found in I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T6GT6XA0\11247720_107391609599959_8789731246890578286_n[1].jpg	Pass
09-8	Instagram	Find Instagram account of suspects logged in via IE	No Evidence Found	Fail
09-9	Instagram	Find viewed Instagram picture via IE	Found Evidence: https://instagram.com/p/3xtHtjPIG2/ Source:I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	pass

Test Scenarios - Belkasoft Evidence Center – hard drive – Twitter & Instagram on Firefox				
Test Number/e vent #	Social network	Expected result	Found Evidence	Actual result
10-2	Twitter	Find posted evidence on Twitter	Found Evidence: Only suspect's profile picture found https://pbs.twimg.com/profile_images/608869050056253441/WCCRY2dd.jpg Source:I:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\8ez4wa3i.default\cache2\entries	Fail

			\3589a80ec798ed81e250e6e43f0cc225661b59a9	
10-3	Twitter	Find uploaded photo in Twitter	Found Evidence: https://pbs.twimg.com/media/CHgOW4WVEAAR_1B.jpg Source: I:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\8ez4wa3i.default\cache2\entries\50ab9effb0164027baf29e14749475b8e085311f	Pass
10-4	Twitter	Find tweets in friends wall	No Evidence Found	Fail
10-5	Twitter	Find Direct messaging with friend	No Evidence Found	Fail
10-7	Twitter	Find shared Instagram picture evidence	No Evidence Found	Fail
10-9	Instagram	Find viewed picture evidence in Instagram	No Evidence Found	Fail
10-10	Twitter	Find suspect's retweets	No Evidence Found	Fail

Test Scenarios - Belkasoft Evidence Center – hard drive – Twitter & Instagram on Chrome				
Test Number/event #	Social network	Expected result	Found Evidence	Actual result
11-2	Twitter	Find posted evidence on Twitter	Found Evidence: Only suspect's profile picture found https://pbs.twimg.com/profile_images/608869050056253441/WCCRY2dd_bigger.jpg Source: I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_2	Fail
11-3	Twitter	Find uploaded photo in Twitter	Found Evidence: https://pbs.twimg.com/media/CHgR34sUsAA-sLd.jpg:large Source: I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3 And D:\belkasoft cases\forensics case 2 - suspect1 hard drive\forensics case2 analysis of suspect 1 HD\forensics case2 analysis of suspect 1 HD\23\Jpeg\1\1045.jpg	Pass
11-4	Twitter	Find tweets in friends wall	Found Evidence: Only found friend's ID https://twitter.com/AlshaifiS Source: I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default	Fail
11-5	Twitter	Find Direct messaging with friend	No Evidence Found	Fail

11-6	Twitter	Find shared Instagram picture evidence	Found Evidence: https://igcdn-photos-g-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11312502_845459245541990_1704121739_n.jpg Source: I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\f_000053	Pass
11-8	Instagram	Find viewed picture evidence in Instagram	Found Evidence: Found URL of the picture https://instagram.com/p/3xtNkYPIHN Source: I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default	Pass
11-9	Twitter	Find suspect's retweets	No Evidence Found	Fail

Test Scenarios - Belkasoft Evidence Center – hard drive – Twitter & Instagram on IE				
Test Number/event #	Social network	Expected result	Found Evidence	Actual result
12-2	Twitter	Find posted evidence on Twitter	No Evidence Found	Fail
12-3	Twitter	Find uploaded photo in Twitter	Found Evidence: https://twitter.com/smithvolko1/status/610256647156412416/photo/1 Source:I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	Pass
12-4	Twitter	Find tweets in friends wall	No Evidence Found	Fail
12-5	Twitter	Find Direct messaging with friend	No Evidence Found	Fail
12-6	Twitter	Find shared Instagram picture evidence	Found Evidence: I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T6GT6XA0\11312502_845459245541990_1704121739_n[1].jpg	Pass
12-8	Instagram	Find viewed picture evidence in Instagram	Found Evidence: https://instagram.com/p/3xtNkYPIHN/ Source: I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	pass
12-9	Twitter	Find suspect's retweets	No Evidence Found	Fail

Appendix 9 – Second Case Scenario: Analysis of RAM Using Belkasoft Evidence Center (Test Plan 3)

TEST PLAN 3 (Belkasoft Evidence Center)

Test Number: 003

Examiner: Saud Alshaifi

Test Title: Analysis of RAM acquired from the suspect's PC (Jason Lopiz), in the second case scenario using Belkasoft Evidence Center.

Test Date: 23/6/2015

Purpose and Scope

After finishing with the first and second test plans for case scenario 1. This test plan and the fourth test plan is made for the second case scenario where LinkedIn and Bayt were used as OSNSs. Belkasoft can analyse different OSNSs including LinkedIn & Bayt from several artefacts. The purpose of this test plan is to examine the RAM acquired from the second case scenario by using Belkasoft Evidence Center to finding Forensic Evidence.

Requirements

- 1) The Created RAM Image using FTK imager should be successfully recognized by Belkasoft Evidence Center.
- 2) Calculation of MD5 hash value by Belkasoft is needed to ensure the integrity of the image being examined. Belkasoft should prevent any process that might affect image integrity.
- 3) After a successful recognition of the RAM image in Belkasoft, the tool should successfully analyse the image.
- 4) All the evidence generated in the second case scenario should be extracted by Belkasoft Evidence Center by analysing the suspect's RAM. The evidence should be found on all the three browsers used for LinkedIn and Bayt activities.

Description of Methodology

The same methodology used in test plan 1 is used in this test plan. The only difference is the control data in this test plan that need to be examined is for the second case scenario where LinkedIn and Bayt are performed. FTK imager is used to acquire RAM after activities is simulated, and MD5 and SHA1 were calculated for integrity assurance and validations. And then creating a new case in belkasoft Evidence Center for evidence analysis and findings.

Expected Results

- 1) Belkasoft will successfully find evidence posted in LinkedIn via Firefox, Chrome, and IE
- 2) Belkasoft will successfully find evidence posted in Bayt via Firefox, Chrome, and IE

Test Scenarios - Belkasoft Evidence Center – RAM – LinkedIn on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
13-2	LinkedIn	Find posted evidence on suspect's wall	Found Evidence: Only found suspect wall URL but not the post URL https://www.linkedin.com/hp/?dnt=qoWZFUztyUIQwfvvdo29qjNtyUyeyYWDC9R Source: firefox.exe	Fail
13-3	LinkedIn	Find Uploaded Picture	Found Evidence: https://image-store.slidesharecdn.com/5ab72fca-35cb-4b9f-b1c1-0f1b22022243-original.jpeg Source: firefox.exe	Pass
13-4	LinkedIn	Find posted comment on picture	No Evidence Found	Fail
13-5	LinkedIn	Find picture likes	No Evidence Found	Fail
13-6	LinkedIn	Find sent messages	Found Evidence: Only found the sent message ID But not the actual message sent https://www.linkedin.com/inbox/#detail?itemId=I6019021968123125760_500&trk=COMM_N Source: firefox.exe Also found URL of viewed profile friends https://www.linkedin.com/profile/view?id=276450954&authType=name&authToken=aFH Source: firefox.exe	Fail

Test Scenarios - Belkasoft Evidence Center – RAM – LinkedIn on Chrome				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
14-2	LinkedIn	Find posted evidence on suspect's wall	No Evidence Found	Fail
14-3	LinkedIn	Find Uploaded Picture	No Evidence Found	Fail
14-4	LinkedIn	Find posted comment on picture	No Evidence Found	Fail
14-5	LinkedIn	Find picture likes	No Evidence Found	Fail
14-6	LinkedIn	Find sent messages	No Evidence Found	Fail

Test Scenarios - Belkasoft Evidence Center – RAM – LinkedIn on IE				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
15-2	LinkedIn	Find posted evidence on suspect's wall	No Evidence Found	Fail
15-3	LinkedIn	Find Uploaded Picture	Found Evidence: https://image-store.slidesharecdn.com/71713020-5a66-4b25-a305-47a7bfc1f2e7-original.jpeg	Pass
15-4	LinkedIn	Find posted comment on picture	No Evidence Found	Fail
15-5	LinkedIn	Find picture likes	No Evidence Found	Fail
15-6	LinkedIn	Find sent messages	No Evidence Found	Fail

Test Scenarios - Belkasoft Evidence Center – RAM – Bayt on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
16-2	Bayt	Find question posted as evidence	No Evidence found	Fail
16-3	Bayt	Find recommendation made	No Evidence found	Fail
16-4	Bayt	Find answer to the question as evidence	No Evidence found	Fail
16-5	Bayt	Find Direct messaging with friend	No Evidence found	Fail

Test Scenarios - Belkasoft Evidence Center – RAM – Bayt on Chrome				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
17-2	Bayt	Find question posted as evidence	No Evidence found	Fail
17-3	Bayt	Find recommendation made	No Evidence found	Fail
17-4	Bayt	Find answer to the question as evidence	No Evidence found	Fail
17-5	Bayt	Find Direct messaging with friend	Found Evidence: Only friend's ID found http://people.bayt.com/saud-alshaifi/#submit-alert-message And Replied URL ID http://www.bayt.com/en/mymailbox-j/#inbox/p1/12686714/ but the message is not extracted Source: chrome.exe	Fail

Test Scenarios - Belkasoft Evidence Center – RAM – Bayt on IE				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
18-2	Bayt	Find question posted as evidence	Found Evidence: http://www.bayt.com/en/specialties/q/205292/generate-question-as-evidence-in-bayt-using-ie/?first_p=1&fb_share=0	Pass
18-3	Bayt	Find recommendation made	No Evidence found	Fail
18-4	Bayt	Find answer to the question as evidence	No Evidence found	Fail
18-5	Bayt	Find Direct messaging with friend	Found Evidence: Only found URL for mailbox http://www.bayt.com/en/mymailbox-j/ Also found URL of viewed profile friends http://people.bayt.com/saud-alshaifi/	Fail

Appendix 10 – Second Case Scenario: Analysis of Hard Drive Using Belkasoft Evidence Center (Test Plan 4)

TEST PLAN 4 (Belkasoft Evidence Center)

Test Number: 004

Examiner: Saud Alshaifi

Test Title: Examination of Hard drive of the Second Case Scenario (Jason Lopiz) using Belkasoft Evidence Center.

Test Date: 25/6/2015

Purpose and Scope

The previous test plan is for analysing RAM in case scenario 2. The purpose of this fourth test plan is to find further evidence from the suspect's hard drive precisely Finding Evidence from Bayt and LinkedIn from the three browsers.

Requirements

- 1) The created hard disk image by Tableau Imager should successfully be recognized by Belkasoft Evidence Center.
- 2) Calculation of MD5 is needed before attempt to perform analysis, in order to ensure integrity process.
- 3) The added forensic image should be write protected by Belkasoft Evidence Center.
- 4) Belkasoft should examine the image evidence created by tableau Imager type .E01.
- 5) The extraction of all the simulation of data in the second case scenario should be achieved by belkasoft Evidence Center, all the activities performed in the three browsers should be extracted for LinkedIn and Bayt via examination of the hard drive.

Description of Methodology

The methodology used in test plan 2 for examining hard drive is used in this test plan. The procedure of seizure, collection of data, write blocker is used, ensure safety for Hard drive, and original evidence image. The only change here is the simulation of data is done on LinkedIn and Bayt is this is for the second case scenario. Belkasot is used for this test plan for examinations and analysis of evidence.

Expected Results

- 1) Belkasoft will successfully find evidence posted in LinkedIn via IE, Chrome and Firefox
- 2) Belkasoft will successfully find evidence posted in Bayt via IE, Chrome and Firefox

Test Scenarios - Belkasoft Evidence Center – hard drive – LinkedIn on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
19-2	LinkedIn	Find posted evidence on suspect's wall	No Evidence found	Fail
19-3	LinkedIn	Find Uploaded Picture	Found Evidence: https://image-store.slidesharecdn.com/5ab72fca-35cb-4b9f-b1c1-0f1b22022243-original.jpeg Source: K:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\zjhbp3me.default\cache2\entries\2886f17fe270506ce798200878ebe450da40188c	Pass
19-4	LinkedIn	Find posted comment on picture	No Evidence found	Fail
19-5	LinkedIn	Find picture likes	No Evidence found	Fail
19-6	LinkedIn	Find sent messages	Found Evidence: subject; Generate message to friend evidence in LinkedIn using Firefox test post 3 Source: K:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\zjhbp3me.default & Found inbox URL accessed via Firefox https://www.linkedin.com/inbox Source: K:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\zjhbp3me.default\cache2\entries\b0ad6bb4f1bd5a718bc65394e0913e040d5d263a	Pass

Test Scenarios - Belkasoft Evidence Center – hard drive – LinkedIn on Chrome				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
20-2	LinkedIn	Find posted evidence on suspect's wall	Partially found: https://www.linkedin.com/pulse/activities/jason-lopiz0_2ztCMRzInOC3PZ2mpC63_v?trk=nav_responsive_sub_nav_yourupdates Jason Lopiz sales team member at Gold-Star LinkedIn	Fail
20-3	LinkedIn	Find Uploaded Picture	Found Evidence: https://image-store.slidesharecdn.com/4db78fe0-b17c-44a5-b164-0d6be97727d5-original.jpeg Source: K:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3	Pass
20-4	LinkedIn	Find posted comment on picture	No Evidence Found	Fail
20-5	LinkedIn	Find picture likes	No Evidence Found	Fail
20-6	LinkedIn	Find sent messages	No Evidence Found	Fail

Test Scenarios - Belkasoft Evidence Center – hard drive – LinkedIn on IE				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
21-2	LinkedIn	Find posted evidence on suspect's wall	No Evidence Found	Fail

21-3	LinkedIn	Find Uploaded Picture	Found Evidence: https://image-store.slidesharecdn.com/71713020-5a66-4b25-a305-47a7bfc1f2e7-original.jpeg Source: K:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	Pass
21-4	LinkedIn	Find posted comment on picture	No Evidence found	Fail
21-5	LinkedIn	Find picture likes	No Evidence found	Fail
21-6	LinkedIn	Find sent messages	No Evidence found	Fail

Test Scenarios - Belkasoft Evidence Center – hard drive – Bayt on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
22-2	Bayt	Find question posted as evidence	Found Evidence: http://www.bayt.com/en/specialties/q/205279/question-as-evidence-in-bayt-using-firefox-test-post-1/?first_p=1&fb_share=0 Question as evidence in Bayt using Firefox test post 1? - Bayt.com Specialties; Source: Firefox Session Store	Pass
22-3	Bayt	Find recommendation made	Found Evidence: Partially found the recommended person's username http://googleads.g.doubleclick.net/pagead/viewthroughconversion/1059390244/?random=1435116442902&cv=7&fst=1435116442902&num=1&fmt=1&label=0gYgCMYlrwcQpIaU-OM&guid=ON&u_h=800&u_w=1280&u_ah=760&u_aw=1280&u_cd=24&u_his=5&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&frm=0&url=http%3A//people.bayt.com/saud-alshaifi/&ref=http%3A//www.bayt.com/en/my-recommendations/&vis=1; Evidence path: K:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\zjhbp3me.default\cache2\entries\b12359084e23c9c69801e2059c70e7838aa7c00e	Fail
22-4	Bayt	Find answer to the question as evidence	Found Evidence: http://www.bayt.com/en/specialties/q/205279/question-as-evidence-in-bayt-using-firefox-test-post-1/?feed=top_stories#answer_70660; Source: NTFS	Pass
22-5	Bayt	Find Direct messaging with friend	Found Evidence: subject; Generate message to friend evidence in Bayt using Firefox test post 4 Evidence Path: K:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\zjhbp3me.default	Pass

Test Scenarios - Belkasoft Evidence Center – hard drive – Bayt on Chrome				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
23-2	Bayt	Find question posted as evidence	Found Evidence: http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?first_p=1&fb_share=0; Source: K:\Users\admin\AppData\Local\Google\Chrome\User Data\Default	Pass
23-3	Bayt	Find recommendation made	Found Evidence: Partially found recommendation URL http://www.bayt.com/en/my-recommendations/ Source: K:\Users\admin\AppData\Local\Google\Chrome\User Data\Default	Fail
23-4	Bayt	Find answer to the question as evidence	Found Evidence: http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?feed=top_stories#answer_706618 Source: K:\Users\admin\AppData\Local\Google\Chrome\User Data\Default	Pass
23-5	Bayt	Find Direct messaging with friend	Found Evidence: Partially found URL and Friend Username http://people.bayt.com/saud-alshaifi/#submit-alert-message Source: K:\Users\admin\AppData\Local\Google\Chrome\User Data\Default	Fail

Test Scenarios - Belkasoft Evidence Center – hard drive – Bayt on IE				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
24-2	Bayt	Find question posted as evidence	Found Evidence: http://www.bayt.com/en/specialties/q/205292/generate-question-as-evidence-in-bayt-using-ie/?feed=top_stories Source: K:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	Pass
24-3	Bayt	Find recommendation made	Found Evidence: Only found URL: http://www.bayt.com/en/my-recommendations/ Source: K:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	Fail
24-4	Bayt	Find answer to the question as evidence	No Evidence Found	Fail
24-5	Bayt	Find Direct messaging with friend	No Evidence Found	Fail

Appendix 11 – First Case Scenario: Belkasoft Report for evidence found on Facebook & Instagram from RAM (Findings for test plan 1)



Report information

Common information

Generated at 29/06/2015 9:44:12 p.m.
Generated by Saud Alahsifi

Case properties

Name forensics case1 analysis of suspect 1 RAM
Description Examination of the Live Memory of the suspect's computer
Created at 15/06/2015 3:16:06 p.m.
Created by saud alshaifi
Time zone (UTC+12:00) Auckland, Wellington

Report options

Sorting Earlier first
Grouping None
Dates All history

Profile properties

Name test1_Livememory_suspect.001
Path D:\test1 Memory acquisition\test1_Livememory_suspect.001
Data source D:\test1 Memory acquisition\test1_Livememory_suspect.001
Profile type Carver data
Created at 15/06/2015 3:22:38 p.m.
Time zone (UTC+12:00) Auckland, Wellington

Chrome Live RAM

URL	Location	Offset	Length
https://www.facebook.com/photo.php?fbid=107391949599925&set=a.106187259720394.1073741827.100009873604315&type=1&theater	D:\test1 Memory acquisition\pagefile.sys	447953544	130
https://www.facebook.com/hanan.alsalem.58?fref=tl_fr_box&pnref=lhc.fri	D:\test1 Memory acquisition\pagefile.sys	295783632	85
https://www.facebook.com/100009873604315/videos/vb.100009873604315/107392542933199/?type=2&theater¬if_t=video_processed	D:\test1 Memory acquisition\pagefile.sys	446459288	133
https://www.facebook.com/photo.php?fbid=106225229716597&set=a.106225223049931.1073741828.100009873604315&type=1&theater	chrome.exe	606093712	130
https://instagram.com/smithvolkov/	D:\test1 Memory acquisition\pagefile.sys	270642160	45
https://instagram.com/p/3xtHtjPIG2/?taken-by=smithvolkov	D:\test1 Memory acquisition\pagefile.sys	619522800	67

Facebook Messenger Live RAM

Time (UTC)	Message	Sender id	Recipient id	Location	Offset	Length
15/06/2015 12:49:55 p.m.	that is so nice, so i be in you thesis haha good luck my cute husband	10000136 8946250	1000098736 04315	D:\test1 Memory acquisition\page file.sys	614132 565	1077
15/06/2015 12:59:02 p.m.	what you mean	10000136 8946250	1000098736 04315	D:\test1 Memory acquisition\page file.sys	662758 152	1021

Firefox






URL	Visit count	Page title	Typed count	Location	Offset	Length
https://www.facebook.com/photo.php?fbid=107391609599959&set=a.106225223049931.1073741828.100009873604315&type=pe=	0	rSmith Volko	0	firefox.exe	43884625	281
https://www.facebook.com/photo.php?fbid=107389486266838&set=a.106187259720394.1073741827.100009873604315&type=1&theate	46	rSmith Volko	0	firefox.exe	43885369	283
https://www.facebook.com/100009873604315/videos/vb.100009873604315/107391359599984/?type=2&theater¬if_t=video_	0	dSmith Volko	0	firefox.exe	72864012	284
https://instagram.com/p/3xtHtjPIG2	0	/Smith Volkov on Instagram: "this is instagram shared in facebook	0	firefox.exe	72863668	251
https://instagram.com/accounts/login	0	/Smith Volkov on Instagram: "this is instagram shared in facebook	0	firefox.exe	43884309	253
https://www.facebook.com/hanan.alsalem.58?fref=tl_fr_box&pnref=lhc.friend	0	sHanan Alsale	0	firefox.exe	72864426	237





Internet Explorer 10

URL	Last Modified Time (UTC)	Last Accessed Time (UTC)	Location	Offset	Length
Visited: admin@https://instagram.com/p/3xtHtjPIG2/	2015.06.15 01:09:25	2015.06.15 01:09:26	svchost.exe	1256860	144
Visited: admin@https://www.facebook.com/messages/?ajaxpipe=1&ajaxpipe_token=AXhV7F_wR5W-0dVz&quickling[version]=1784025;0;&__user=100009873604315&__a=1&__dyn=7AmajEyl2lm9o-t2u5bHaEWy6zECiq78hAKGgyi8DCqrWU8ponUKedwOhEyfyUnwPUS2O4K5e8Dx53588z4qqaBGZ28GbLV8W&__req=jsonp	2015.06.15 01:05:56	2015.06.15 01:05:56	D:\test1 Memory acquisition\ pagefile.sys	8970496 42	626
Visited: admin@https://www.facebook.com/hanan.alsalem.58?fref=tl_fr_box&pnref=lhc.friends&ajaxpipe=1&ajaxpipe_token=AXhV7F_wR5W-0dVz&quickling[version]=1784025;0;&__user=100009873604315&__a=1&__dyn=7AmajEyl2lm9o-t2u5bHaEWy6zECiq78hAKGgyi8DCqrWU8popyUWu396y8-bxu3fzob8iUkUyu4kckwychFEGmHQ8yEK_AzE&__r	2015.06.15 01:05:10	2015.06.15 01:05:10	D:\test1 Memory acquisition\ pagefile.sys	8970482 44	706

Profile properties

Name Pictures
Path Pictures
Data source D:\test1 Memory acquisition\pagefile.sys
Profile type Pictures
Created at 15/06/2015 3:26:06 p.m.
Time zone (UTC+12:00) Auckland, Wellington

Picture	Picture size in pixels	Path	Created (UTC)	Modified (UTC)	Size
	640 x 640	D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\376.jpg			62875
	320 x 240	D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\470.jpg			12522
	375 x 225	D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\126.jpg			15044
	375 x 225	D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\442.jpg			14827
	157 x 118	D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\511.jpg			4976

	110 x 110	D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\120.jpg	4600
	375 x 225	D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\75.jpg	14802
	375 x 225	D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\122.jpg	14683
	640 x 640	D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\151.jpg	62978

Appendix 12 – First Case Scenario: Belkasoft Report for evidence found on Twitter & Instagram from RAM (Findings for Test Plan 1)



Report information

Common information

Generated at 29/06/2015 11:16:22 p.m.
Generated by Saud Alahsifi

Case properties

Name forensics case1 analysis of suspect 1 RAM
Description Examination of the Live Memory of the suspect's computer
Created at 15/06/2015 3:16:06 p.m.
Created by saud alshaifi
Time zone (UTC+12:00) Auckland, Wellington

Report options

Sorting Earlier first
Grouping None
Dates All history

Profile properties

Name test1_Livememory_suspect.001
Path D:\test1 Memory acquisition\test1_Livememory_suspect.001
Data source D:\test1 Memory acquisition\test1_Livememory_suspect.001
Profile type Carver data
Created at 15/06/2015 3:22:38 p.m.
Time zone (UTC+12:00) Auckland, Wellington

Chrome Live RAM

URL	Location	Offset	Length
https://instagram.com/p/3xtNkYPIHN/	chrome.exe	574765608	46
https://twitter.com/AlshaifiS	chrome.exe	74976588	40

Firefox

URL	Visit count	Page title	Typed count	Location	Offset	Length
https://instagram.com/p/3xtNkYPIHN	0	/Instagram photo by Smith Volkov • Invalid date at Invalid dat	0	firefox.exe	43883090	246
https://twitter.com/AlshaifiS	1		0	firefox.exe	228342072	40

Firefox Session Store

URL	Topic	Location	Offset	Length
https://twitter.com/smithvolko1/status/610253537465925632/photo/1	smithvolkov on Twitter: \	firefox.exe	344827322	110

Internet Explorer 10



URL	Last Modified Time (UTC)	Last Accessed Time (UTC)	Location	Offset	Length
Visited: admin@https://twitter.com/smithvolko1/status/610256647156412416/photo/1	2015.06.15 01:24:45	2015.06.15 01:24:45	taskhost.exe	76111	204
Visited: admin@https://instagram.com/p/3xtNkYPIHN/	2015.06.15 01:21:44	2015.06.15 01:29:34	taskhost.exe	2465864	144

Twitter Live RAM

Time	Message	Sender Id	Location	Offset	Length
15/06/2015 1:11:13 p.m.	lang="en" data-aria-label-part="0">Generate Ev. using Firefox, Tweeting in Twitter is very nice	smithvolko1	D:\test1 Memory acquisition\page file.sys	842998712	1472
15/06/2015 1:18:23 p.m.	lang="en" data-aria-label-part="0">Generate Ev. using chrom, Tweeting in Twitter is very nice	smithvolko1	D:\test1 Memory acquisition\page file.sys	842980613	1060
15/06/2015 12:11:04 p.m.	lang="en" data-aria-label-part="0">@nzherald Wonder what sort of salary increases top NZ journalists got this year - and how that affects their reporting?	Suzyiam	firefox.exe	31495934	1257
15/06/2015 12:35:07 p.m.	lang="en" data-aria-label-part="0">???I can???t even??? is a confession interrupted http://nyti.ms/1I9RLUR p	nytimes	D:\test1 Memory acquisition\page file.sys	241667457	1510
15/06/2015 12:40:29 p.m.	lang="en" data-aria-label-part="0">Editorial: Labour will win back its supporters http://nzh.nu/Oj3Vd 	nzherald	D:\test1 Memory acquisition\page file.sys	241647047	1504
15/06/2015 1:24:31 p.m.	lang="en" data-aria-label-part="0">Generate Ev. Using IE Tweeting in Twitter is very nice	smithvolko1	SearchProtocol	480497720	2910
15/06/2015 1:18:57 p.m.	lang="und" data-aria-label-part="0">pic.twitter.com\ONI3k5XAr7	smithvolko1	chrome.exe	379282044	3146

Profile properties

Name Pictures
Path Pictures
Data source D:\test1 Memory acquisition\pagefile.sys
Profile type Pictures
Created at 15/06/2015 3:26:06 p.m.
Time zone (UTC+12:00) Auckland, Wellington

Picture	Picture size in pixels	Path	Created (UTC)	Modified (UTC)	Size
	375 x 225	D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\389.jpg			15356
	375 x 225	D:\belkasoft cases\forensics case 1\forensics case1 analysis of suspect 1 RAM\forensics case1 analysis of suspect 1 RAM\215\Jpeg\432.jpg			15127

Appendix 13 – First Case Scenario: Belkasoft Report for evidence found on Facebook & Instagram from Hard Drive (Findings for Test Plan 2)



Report information

Common information

Generated at 30/06/2015 12:35:16 a.m.
Generated by Saud Alahsifi

Case properties

Name forensics case2 analysis of suspect 1 HD
Description Examination of the Hard Drive of the suspect's computer
Created at 17/06/2015 6:32:05 p.m.
Created by saud alshaifi
Time zone (UTC+12:00) Auckland, Wellington

Report options

Sorting Earlier first
Grouping None
Dates All history

Profile properties

Name IMAGE-suspect1-harddrive.E01
Path D:\suspect1 hard disk\IMAGE-suspect1-harddrive.E01
Data source D:\suspect1 hard disk\IMAGE-suspect1-harddrive.E01
Profile type Browsers
Created at 17/06/2015 6:36:32 p.m.
Time zone (UTC+12:00) Auckland, Wellington





Link	Cache	Location	Fetch Count
https://fbcdn-profile-a.akamaihd.net/hprofile-ak-xat1/v/t1.0-1/p160x160/11159962_106185986387188_3447611650442873588_n.jpg?oh=d88081d179ae0b0f1c29f34d399c562c&oe=55F64555&__gda__=1441600379_021ca8ea5a8ace8daed18faca2958262		I:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\8ez4wa3i.default\cache2\entries\6207ece090c815f2b092349f937ef0b2635fb870	2
https://scontent-lax1-1.xx.fbcdn.net/hphotos-xat1/v/t1.0-9/111393087_106187236387063_2759516425629086158_n.jpg?oh=cda7b148a070badd8bc50a696e6d6d39&oe=5629DD79		I:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\8ez4wa3i.default\cache2\entries\4d2357ae5f12be38cf6d6152ab04f8699d3fac12	1
https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11374779_914991828542812_1414951129_n.jpg		I:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\8ez4wa3i.default\cache2\entries\11867d59bda6affbe1e0767b56e08c1f2381db8d	1
https://scontent-lax1-1.xx.fbcdn.net/hphotos-xft1/v/t1.0-9/11425855_107391949599925_6391389738211779334_n.jpg?oh=477468cb2594b99bf21b27d12eeb2575&oe=55F800E3		I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3	0
https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11374779_914991828542812_1414951129_n.jpg		I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\00004A	0
https://fbcdn-sphotos-b-a.akamaihd.net/hphotos-ak-xtf1/v/t1.0-9/11407100_107392949599825_1997037522158782039_n.jpg?oh=5a4b48eafe97f229ae2b6de1449e96ba&oe=55F6B044&__gda__=1446151455_501780dacec66e0e34f80f5f14600292		I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE556GGEP5W\11407100_107392949599825_1997037522158782039_n[1].jpg	1
https://fbcdn-sphotos-g-a.akamaihd.net/hphotos-ak-xat1/v/t1.0-9/11401437_106219636383823_5785327220111996688_n.jpg?oh=62b81a63fd2e3b9415f109d4479b6a7c&oe=55E7B2EB&__gda__=1446082612_29171c540e6edacfa26169f4aeb2183b		I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE556GGEP5W\11401437_106219636383823_5785327220111996688_n[1].jpg	1




URLs

Link	Last visit time (UTC)	Access count	Page name	Location
https://www.facebook.com/100009873604315/videos/vb.100009873604315/107392542933199/?type=2&theater¬if_t=video_processed	15/06/2015 1:01:10 p.m.	1		I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sites
https://instagram.com/p/3xtHtjPIG2/	15/06/2015 1:02:33 p.m.	2	Smith Volkov on Instagram: "this is instagram shared in facebook"	I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sites
https://instagram.com/smithvolkov/	15/06/2015 1:01:45 p.m.	2		I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sites
https://instagram.com/p/3xtHtjPIG2/	15/06/2015 1:09:25 p.m.	1		I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

Profile properties

Name Pictures
Path Pictures
Data source D:\suspect1 hard disk\IMAGE-suspect1-harddrive.E01
Profile type Pictures
Created at 17/06/2015 6:34:33 p.m.
Time zone (UTC+12:00) Auckland, Wellington

Picture	Picture size in pixels	Path	Created (UTC)	Modified (UTC)	Size
	256 x 154	D:\belkasoft cases\forensics case 2 - suspect1 hard drive\forensics case2 analysis of suspect 1 HD\forensics case2 analysis of suspect 1 HD\23\Jpeg\229.jpg			10530
	256 x 154	D:\belkasoft cases\forensics case 2 - suspect1 hard drive\forensics case2 analysis of suspect 1 HD\forensics case2 analysis of suspect 1 HD\23\Jpeg\233.jpg			10384
	320 x 240	D:\belkasoft cases\forensics case 2 - suspect1 hard drive\forensics case2 analysis of suspect 1 HD\forensics case2 analysis of suspect 1 HD\23\Jpeg\1\1037.jpg			8474
	375 x 225	D:\belkasoft cases\forensics case 2 - suspect1 hard drive\forensics case2 analysis of suspect 1 HD\forensics case2 analysis of suspect 1 HD\23\Jpeg\1\1039.jpg			14827

 <p>Browser: IE website: Facebook Picture Evidence</p>	375 x 225	D:\belkasoft cases\forensics case 2 - suspect1 hard drive\forensics case2 analysis of suspect 1 HD\forensics case2 analysis of suspect 1 HD\23\Jpeg\1\1038.jpg	14802			
 <p>Browser: IE website: Facebook Video Evidence</p>	375 x 225	D:\belkasoft cases\forensics case 2 - suspect1 hard drive\forensics case2 analysis of suspect 1 HD\forensics case2 analysis of suspect 1 HD\23\Jpeg\1\1036.jpg	14683			
 <p>App:Instagram Instagram to facebook share Picture Evidence</p>	526 x 526	I:\Users\admin\AppData\Local \Microsoft\Windows\Temporar y Internet Files\Low\Content.IE5\T6GT6 XA0\11247720_10739160959 9959_8789731246890578286 _n[1].jpg	15/06/20 15 1:08:01 p.m.	15/06/20 15 1:08:01 p.m.	30868	

**Appendix 14 – First Case Scenario: Belkasoft Report for evidence found on
Twitter & Instagram from Hard Drive (Findings for Test Plan 2)**



Report information

Common information

Generated at 30/06/2015 1:39:42 a.m.
Generated by Saud Alahsifi

Case properties

Name forensics case2 analysis of suspect 1 HD
Description Examination of the Hard Drive of the suspect's computer
Created at 17/06/2015 6:32:05 p.m.
Created by saud alshaifi
Time zone (UTC+12:00) Auckland, Wellington

Report options

Sorting Earlier first
Grouping None
Dates All history

Profile properties

Name IMAGE-suspect1-harddrive.E01
Path D:\suspect1 hard disk\IMAGE-suspect1-harddrive.E01
Data source D:\suspect1 hard disk\IMAGE-suspect1-harddrive.E01
Profile type Browsers
Created at 17/06/2015 6:36:32 p.m.
Time zone (UTC+12:00) Auckland, Wellington



Link	Cache Location	Fetch Count
https://pbs.twimg.com/profile_images/608869050056253441/WCCRY2dd_bi_gger.jpg	I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_2	0
https://pbs.twimg.com/media/CHgR34sUsAA-sLd.jpg:large	I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3	0
https://igcdn-photos-g-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11312502_845459245541990_1704121739_n.jpg	I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\l_000053	0
https://pbs.twimg.com/media/CHgOW4WVEAAR_IB.jpg	I:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\8ez4wa3i.default\cache2\entries\50ab9effb0164027baf29e14749475b8e085311f	6
https://pbs.twimg.com/profile_images/608869050056253441/WCCRY2dd.jpg	I:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\8ez4wa3i.default\cache2\entries\3589a80ec798ed81e250e6e43f0cc225661b59a9	1

URLs

Link	Last visit time (UTC)	Access count	Page name	Location
https://instagram.com/p/3xtNkYPIHN/	15/06/2015 1:21:44 p.m.	1		I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default
https://twitter.com/smithvolko1/status/610256647156412416/photo/1	15/06/2015 1:24:45 p.m.	1		I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
https://instagram.com/p/3xtNkYPIHN/	15/06/2015 1:29:59 p.m.	3	Smith Volkov on Instagram:	I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
https://twitter.com/AlshaifiS	15/06/2015 1:20:12 p.m.	1	Saud (@AlshaifiS) Twitter	I:\Users\admin\AppData\Local\Google\Chrome\User Data\Default

Profile properties

Name Pictures
Path Pictures
Data source D:\suspect1 hard disk\IMAGE-suspect1-harddrive.E01
Profile type Pictures
Created at 17/06/2015 6:34:33 p.m.
Time zone (UTC+12:00) Auckland, Wellington

Picture	Picture size in pixels	Path	Created (UTC)	Modified (UTC)	Size
	375 x 225	D:\belkasoft cases\forensics case 2 - suspect1 hard drive\forensics case2 analysis of suspect 1 HD\forensics case2 analysis of suspect 1 HD\23\Jpeg\1\1045.jpg			15127
	640 x 640	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T6GT6XAXA0\11312502_845459245541990_1704121739_n[1].jpg	15/06/2015 1:28:30 p.m.	15/06/2015 1:28:30 p.m.	62984

Appendix 15 – Second Case Scenario: Belkasoft Report for evidence found on LinkedIn from RAM (Findings for Test Plan 3)



Report information

Common information

Generated at 30/06/2015 4:33:07 p.m.
Generated by Saud Alahsifi

Case properties

Name forensics case3 analysis of suspect 2 RAM
Description This case is to analyse the RAM acquired from Case scenario 2 suspect 2
Created at 23/06/2015 10:59:06 p.m.
Created by saud alshaifi
Time zone (UTC+12:00) Auckland, Wellington

Report options

Sorting Earlier first
Grouping None
Dates All history

Profile properties

Name test2_Livememory_suspect2.001
Path D:\test2 Memory Acquisition\test2_Livememory_suspect2.001
Data source D:\test2 Memory Acquisition\test2_Livememory_suspect2.001
Profile type Carver data
Created at 23/06/2015 11:00:23 p.m.
Time zone (UTC+12:00) Auckland, Wellington

Firefox

URL	Visit count	Page title	Typed count	Location	Offset	Length
https://www.linkedin.com/profile/view?id=276450954&authType=name&authToken=aFH	0	=saud alshaifi LinkedI	0	firefox.exe	12833863	261
https://www.linkedin.com/inbox/?goto=messages&trk=nav_utilities_	0	xInbox LinkedI	0	firefox.exe	12833589	235
https://www.linkedin.com/inbox/#detail?itemId=I6019021968123125760_500&trk=COMM_N			0	firefox.exe	12832883	250
https://www.linkedin.com/hp/?dnr=qoWZFUztyUIQwfvvdo29qjNtyUyeyYWDc9R			0	firefox.exe	12834749	238
https://image-store.slidesharecdn.com/5ab72fca-35cb-4b9f-b1c1-0f1b22022243-original.jpeg	0	g5ab72fca-35cb-4b9f-b1c1-0f1b22022243-original.jpeg (JPEG Image, 375 x 225 pixels)	0	firefox.exe	12834377	336

Internet Explorer Live RAM

URL	Name	Offset	Length
https://image-store.slidesharecdn.com/71713020-5a66-4b25-a305-47a7bfc1f2e7-original.jpeg	ÄÜ	76282114	640

**Appendix 16 – Second Case Scenario: Belkasoft Report for evidence found on
Bayt from RAM (Findings for Test Plan 3)**



Report information

Common information

Generated at 30/06/2015 5:13:19 p.m.
Generated by Saud Alahsifi

Case properties

Name forensics case3 analysis of suspect 2 RAM
Description This case is to analyse the RAM acquired from Case scenario 2 suspect 2
Created at 23/06/2015 10:59:06 p.m.
Created by saud alshaifi
Time zone (UTC+12:00) Auckland, Wellington

Report options

Sorting Earlier first
Grouping None
Dates All history

Profile properties

Name test2_Livememory_suspect2.001
Path D:\test2 Memory Acquisition\test2_Livememory_suspect2.001
Data source D:\test2 Memory Acquisition\test2_Livememory_suspect2.001
Profile type Carver data
Created at 23/06/2015 11:00:23 p.m.
Time zone (UTC+12:00) Auckland, Wellington

Chrome Live RAM

URL	Location	Offset	Length
http://people.bayt.com/saud-alshaifi/#submit-alert-message	chrome.exe	461314258	68
http://www.bayt.com/en/mymailbox-j/#inbox/p1/12686714/	chrome.exe	93020206	64
https://www.bayt.com/en/login/	chrome.exe	556162052	41
http://people.bayt.com/saud-alshaifi/	chrome.exe	626143945	47

Internet Explorer Live RAM

URL	Name	Location	Offset	Length
http://www.bayt.com/en/specialties/q/205292/generate-question-as-evidence-in-bayt-using-ie/?first_p=1&fb_share=0	Ã¸	wisptis.exe	76282972	586
http://www.bayt.com/en/specialties/dashboard/	Ã¸	wisptis.exe	76283441	436
http://www.bayt.com/en/mymailbox-j/	Ã¸	wisptis.exe	76281177	412
http://people.bayt.com/saud-alshaifi/	Ã¸	wisptis.exe	76280858	416

**Appendix 17 – Second Case Scenario: Belkasoft Report for evidence found on
LinkedIn from Hard Drive (Findings for Test Plan 4)**



Report information

Common information

Generated at 1/07/2015 7:23:14 a.m.
Generated by Saud Alahsifi

Case properties

Name forensics case4 analysis of suspect 2 HD
Description Hard drive analysis of suspect 2
Created at 25/06/2015 5:53:20 p.m.
Created by saud alshaifi
Time zone (UTC+12:00) Auckland, Wellington

Report options

Sorting Earlier first
Grouping None
Dates All history

Profile properties

Name	IMAGE_suspect2_harddrive.E01
Path	D:\suspect2 hard disk\IMAGE_suspect2_harddrive.E01
Data source	D:\suspect2 hard disk\IMAGE_suspect2_harddrive.E01
Profile type	Browsers
Created at	25/06/2015 5:55:37 p.m.
Time zone	(UTC+12:00) Auckland, Wellington

Cache

Link	Location	Fetch Count
https://image-store.slidesharecdn.com/4db78fe0-b17c-44a5-b164-0d6be97727d5-original.jpeg	K:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3	0
https://image-store.slidesharecdn.com/5ab72fca-35cb-4b9f-b1c1-0f1b22022243-original.jpeg	K:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\zjhbp3me.default\cache2\entries\2886f17fe270506ce798200878ebe450da40188c	3
https://media.licdn.com/mpr/mpr/shrinknp_100_100/AEEAAQAA AAAAALsAAAAJGU0NjI4ZDRiLT11NzAtNGM0OS05NjY0LTZmOThhMWE3NDIkYg.jpg	K:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\zjhbp3me.default\cache2\entries\cefb4a646da80ab3a6a26881a07451fb79c26210	1
https://www.linkedin.com/inbox/	K:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\zjhbp3me.default\cache2\entries\b0ad6bb4f1bd5a718bc65394e0913e040d5d263a	0

Form Values

Field name	Value	Location
subject	Generate message to friend evidence in LinkedIn using Firefox test post 3	K:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\zjhbp3me.default

Passwords

Login	Password	Host name
jasonlopiz@hotmail.com	jason@123	https://www.linkedin.com

URLs

Link	Last visit time (UTC)	Access count	Page name	Location
https://image-store.slidesharecdn.com/71713020-5a66-4b25-a305-47a7bfc1f2e7-original.jpeg	23/06/2015 8:17:53 p.m.	3		K:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

Profile properties




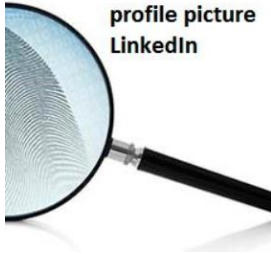
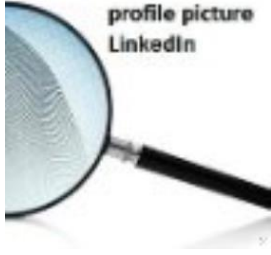
Name NTFS
Path D:\suspect2 hard disk\IMAGE_suspect2_harddrive.E01
Data source D:\suspect2 hard disk\IMAGE_suspect2_harddrive.E01
Profile type Carver data
Created at 25/06/2015 5:54:04 p.m.
Time zone (UTC+12:00) Auckland, Wellington

Chrome

Time (UTC)	URL	Visit count	Page title	Typed count	Offset	Length
23/06/2015 8:8:54 p.m.	https://www.linkedin.com/pulse/activities/jason-lopiz0_2ztCMRzInOC3PZ2mpC63_v?trk=nav_responsive_sub_nav_yourupdates	0	Jason Lopiz sales team member at Gold-Star LinkedIn	0	3557218857	289

Profile properties

Name Pictures
Path Pictures
Data source D:\suspect2 hard disk\IMAGE_suspect2_harddrive.E01
Profile type Pictures
Created at 25/06/2015 5:54:04 p.m.
Time zone (UTC+12:00) Auckland, Wellington

Picture	Picture size in pixels	Path	Created (UTC)	Modified (UTC)	Size
	375 x 225	D:\belkasoft cases\forensics case4 -scenario2-suspect 2 hard drive\forensics case4 analysis of suspect 2 HD\forensics case4 analysis of suspect 2 HD\23\Jpeg\2\1638.jpg			14899
	100 x 100	D:\belkasoft cases\forensics case4 -scenario2-suspect 2 hard drive\forensics case4 analysis of suspect 2 HD\forensics case4 analysis of suspect 2 HD\23\Jpeg\3\858.jpg			3211
	375 x 225	D:\belkasoft cases\forensics case4 -scenario2-suspect 2 hard drive\forensics case4 analysis of suspect 2 HD\forensics case4 analysis of suspect 2 HD\23\Jpeg\1\4.jpg			14692
	225 x 225	D:\belkasoft cases\forensics case4 -scenario2-suspect 2 hard drive\forensics case4 analysis of suspect 2 HD\forensics case4 analysis of suspect 2 HD\23\Jpeg\2\1649.jpg			10414
	100 x 100	D:\belkasoft cases\forensics case4 -scenario2-suspect 2 hard drive\forensics case4 analysis of suspect 2 HD\forensics case4 analysis of suspect 2 HD\23\Jpeg\3\1942.jpg			3211



256 x 154

D:\belkasoft cases\forensics
case4 -scenario2-suspect 2
hard drive\forensics case4
analysis of suspect 2
HD\forensics case4 analysis
of suspect 2
HD\23\Jpeg\4\1501.jpg

10238

**Appendix 18 – Second Case Scenario: Belkasoft Report for evidence found on
Bayt from Hard Drive (Findings for Test Plan4)**



Report information

Common information

Generated at 1/07/2015 8:12:22 a.m.
Generated by Saud Alahsifi

Case properties

Name forensics case4 analysis of suspect 2 HD
Description Hard drive analysis of suspect 2
Created at 25/06/2015 5:53:20 p.m.
Created by saud alshaifi
Time zone (UTC+12:00) Auckland, Wellington

Report options

Sorting Earlier first
Grouping None
Dates All history

Profile properties

Name IMAGE_suspect2_harddrive.E01
Path D:\suspect2 hard disk\IMAGE_suspect2_harddrive.E01
Data source D:\suspect2 hard disk\IMAGE_suspect2_harddrive.E01
Profile type Browsers
Created at 25/06/2015 5:55:37 p.m.
Time zone (UTC+12:00) Auckland, Wellington

URLs

Link	Last visit time (UTC)	Access count	Page name	Location
http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?first_p=1&fb_share=0	23/06/2015 8:36:10 p.m.	1	Generate question as evidence in Bayt using Chrome test post 1? - Bayt.com Specialties	K:\Users\admin\AppData\Local\Google\Chrome\User Data\Default
http://people.bayt.com/saud-alshaifi/#submit-alert-message	23/06/2015 8:43:16 p.m.	1	Saud Alshaifi - Public Profile at Bayt.com	K:\Users\admin\AppData\Local\Google\Chrome\User Data\Default
http://www.bayt.com/en/my-recommendations/	23/06/2015 8:39:40 p.m.	1	My Recommendations - Bayt.com	K:\Users\admin\AppData\Local\Google\Chrome\User Data\Default
http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?feed=top_stories#answer_706618	23/06/2015 8:41:50 p.m.	1	Generate question as evidence in Bayt using Chrome test post 1? - Bayt.com Specialties	K:\Users\admin\AppData\Local\Google\Chrome\User Data\Default
http://www.bayt.com/en/my-recommendations/	23/06/2015 8:56:25 p.m.	7		K:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
http://www.bayt.com/en/specialties/q/205292/generate-question-as-evidence-in-bayt-using-ie/?feed=top_stories	23/06/2015 8:50:59 p.m.	6		K:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

Cache			
Link	Location	Fetch Count	
http://googleads.g.doubleclick.net/pagead/viewthroughconversion/1059390244/?random=1435116442902&cv=7&fst=1435116442902&num=1&fmt=1&label=0gYgCMyLrwcQplaU-QM&guid=ON&u_h=800&u_w=1280&u_ah=760&u_aw=1280&u_cd=24&u_his=5&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&frm=0&url=http%3A//people.bayt.com/saud-alshaifi/&ref=http%3A//www.bayt.com/en/my-recommendations/&vis=1;	K:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\zjhbp3me.default\cache2\entries\b12359084e23c9c69801e2059c70e7838aa7c00e	1	

Form Values

Field name	Value	Location
subject	Generate message to friend evidence in Bayt using Firefox test post 4	K:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\zjhbp3me.default

Profile properties

Name NTFS
Path D:\suspect2 hard disk\IMAGE_suspect2_harddrive.E01
Data source D:\suspect2 hard disk\IMAGE_suspect2_harddrive.E01
Profile type Carver data
Created at 25/06/2015 5:54:04 p.m.
Time zone (UTC+12:00) Auckland, Wellington

Firefox

URL	Visit count	Page title	Typed count	Offset	Length
http://www.bayt.com/en/specialties/q/205279/question-as-evidence-in-bayt-using-firefox-test-post-1/?feed=top_stories#answer_70660	0	2Question as evidence in Bayt using Firefox test post 1? - Bayt.com Specialtie	0	2879162802	356

Firefox Session Store

URL	Topic	Offset	Length
http://www.bayt.com/en/specialties/q/205279/question-as-evidence-in-bayt-using-firefox-test-post-1/?first_p=1&fb_share=0	Question as evidence in Bayt using Firefox test post 1? - Bayt.com Specialties	2292541245	218

Appendix 19 – First Case Scenario: Analysis of RAM Using Internet Examiner Toolkit (Test Plan 5)

TEST PLAN 5 (Internet Examiner Toolkit)

Test Number: 005

Examiner: Saud Alshaifi

Test Title: Test of Internet Examiner Toolkit version 5.12 Beta for finding forensic evidence from the first case scenario Image RAM, Suspect: Smith Volkov

Test Date: 9/9/2015

Purpose and Scope

Internet Examiner Toolkit is a digital forensic tool developed by SiQuest, IXTK is an integrated suite of tools aimed specifically for identification, collection, analysis, and reporting forensic evidence activities conducted on the internet, the tool can perform investigation on computer based, mobile phones, and live cloud. It is currently being used by a wide range of digital forensic experts from police department, militaries, and academic institutes. The purpose of test plan 5 is to examine the RAM image created for the first case scenario using Internet Examiner Toolkit Instead of Belkasoft in order to make a comparison at the end between the digital forensic tools.

Requirements

- 1) Same image used in Test plan 1 in belkasoft is used in this test plan, IXTK should be able to recognize the same RAM image.
- 2) Internet Examiner Toolkit should be able to process the image and create hash values in order to compare it with the hash values created when the image was acquired.
- 3) Internet Examiner Toolkit must protect the image from being altered.
- 4) Internet Examiner should be able to analyse the RAM image through data carving method suggested by the vendor.
- 5) The simulated data in the first case scenario (Facebook, Twitter, Instagram) using the three selected web browsers should successfully reconstructed by Internet Examiner Toolkit through RAM analysis.

Description of Methodology

After finishing with the first digital forensic tool (Belkasoft Evidence Center) the investigator started using Internet Examiner Toolkit to find evidence from the same acquired digital forensic images created initially. Since there are 4 images. First Case scenario's RAM and HD, Second Case Scenario RAM & HD. The investigator started created the cases in IXTK and went through the steps described in IXTK User Guide. It is important to follow the same steps used in the first tool in order to draw a fair conclusion with fair answer to the research question proposed.

Expected Results

- 1) It is expected that IXTK will successfully extract all the activities conducted on Facebook using the three browsers.
- 2) It is expected that IXTK will successfully extract all the activities conducted on Twitter using the three browsers.
- 3) It is expected that IXTK will successfully extract all the activities conducted on Instagram using the three browsers.

Test Scenarios - Internet Examiner Toolkit - RAM - Facebook & Instagram on Firefox				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
25-2	Facebook	Find posted evidence on suspect's wall	No Evidence Found	Fail
25-3	Facebook	Find Uploaded Picture	No Evidence Found	Fail
25-4	Facebook	Find post on friend's wall	No Evidence Found	Fail
25-5	Facebook	Find Instant messaging with friend	No Evidence Found	Fail
25-6	Facebook	Find video evidence post	No Evidence Found	Fail
25-9	Facebook	Find shared Instagram picture evidence	https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11374779_914991828542812_1414951129_n.jpg Record_ID: 176903	Pass
25-10	Instagram	Find Instagram account of suspects logged in via Firefox	No Evidence Found	Fail
25-11	Instagram	Find viewed Instagram picture via Firefox	No Evidence Found	Fail

Test Scenarios - Internet Examiner Toolkit - RAM - Facebook & Instagram on Chrome				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
26-2	Facebook	Find posted evidence on suspect's wall	No Evidence Found	Fail
26-3	Facebook	Find Uploaded Picture	No Evidence Found	Fail
26-4	Facebook	Find post on friend's wall	No Evidence Found	Fail
26-5	Facebook	Find Instant messaging with friend	No Evidence Found	Fail
26-6	Facebook	Find video evidence post	No Evidence Found	Fail
26-7	Facebook	Find shared Instagram picture evidence	https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11374779_914991828542812_1414951129_n.jpg Record_ID: 162335	Pass
26-8	Instagram	Find Instagram account of suspects logged in via Chrome	No Evidence Found	Fail
26-9	Instagram	Find viewed Instagram picture via Chrome	No Evidence Found	Fail

Test Scenarios - Internet Examiner Toolkit - RAM - Facebook & Instagram on IE				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
27-2	Facebook	Find posted evidence on suspect's wall	No Evidence Found	Fail
27-3	Facebook	Find Uploaded Picture	No Evidence Found	Fail
27-4	Facebook	Find post on friend's wall	No Evidence Found	Fail
27-5	Facebook	Find Instant messaging with friend	No Evidence Found	Fail
27-6	Facebook	Find video evidence post	No Evidence Found	Fail
27-7	Facebook	Find shared Instagram picture evidence	https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-	Pass

			15/11374779_914991828542812_1414951129_n.jpg Record_ID: 140779	
27-8	Instagram	Find Instagram account of suspects logged in via IE	No Evidence Found	Fail
27-9	Instagram	Find viewed Instagram picture via IE	No Evidence Found	Fail

Test Scenarios - Internet Examiner Toolkit - RAM - Twitter & Instagram on Firefox				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
28-2	Twitter	Find posted evidence on Twitter	No Evidence Found	Fail
28-3	Twitter	Find uploaded photo in Twitter	No Evidence Found	Fail
28-4	Twitter	Find tweets in friends wall	No Evidence Found	Fail
28-5	Twitter	Find Direct messaging with friend	No Evidence Found	Fail
28-7	Twitter	Find shared Instagram picture evidence	No Evidence Found	Fail
28-9	Instagram	Find viewed picture evidence in Instagram	https://igcdn-photos-g-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11312502_845459245541990_1704121739_n.jpg Record_ID: 517035	Pass
28-10	Twitter	Find suspect's retweets	No Evidence Found	Fail

Test Scenarios - Internet Examiner Toolkit - RAM - Twitter & Instagram on Chrome				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
29-2	Twitter	Find posted evidence on Twitter	No Evidence Found	Fail
29-3	Twitter	Find uploaded photo in Twitter	No Evidence Found	Fail
29-4	Twitter	Find tweets in friends wall	No Evidence Found	Fail
29-5	Twitter	Find Direct messaging with friend	No Evidence Found	Fail
29-6	Twitter	Find shared Instagram picture evidence	No Evidence Found	Fail
29-8	Instagram	Find viewed picture evidence in Instagram	https://igcdn-photos-g-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11312502_845459245541990_1704121739_n.jpg Record_ID: 185348	Pass
29-9	Twitter	Find suspect's retweets	No Evidence Found	Fail

Test Scenarios - Internet Examiner Toolkit - RAM - Twitter & Instagram on IE				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
30-2	Twitter	Find posted evidence on Twitter	No Evidence Found	Fail
30-3	Twitter	Find uploaded photo in Twitter	No Evidence Found	Fail
30-4	Twitter	Find tweets in friends wall	No Evidence Found	Fail

30-5	Twitter	Find Direct messaging with friend	No Evidence Found	Fail
30-6	Twitter	Find shared Instagram picture evidence	No Evidence Found	Fail
30-8	Instagram	Find viewed picture evidence in Instagram	https://igcdn-photos-g-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11312502_845459245541990_1704121739_n.jpg Record_ID: 146372	pass
30-9	Twitter	Find suspect's retweets	No Evidence Found	Fail

Appendix 20 – First Case Scenario: Analysis of Hard Drive Using Internet Examiner Toolkit (Test Plan 6)

TEST PLAN 6 (Internet Examiner Toolkit)

Test Number: 006

Examiner: Saud Alshaifi

Test Title: Test of IXTK version 5.12 Beta for finding evidence from the first Scenario Image Hard Drive, OSNs: Instagram, Twitter, and Facebook, and Suspect: Smith Volkov

Test Date: 17/9/2015

Purpose and Scope

The purpose of Test plan 6 is to analyse the same image examined in test plan 2, where the image is for case scenario 1 Hard Drive, which is created using Write blocker and Tableau Imager. The same image again used with different digital forensic tool which is internet examiner toolkit, in order to find out which tool would suit when conducting forensic investigation on Facebook, Instagram and Twitter, where the source of evidence is the hard drive.

Requirements

- 1) IXTK should recognize the same image used in test plan 2.
- 2) IXTK should be able to process the image and create the hash sets.
- 3) The image must be write blocked by IXTK
- 4) Analysis of the image must be conducted using data carving method in IXTK
- 5) IXTK should be successful in extracted the evidence from suspect's HD.

Description of Methodology

Since the same images is used in all the digital forensic tools, this test plan will use the same image used in test plan 2. Since IXTK require mounting of evidence before searching, the evidence will be mounted as a physical drive, then the important artefacts will be selected in order to perform the analysis, some unwanted artefacts were needed to be excluded in order to minimise the time of search since IXTK search every sector within the image. After analysis, searching and bookmarks is conducted to find relevant information in the data pane and then report the findings.

Expected Results

- 1) It is expected that IXTK will successfully extract all the activities conducted on Facebook using the three browsers.
- 2) It is expected that IXTK will successfully extract all the activities conducted on Twitter using the three browsers.
- 3) It is expected that IXTK will successfully extract all the activities conducted on Instagram using the three browsers.

Test Scenarios - Internet Examiner Toolkit - hard drive- Facebook & Instagram on Firefox				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
31-2	Facebook	Find posted evidence on suspect's wall	No Evidence Found	Fail
31-3	Facebook	Find Uploaded Picture	No Evidence Found	Fail
31-4	Facebook	Find post on friend's wall	No evidence found	Fail
31-5	Facebook	Find Instant messaging with friend	Partially found the messages sent to friend Screenshot partially found (See Figure 4.14) Record_ID: 28935	Fail
31-6	Facebook	Find video evidence post	No Evidence Found	Fail
31-9	Facebook	Find shared Instagram picture evidence	No Evidence Found	Fail
31-10	Instagram	Find Instagram account of suspects logged in via Firefox	No Evidence Found	Fail
31-11	Instagram	Find viewed Instagram picture via Firefox	No Evidence Found	Fail

Test Scenarios - Internet Examiner Toolkit - hard drive- Facebook & Instagram on Chrome				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
32-2	Facebook	Find posted evidence on suspect's wall	No Evidence found	Fail
32-3	Facebook	Find Uploaded Picture	No Evidence Found	Fail
32-4	Facebook	Find post on friend's wall	No Evidence found	Fail
32-5	Facebook	Find Instant messaging with friend	Partially found message sent to friend on Chrome (See Figure 4.15) Screenshot partially found Record_ID ID: 29527	Fail
32-6	Facebook	Find video evidence post	Found the picture file name: 11331778_107392609599859_678060524_n[1].jpg Path: I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\CSQM77NR\11331778_107392609599859_678060524_n[1].jpg Record_ID: 4946	Pass
32-7	Facebook	Find shared Instagram picture evidence	No Evidence Found	Fail
32-8	Instagram	Find Instagram account of suspects logged in via Chrome	No Evidence Found	Fail
32-9	Instagram	Find viewed Instagram picture via Chrome	No Evidence Found	Fail

Test Scenarios - Internet Examiner Toolkit - hard drive- Facebook & Instagram on IE				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result

33-2	Facebook	Find posted evidence on suspect's wall	No Evidence found	Fail
33-3	Facebook	Find Uploaded Picture	Found the picture file name: 11407100_107392949599825_1997037522158782039_n[1].jpg Path: I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11407100_107392949599825_1997037522158782039_n[1].jpg Record_ID: 4867	Pass
33-4	Facebook	Find post on friend's wall	No Evidence Found	Fail
33-5	Facebook	Find Instant messaging with friend	No Evidence Found	Fail
33-6	Facebook	Find video evidence post	Found the video file name: 11401437_106219636383823_5785327220111996688_n[1].jpg Path: I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11401437_106219636383823_5785327220111996688_n[1].jpg Record_ID: 4866	Pass
33-7	Facebook	Find shared Instagram picture evidence	Found the picture file name: 1908153_106225229716597_2637932451814024505_n[1].jpg Source: I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\CSQM77NR\1908153_106225229716597_2637932451814024505_n[1].jpg Record_ID: 4939	Pass
33-8	Instagram	Find Instagram account of suspects logged in via IE	No Evidence Found	Fail
33-9	Instagram	Find viewed Instagram picture via IE	Found Evidence: https://instagram.com/p/3xtHtjPIG2/ Path: I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat Record_ID: 7796	pass

Test Scenarios - Internet Examiner Toolkit - hard drive- Twitter & Instagram on Firefox				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
34-2	Twitter	Find posted evidence on Twitter	No Evidence Found	Fail

34-3	Twitter	Find uploaded photo in Twitter	Found the picture file name: CHMlk11UIAENEDx[1].jpg Path: I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\CHMlk11UIAENEDx[1].jpg Record_ID: 4893	Pass
34-4	Twitter	Find tweets in friends wall	No evidence found	Fail
34-5	Twitter	Find Direct messaging with friend	No Evidence found	Fail
34-7	Twitter	Find shared Instagram picture evidence	No Evidence found	Fail
34-9	Instagram	Find viewed picture evidence in Instagram	No Evidence found	Fail
34-10	Twitter	Find suspect's retweets	No Evidence found	Fail

Test Scenarios - Internet Examiner Toolkit - hard drive- Twitter & Instagram on Chrome

Test Number /event #	Social network	Expected result	Source of evidence	Actual result
35-2	Twitter	Find posted evidence on Twitter	No Evidence Found	Fail
35-3	Twitter	Find uploaded photo in Twitter	Found the picture on https://twitter.com/smithvolko1/status/610255124145967106/photo/1 Path: I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat Record_ID: 7771	Pass
35-4	Twitter	Find tweets in friends wall	No Evidence Found	Fail
35-5	Twitter	Find Direct messaging with friend	No Evidence Found	Fail
35-6	Twitter	Find shared Instagram picture evidence	No Evidence Found	Fail
35-8	Instagram	Find viewed picture evidence in Instagram	No Evidence Found	Fail
35-9	Twitter	Find suspect's retweets	No Evidence Found	Fail

Test Scenarios - Internet Examiner Toolkit - hard drive- Twitter & Instagram on IE

Test Number /event #	Social network	Expected result	Source of evidence	Actual result
36-2	Twitter	Find posted evidence on Twitter	Only found Username on Twitter and wall page: https://twitter.com/smithvolko1 I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat Record_ID: 6026	Fail

36-3	Twitter	Find uploaded photo in Twitter	Only found Profile Picture on I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11159962_106185986387188_3447611650442873588_n[1].jpg Record_ID: 4838	Fail
36-4	Twitter	Find tweets in friends wall	No evidence found	Fail
36-5	Twitter	Find Direct messaging with friend	No evidence found	Fail
36-6	Twitter	Find shared Instagram picture evidence	No Evidence found	Fail
36-8	Instagram	Find viewed picture evidence in Instagram	Evidence Found: https://instagram.com/p/3xtNkYPIHN/ path: I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat Record_ID: 6001	pass
36-9	Twitter	Find suspect's retweets	No Evidence Found	Fail

Appendix 21 – Second Case Scenario: Analysis of Hard Drive Using Internet Examiner Toolkit (Test Plan 8)

TEST PLAN 8 (Internet Examiner Toolkit)

Test Number: 008

Examiner: Saud Alshaifi

Test Title: 2nd Case Scenario, Hard Disk analysis Using Internet Examiner Toolkit (IXTK).

OSNs: LinkedIn, Bayt, and Suspect: Jason Lopiz

Test Date: 26/9/2015

Purpose and Scope

The purpose of Test Plan 8 is to examine the same Image used in Test plan 4, where the image is for Case Scenario 2 Hard Drive. However, in this test plan the image is being analysed using the second digital forensic tool (Internet Examiner Toolkit), In order to find out how much Evidence can be found from each of the tool. This will certainly help in findings, and giving recommendation when conducting a forensic investigation on LinkedIn and Bayt Social Networking Sites.

Requirements

- 1) The same Image used in test plan 4 should be recognized by IXTK via mounting process.
- 2) Creating the hash values should be done in Internet Examiner Toolkit.
- 3) After mounting image, IXTK should ensure evidence will not be changed or being altered by counting hash values.
- 4) Through Data Carving in IXTK, the image must be analysed to find forensic evidence.
- 5) Reconstruction of evidence or simulated data in the Second case scenario and evidence reporting should be achieved using Internet Examiner Toolkit.

Description of Methodology

This test plan intended for the hard drive image created for the second case scenario, which was previously examined by Belkasoft in test plan 4. This image will be mounted as physical drive in IXTK as it needs to be mounted first in order to be examined. Then choosing the artefacts needed and excluded the once that are not needed such as searching for Visa cards, Searching for mobile social networking apps and other artefacts such as YouTube activities. This procedure is highly recommended by the vendors as the searching may take a while in order to finish the whole sectors search, clean carving is also recommend which will be conducted. Then, Reconstruction of the evidence, searching through Hex will be made, bookmarking the relevant once to report the relevant data instead of reporting the whole data in the data pane.

Expected Results

- 1) Internet Examiner Toolkit will successfully find evidence posted in LinkedIn via IE, Chrome and Firefox
- 2) Internet Examiner Toolkit will successfully find evidence posted in Bayt via IE, Chrome and Firefox

Test Scenarios - Internet Examiner Toolkit – hard drive – LinkedIn on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
43-2	LinkedIn	Find posted evidence on suspect's wall	No Evidence found	Fail
43-3	LinkedIn	Find Uploaded Picture	No Evidence found	Fail
43-4	LinkedIn	Find posted comment on picture	No Evidence found	Fail
43-5	LinkedIn	Find picture likes	No Evidence found	Fail
43-6	LinkedIn	Find sent messages	No Evidence found	Fail

Test Scenarios - Internet Examiner Toolkit – hard drive – LinkedIn on Chrome				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
44-2	LinkedIn	Find posted evidence on suspect's wall	No Evidence found	Fail
44-3	LinkedIn	Find Uploaded Picture	No Evidence found	Fail
44-4	LinkedIn	Find posted comment on picture	No Evidence found	Fail
44-5	LinkedIn	Find picture likes	No Evidence found	Fail
44-6	LinkedIn	Find sent messages	No Evidence found	Fail

Test Scenarios - Internet Examiner Toolkit – hard drive – LinkedIn on IE				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
45-2	LinkedIn	Find posted evidence on suspect's wall	Only found profile picture of the suspect: \\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QPLEAEU8\AAEAAQAAAAAAAAALsAAAAJGU0NjI4ZDRiLTl1NzAtNGM0OS05NjY0LTZmOThhMWE3NDlkYg[1].jpg Record_ID: 293	Fail
45-3	LinkedIn	Find Uploaded Picture	Evidence is found: \\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\MPRP85WH\71713020-5a66-4b25-a305-47a7bfc1f2e7-original[1].jpg Record_ID: 224	Pass
45-4	LinkedIn	Find posted comment on picture	No Evidence found	Fail
45-5	LinkedIn	Find picture likes	No Evidence found	Fail
45-6	LinkedIn	Find sent messages	No Evidence found	Fail

Test Scenarios - Internet Examiner Toolkit – hard drive – Bayt on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
46-2	Bayt	Find question posted as evidence	No Evidence found	Fail
46-3	Bayt	Find recommendation made	No Evidence found	Fail
46-4	Bayt	Find answer to the question as evidence	No Evidence found	Fail
46-5	Bayt	Find Direct messaging with friend	No Evidence found	Fail

Test Scenarios - Internet Examiner Toolkit – hard drive – Bayt on Chrome				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
47-2	Bayt	Find question posted as evidence	No Evidence found	Fail
47-3	Bayt	Find recommendation made	No Evidence found	Fail
47-4	Bayt	Find answer to the question as evidence	No Evidence found	Fail
47-5	Bayt	Find Direct messaging with friend	No Evidence found	Fail

Test Scenarios - Internet Examiner Toolkit – hard drive – Bayt on IE				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
48-2	Bayt	Find question posted as evidence	No Evidence found	Fail
48-3	Bayt	Find recommendation made	No Evidence found	Fail
48-4	Bayt	Find answer to the question as evidence	No Evidence found	Fail
48-5	Bayt	Find Direct messaging with friend	Only found profile picture of the suspect: \\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\G0E76ZUI\29424820_20150623073738[2].jpg Record_ID: 67	Fail

Appendix 22 – First Case Scenario: IXTK Report for Evidence found on
Facebook, Twitter & Instagram from RAM (Findings for Test Plan 5)



Internet Examiner Toolkit – Pictures Report

IN THE MATTER OF:	Smith Volkov
Case Number:	001
Author:	Saud Alshaifi
Organization:	
Time Created:	Tuesday, September 15, 2015 20:20:02 (+12:00)
Time Zone Setting:	Times are displayed in (UTC+12:00) Auckland, Wellington

RECORDS

Record 1 of 6



RECORD COLUMN	COLUMN VALUE
Record_ID	517035
Activity	Recovered
Time	15/09/2015 4:47:11 p.m
TimeUTC	15/09/2015 4:47:11 a.m.
Brand	twitter logo
Icon	digital camera
Type	Photo Url
Url	https://igcdn-photos-g-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11312502_845459245541990_1704121739_n.jpg
Visits	1

Record 2 of 6



RECORD COLUMN	COLUMN VALUE
Record_ID	185348
Activity	Recovered
Time	14/09/2015 5:25:29 p.m.
TimeUTC	14/09/2015 5:25:29 a.m.
Brand	twitter logo
Icon	digital camera
Type	Photo Url
Url	https://igcdn-photos-g-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11312502_845459245541990_1704121739_n.jpg
Visits	1

Record 3 of 6



RECORD COLUMN	COLUMN VALUE
Record_ID	176903
Activity	Recovered
Time	14/09/2015 5:09:46 p.m.
TimeUTC	14/09/2015 5:09:46 a.m.
Brand	facebook logo
Icon	digital camera
Type	Photo Url
Url	https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11374779_914991828542812_1414951129_n.jpg
Visits	1

Record 4 of 6



RECORD COLUMN	COLUMN VALUE
Record_ID	162335
Activity	Recovered
Time	14/09/2015 4:44:17 p.m
TimeUTC	14/09/2015 4:44:17 a.m.
Brand	facebook logo
Icon	digital camera
Type	Photo Url
Url	https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11374779_914991828542812_1414951129_n.jpg
Visits	1



RECORD COLUMN	COLUMN VALUE
Record_ID	146372
Activity	Recovered
Time	14/09/2015 4:18:00 p.m.
TimeUTC	14/09/2015 4:18:00 a.m
Brand	twitter logo
Icon	digital camera
Type	Photo Url
Url	https://igcdn-photos-g-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11312502_845459245541990_1704121739_n.jpg
Visits	1



RECORD COLUMN	COLUMN VALUE
Record_ID	140779
Activity	Recovered
Time	14/09/2015 4:09:33 p.m.
TimeUTC	14/09/2015 4:09:33 a.m
Brand	facebook logo
Icon	digital camera
Type	Photo Url
Url	https://igcdn-photos-e-a.akamaihd.net/hphotos-ak-xaf1/t51.2885-15/11374779_914991828542812_1414951129_n.jpg
Visits	1

Report created using Internet Examiner Toolkit Version 5.12.1507.2818

Disclaimer:	
Contact:	
Legal Notice:	

**Appendix 23 – First Case Scenario: IXTK Report for Evidence Found on
Facebook, Twitter & Instagram from HD (Findings for Test Plan 6)**



Internet Examiner Toolkit – Pictures Report

IN THE MATTER OF:	Smith Volkov
Case Number:	002
Author:	Saud Alshaifi
Organization:	
Time Created:	Monday, September 21, 2015 19:42:03 (+12:00)
Time Zone Setting:	Times are displayed in (UTC+12:00) Auckland, Wellington

RECORDS

Record 1 of 12



RECORD COLUMN	COLUMN VALUE
Record_ID	4893
Activity	Imported
ArtifactBrand	Internet Explorer
ArtifactType	
FileOriginalPath	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\CHMIk11UIAENEDx[1].jpg
RecordType	File
Status	Imported
Subject	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\CHMIk11UIAENEDx[1].jpg

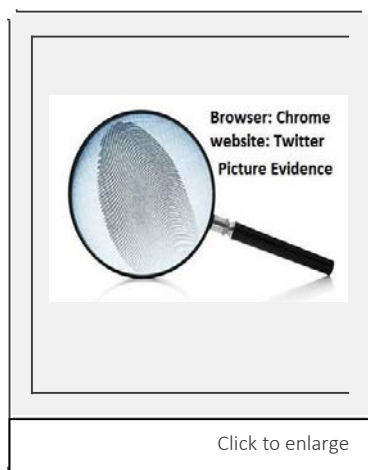
Url	file:///I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\CHMlkl1UIAENEDx[1].jpg
Visits	1

Record 2 of 12



RECORD COLUMN	COLUMN VALUE
Record_ID	7796
Activity	Accessed
ArtifactBrand	Internet Explorer
ArtifactType	Cache
FileOriginalPath	I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
Host	instagram.com
RecordType	Cache
Status	Cached
Subject	https://instagram.com/p/3xtHtjPIG2/
SubjectMD5	8086AFBCA5207E2C168F5D3CD416A552
SubjectSHA1	DB8DCF98F87BE61AD7F8F52A4B7CB8271DDD1D5C
Url	https://instagram.com/p/3xtHtjPIG2/
Visits	1

Record 3 of 12



RECORD COLUMN	COLUMN VALUE
Record_ID	7771
Activity	Accessed
ArtifactBrand	Internet Explorer
ArtifactType	Cache
FileOriginalPath	I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
Host	twitter.com
RecordType	Cache
Status	Cached
Subject	https://twitter.com/smithvolko1/status/610255124145967106/photo/1
SubjectMD5	55A1800774EE9F67FE6418168311F7AC
SubjectSHA1	A8DC61F4528494846C0CDD6F2BDF7C1E14F65B57
Url	https://twitter.com/smithvolko1/status/610255124145967106/photo/1

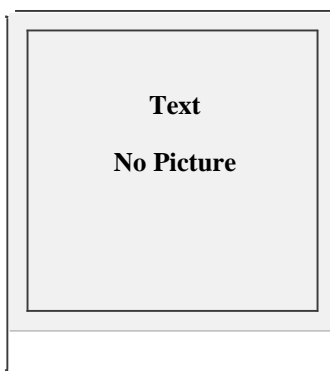
Visits	1
--------	---

Record 4 of 12



RECORD COLUMN	COLUMN VALUE
Record_ID	6001
Activity	Accessed
ArtifactBrand	Internet Explorer
ArtifactType	History
FileOriginalPath	I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
Host	instagram.com
RecordType	History
Status	Visited
Subject	https://instagram.com/p/3xtNkYPIHN/
SubjectMD5	0BF1EAD9AB494E93D0A7F5A3A4F7ADFA
SubjectSHA1	F18AB180B895C4EEEF7426EF85B515ADE9D9B64B
Url	https://instagram.com/p/3xtNkYPIHN/
Visits	1

Record 5 of 12





RECORD COLUMN	COLUMN VALUE
Record_ID	6026
Activity	Accessed
ArtifactBrand	Internet Explorer
ArtifactType	History
FileOriginalPath	I:\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
Host	twitter.com
RecordType	History
Status	Visited
Subject	https://twitter.com/smithvolko1
SubjectMD5	AA938D93DDDEF9D559BA04863B113FA3
SubjectSHA1	DOE200F43C72EC952349B85A33DE66F50CC595D1
Url	https://twitter.com/smithvolko1
Visits	4

Record 6 of 12





Click to enlarge

RECORD COLUMN	COLUMN VALUE
Record_ID	4838
Activity	Imported
ArtifactBrand	 Internet Explorer
ArtifactType	
FileOriginalPath	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11159962_106185986387188_3447611650442873588_n[1].jpg
Host	
RecordType	File
Status	Imported
Subject	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11159962_106185986387188_3447611650442873588_n[1].jpg
SubjectMD5	
SubjectSHA1	
Url	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11159962_106185986387188_3447611650442873588_n[1].jpg
Visits	0

Record 7 of 12

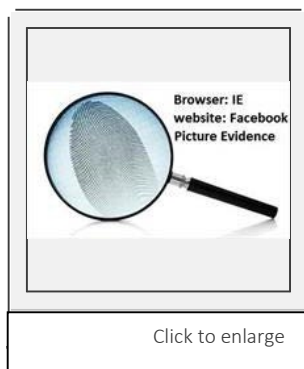


Click to enlarge

RECORD COLUMN	COLUMN VALUE
Record_ID	4866
Activity	Imported
ArtifactBrand	 Internet Explorer
ArtifactType	
FileOriginalPath	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11401437_106219636383823_5785327220111996688_n[1].jpg
Host	
RecordType	File
Status	Imported
Subject	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11401437_106219636383823_5785327220111996688_n[1].jpg
SubjectMD5	
SubjectSHA1	

Url	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11401437_106219636383823_5785327220111996688_n[1].jpg
Visits	0

Record 8 of 12



RECORD COLUMN	COLUMN VALUE
Record_ID	4867
Activity	Imported
ArtifactBrand	Internet Explorer
ArtifactType	
FileOriginalPath	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11407100_107392949599825_1997037522158782039_n[1].jpg
Host	
RecordType	File
Status	Imported
Subject	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11407100_107392949599825_1997037522158782039_n[1].jpg
SubjectMD5	
SubjectSHA1	
Url	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11407100_107392949599825_1997037522158782039_n[1].jpg
Visits	0

Record 9 of 12



RECORD COLUMN	COLUMN VALUE
Record_ID	4939
Activity	Imported
ArtifactBrand	Internet Explorer
ArtifactType	
FileOriginalPath	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\CSQM77NR\1908153_106225229716597_2637932451814024505_n[1].jpg

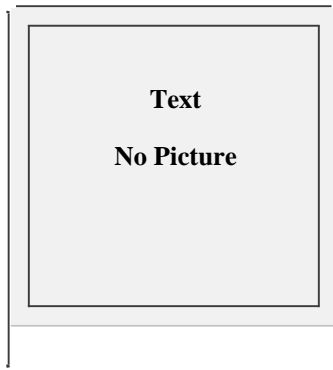
Host	
RecordType	File
Status	Imported
Subject	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\CSQM77NR\1908153_106225229716597_2637932451814024505_n[1].jpg
SubjectMD5	
SubjectSHA1	
Url	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\CSQM77NR\1908153_106225229716597_2637932451814024505_n[1].jpg
Visits	0



Record 10 of 12



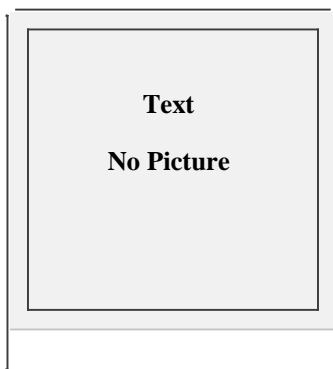
RECORD COLUMN	COLUMN VALUE
Record_ID	4946
Activity	Imported
ArtifactBrand	Internet Explorer
ArtifactType	
FileOriginalPath	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\CSQM77NR\11331778_107392609599859_678060524_n[1].jpg
Host	
RecordType	File
Status	Imported
Subject	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\CSQM77NR\11331778_107392609599859_678060524_n[1].jpg
SubjectMD5	
SubjectSHA1	
Url	I:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\CSQM77NR\11331778_107392609599859_678060524_n[1].jpg
Visits	0



Record 11 of 12



RECORD COLUMN	COLUMN VALUE
Record_ID	28935
Activity	Message
ArtifactBrand	 Facebook
ArtifactType	 Message Snippet
FileOriginalPath	
Host	
RecordType	Message Fragment
Status	Recovered
Subject	that is so nice, so i be in you thesis haha good luck my cute husband
SubjectMD5	D0CFC60D1C501FD3C26F811C22D76C58
SubjectSHA1	841564C0FB6D3EE5FD880FCAFEF82CC3BC1B01FB
Url	
Visits	1

Record 12 of 12



RECORD COLUMN	COLUMN VALUE
Record_ID	29527
Activity	Message
ArtifactBrand	 Facebook
ArtifactType	 Message Snippet
FileOriginalPath	
Host	
RecordType	Message Fragment
Status	Recovered
Subject	what you mean
SubjectMD5	E9392E9E7DC731D3AEF82B5E7FFAF674
SubjectSHA1	2BCC4D22886ADFB5AE5B0D567F222116A34AD464
Url	
Visits	1

Report created using Internet Examiner Toolkit Version 5.12.1507.2818

Disclaimer:	
Contact:	
Legal Notice:	

**Appendix 24 – Second Case Scenario: IXTK Report for Evidence Found on
LinkedIn & Bayt from HD (Findings for Test Plan 8)**

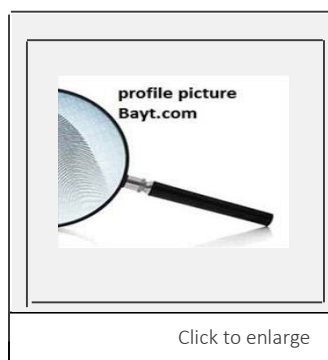


Internet Examiner Toolkit – Pictures Report

IN THE MATTER OF:	Jason Lopiz
Case Number:	004
Author:	Saud Alshaifi
Organization:	
Time Created:	Tuesday, September 29, 2015 19:04:55 (+13:00)
Time Zone Setting:	Times are displayed in New Zealand Daylight Time

RECORDS

Record 1 of 3



RECORD COLUMN	COLUMN VALUE
Record_ID	67
Activity	Imported
ArtifactBrand	Internet Explorer
ArtifactType	
FileMD5	4008408A152637B95EF0CC3D9798E94E
FileName	29424820_20150623073738[2].jpg
FileOriginalPath	\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\G0E76ZUI\29424820_20150623073738[2].jpg
Host	
RecordType	File
Status	Imported
Subject	\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet

	Files\Low\Content.IE5\G0E76ZUI\29424820_20150623073738[2].jpg
SubjectMD5	
SubjectSHA1	
Url	file:///\\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\G0E76ZUI\29424820_20150623073738[2].jpg
Visits	1

Record 2 of 3



RECORD COLUMN	COLUMN VALUE
Record_ID	224
Activity	Imported
ArtifactBrand	Internet Explorer
ArtifactType	
FileMD5	971E8A76FDEB2E5895ED574EF14CF7BC
FileName	71713020-5a66-4b25-a305-47a7bfc1f2e7-original[1].jpg
FileOriginalPath	\\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\MPRP85WH\71713020-5a66-4b25-a305-47a7bfc1f2e7-original[1].jpg
Host	
RecordType	File
Status	Imported
Subject	\\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\MPRP85WH\71713020-5a66-4b25-a305-47a7bfc1f2e7-original[1].jpg
SubjectMD5	
SubjectSHA1	
Url	file:///\\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\MPRP85WH\71713020-5a66-4b25-a305-47a7bfc1f2e7-original[1].jpg
Visits	2



RECORD COLUMN	COLUMN VALUE
Record_ID	293
Activity	Imported
ArtifactBrand	Internet Explorer
ArtifactType	
FileMD5	230B1FC7A801E2197F3EDCA2FDA4AA6C
FileName	AAEAAQAAAAAAAAAALsAAAAJGU0Nji4ZDRiLTl1NzAtNGM0OS05NjY0LTZmOThhMWE3NDlkYg
FileOriginalPath	\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QPLEAEU8\AAEAAQAAAAAAAAAALsAAAAJGU0Nji4ZDRiLTl1NzAtNGM0OS05NjY0LTZmOThhMWE3NDlkYg[1].jpg
Host	
RecordType	File
Status	Imported
Subject	\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QPLEAEU8\AAEAAQAAAAAAAAAALsAAAAJGU0Nji4ZDRiLTl1NzAtNGM0OS05NjY0LTZmOThhMWE3NDlkYg[1].jpg
SubjectMD5	
SubjectSHA1	
Url	file:///Users\admin\AppData\Local\Microsoft\Windows\Temporay Internet Files\Low\Content.IE5\QPLEAEU8\AAEAAQAAAAAALsAAAAJGU0Nji4ZDRiLTl1NzAtNGM0OS05NjY0LTZmOThhMWE3NDlkYg[1].jpg
Visits	0

Report created using Internet Examiner Toolkit Version 5.12.1507.2818

Disclaimer:	
Contact:	
Legal Notice:	

Appendix 25 – First Case Scenario: Analysis of RAM Using Internet Evidence Finder (Test Plan 9)

TEST PLAN 9 (Internet Evidence Finder)

Test Number: 009

Examiner: Saud Alshaifi

Test Title: Test for Internet Evidence Finder for the first case scenario, Suspect: Smith

Volkov Source of Evidence: RAM image

Test Date: 8/10/15

Purpose and Scope

Internet Evidence Finder is a digital forensic tool developed by Magnet Forensics (Formerly JADsoftware), which is one of the global leader in the development of forensic software that assist forensic investigators to recover a broad range of internet-related communications. IEF is currently used by many forensics professionals including world's top law enforcement, government, military, and corporate organizations. The main focus for IEF is to recover evidence from online social networks, webmail, and browser artefacts. According to Magnet, IEF is designed to investigate and recover forensic evidence from computers, smartphones, and tablets. After finishing with Internet examiner toolkit and generation of its reports, from test plan 5 to 8. This test plan 9 will be the first test plan for Internet Evidence Finder, this test plan will examine the RAM image acquired at the beginning of experiment, the purpose of examining the same image is to draw a conclusion on which of the three selected forensic tools is best suits when investigating Facebook, Twitter, and Instagram by examining the suspect RAM.

Requirements

- 1) The image examined in test plan 1 and test plan 5 should be also recognized by IEF
- 2) The image should be processed and hash values should be generated before attempt examining the source by IEF.
- 3) When processing the image, it should be write-blocked by Internet Evidence finder.
- 4) IEF should be able to analyse the image and find artefacts evidence from RAM.
- 5) The data generated in the 1st case scenario for the suspect smith volkov should be found by IEF, and reported.

Description of Methodology

The image created from RAM and examined by Belkasoft Evidence Center, and Internet Examiner Toolkit, will be also examined by Internet Evidence Finder. In Test plan 1 and test plan 5 we have seen a huge difference between the numbers of evidence extracted. Belkasoft performed better than IXTK. This test plan will be conducted to determine which of the selected tools would perform better in terms of examining RAM for finding Facebook, Twitter, and Instagram evidence posted in the first case scenario. The similar steps will be taking into considerations and reporting of found evidence will be generated after the test finished.

Expected Results

- 1) Internet Evidence Finder is expected to achieve and extract the evidence posted on Facebook via the three browsers.
- 2) Internet Evidence Finder is expected to achieve and extract the evidence posted on Twitter via the three browsers.
- 3) Internet Evidence Finder is expected to achieve and extract the shared links of Instagram on Facebook and twitter which are accessed via the three browsers.

Test Scenarios - Internet Evidence Finder - RAM - Facebook & Instagram on Firefox				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
49-2	Facebook	Find posted evidence on suspect's wall	No Evidence Found Only the Suspect wall page is found https://www.facebook.com/profile.php?id=100009873604315 Located at: Physical Sector 258528 Record Number 8	Fail
49-3	Facebook	Find Uploaded Picture	The uploaded picture is found: https://www.facebook.com/photo.php?fbid=107389486266838&set=a.106187259720394.1073741827.100009873604315&type=1&theater Located at: Physical Sector 295573 Record Number 11	Pass
49-4	Facebook	Find post on friend's wall	No Evidence Found Only Friend's profile is found https://www.facebook.com/hanan.alsalem.58?fref=tl_fr_box&pnref=lhc.friends Located at: Physical Sector 554940 Record Number 22	Fail
49-5	Facebook	Find Instant messaging with friend	Found only one message out of 6 done on Firefox See Figure 4.16 Located at File Offset 614132803 Source: Pagefile.sys Record Number 9	Fail
49-6	Facebook	Find video evidence post	The uploaded video is found: https://www.facebook.com/100009873604315/videos/vb.100009873604315/107391359599984/?type=2&theater&notif_t=video_processed Located at: Physical Sector 452728 Record Number 18	Pass
49-9	Facebook	Find shared Instagram picture evidence	The Picture is found: https://www.facebook.com/photo.php?fbid=107391609599959&set=a.106225223049931.1073741828.100009873604315&type=1&theater Located at: Physical Sector 70883 Record Number 5	Pass
49-10	Instagram	Find Instagram account of suspects logged in via Firefox	Evidence is found https://instagram.com/smithvolkov/ Located at: Physical Sector 1952081 Record Number 10	Pass
49-11	Instagram	Find viewed Instagram picture via Firefox	Evidence is found https://instagram.com/p/3xtHtjPIG2/?taken-by=smithvolkov Located at: Physical Sector 1952082 Record Number 11	Pass

Test Scenarios - Internet Evidence Finder - RAM - Facebook & Instagram on Chrome				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
50-2	Facebook	Find posted evidence on suspect's wall	No Evidence Found	Fail
50-3	Facebook	Find Uploaded Picture	Evidence is found	Pass

			https://www.facebook.com/photo.php?fbid=107391949599925&set=a.106187259720394.1073741827.100009873604315&type=1&theater Located at: File offset 327275474 Source: pagefile.sys Record Number 98	
50-4	Facebook	Find post on friend's wall	No Evidence Found	Fail
50-5	Facebook	Find Instant messaging with friend	Only found one message received from a friend out of 5 See Figure 4.16 Located at: File offset 662758390 Source: pagefile.sys Record Number 10	Fail
50-6	Facebook	Find video evidence post	Evidence is found https://www.facebook.com/100009873604315/videos/vb.100009873604315/107392542933199/?type=2&theater&notif_t=video_processed Located at: File offset 327275040 Source: pagefile.sys Record Number 94	Pass
50-7	Facebook	Find shared Instagram picture evidence	Evidence is found https://www.facebook.com/photo.php?fbid=106225229716597&set=a.106225223049931.1073741828.100009873604315&type=1&theater Located at: File offset 621721119 Source: pagefile.sys Record Number 108	Pass
50-8	Instagram	Find Instagram account of suspects logged in via Chrome	Evidence is found https://instagram.com/smithvolkov/ Located at: File offset 622044188 Source: pagefile.sys Record Number 30	Pass
50-9	Instagram	Find viewed Instagram picture via Chrome	Evidence is found https://instagram.com/p/3xtHtjPIG2/?taken-by=smithvolkov Located at: File offset 622044113 Source: pagefile.sys Record Number 29	Pass

Test Scenarios - Internet Evidence Finder - RAM - Facebook & Instagram on IE				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
51-2	Facebook	Find posted evidence on suspect's wall	No Evidence Found	Fail
51-3	Facebook	Find Uploaded Picture	No Evidence Found	Fail
51-4	Facebook	Find post on friend's wall	No Evidence Found	Fail
51-5	Facebook	Find Instant messaging with friend	Evidence is Found All the messages conducted on IE on Facebook Were successfully extracted (See Figure 4.16) Source: pagefile.sys Record Numbers 1 to 7	Pass
51-6	Facebook	Find video evidence post	No Evidence Found	Fail
51-7	Facebook	Find shared Instagram picture evidence	No Evidence Found	Fail

51-8	Instagram	Find Instagram account of suspects logged in via IE	No Evidence Found	Fail
51-9	Instagram	Find viewed Instagram picture via IE	Evidence is found https://instagram.com/p/3xtHtjPIG2/ Located At Physical Sector 764828 Record Number 9	Pass

Test Scenarios - Internet Evidence Finder - RAM - Twitter & Instagram on Firefox				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
52-2	Twitter	Find posted evidence on Twitter	Evidence is found https://twitter.com/smithvolko1/status/610253303985745920 Located at Physical Sector 10205 Record Number 4	Pass
52-3	Twitter	Find uploaded photo in Twitter	Picture is found https://twitter.com/smithvolko1/status/610253537465925632/photo/1 Located at: Physical Sector 64538 Record Number 2	Pass
52-4	Twitter	Find tweets in friends wall	No Evidence Found	Fail
52-5	Twitter	Find Direct messaging with friend	No Evidence Found	Fail
52-7	Twitter	Find shared Instagram picture evidence	No Evidence Found	Fail
52-9	Instagram	Find viewed picture evidence in Instagram	Picture is found https://instagram.com/p/3xtNkYPIHN/ Located at: Physical Sector 774438 Record Number 7	Pass
52-10	Twitter	Find suspect's retweets	No Evidence Found	Fail

Test Scenarios - Internet Evidence Finder - RAM - Twitter & Instagram on Chrome				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
53-2	Twitter	Find posted evidence on Twitter	Evidence is found https://twitter.com/smithvolko1/status/610254995993178112 Located at: Physical Sector 3065945 Record Number 255	Pass
53-3	Twitter	Find uploaded photo in Twitter	Picture is found https://twitter.com/smithvolko1/status/610257403028738050/photo/1 Located at: Physical Sector 474847 Record Number 47	Pass
53-4	Twitter	Find tweets in friends wall	No Evidence Found	Fail
53-5	Twitter	Find Direct messaging with friend	No Evidence Found	Fail

53-6	Twitter	Find shared Instagram picture evidence	No Evidence Found	Fail
53-8	Instagram	Find viewed picture evidence in Instagram	No Evidence Found	Fail
53-9	Twitter	Find suspect's retweets	No Evidence Found	Fail

Test Scenarios - Internet Evidence Finder - RAM - Twitter & Instagram on IE				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
54-2	Twitter	Find posted evidence on Twitter	Evidence is found https://twitter.com/smithvolko1/status/610256537047576576 Located at: Physical Sector 3065947 Record Number 258	Pass
54-3	Twitter	Find uploaded photo in Twitter	Picture is found https://twitter.com/smithvolko1/status/610256647156412416/photo/1 Located at: Physical Sector1926361 Record Number 167	Pass
54-4	Twitter	Find tweets in friends wall	No Evidence Found	Fail
54-5	Twitter	Find Direct messaging with friend	No Evidence Found	Fail
54-6	Twitter	Find shared Instagram picture evidence	No Evidence Found	Fail
54-8	Instagram	Find viewed picture evidence in Instagram	No Evidence Found	Fail
54-9	Twitter	Find suspect's retweets	No Evidence Found	Fail

Appendix 26 – First Case Scenario: Analysis of Hard Drive Using Internet Evidence Finder (Test Plan 10)

TEST PLAN 10 (Internet Evidence Finder)

Test Number: 010

Examiner: Saud Alshaifi

Test Title: Test for IEF to find forensic evidence from the suspect: smith Volkov, and source of evidence is his hard drive, First Case Scenario involve: Facebook, Twitter, Instagram.

Test Date: 15/10/15

Purpose and Scope

The purpose of test plan 10 is to examine the hard drive image which is previously examined by Belkasoft Evidence Center in test plan 2, and Internet Examiner Toolkit in test plan 6. According to previous testing plans, there are many artefacts retrieved from the hard drive. This test plan will indicate if IEF can retrieve the same artefacts, more artefacts, or less, and to determine the types of artefacts that Internet Evidence Finder can support.

Requirements

- 1) Internet Evidence finder should be able to recognize the acquired image type .E01 for the hard drive image.
- 2) Hash values should be produced by IEF
- 3) Internet Evidence Finder should be forensically sound and does not modify evidence files upon reading them.
- 4) When the .E01 image is added and processed IEF should be able to analyse the source and find evidence Facebook, Instagram and Twitter artefacts.
- 5) Extraction of the evidence and reporting should be achieved by Internet Evidence Finder.

Description of Methodology

After finishing with examination of RAM in the previous test plan, a new case will be created to examine the suspect's hard drive. Artefacts should be range from different verities such as caches, history, temporary internet files etc.

Expected Results

- 1) Internet Evidence Finder is expected to achieve and extract the evidence posted on Facebook via the three browsers.
- 2) Internet Evidence Finder is expected to achieve and extract the evidence posted on Twitter via the three browsers.
- 3) Internet Evidence Finder is expected to achieve and extract the shared links of Instagram on Facebook and twitter which are accessed via the three browsers.

Test Scenarios - Internet Evidence Finder - hard drive- Facebook & Instagram on Firefox				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
55-2	Facebook	Find posted evidence on suspect's wall	No Evidence Found	Fail
55-3	Facebook	Find Uploaded Picture	Evidence is Found https://www.facebook.com/photo.php?fbid=107389486266838&set=a.106187259720394.1073741827.100009873604315&type=1&theater Source: Files and Folders > Firefox Web History Located at: Table: moz_places(id: 27) Record Number 541	Pass
55-4	Facebook	Find post on friend's wall	No evidence found	Fail
55-5	Facebook	Find Instant messaging with friend	No evidence found	Fail
55-6	Facebook	Find video evidence post	Evidence is Found https://www.facebook.com/100009873604315/videos/vb.100009873604315/107391359599984/?type=2&theater&notif_t=video_processed Source: Files and Folders > Firefox Web History Located at: Table: moz_places(id: 31) Record Number 545	Pass
55-9	Facebook	Find shared Instagram picture evidence	Evidence is Found https://www.facebook.com/photo.php?fbid=107391609599959&set=a.106225223049931.1073741828.100009873604315&type=1&theater Source: File Slack Space > Firefox Session Store Artifacts Located at: Physical Sector 9809869 Record Number 792	Pass
55-10	Instagram	Find Instagram account of suspects logged in via Firefox	Evidence is Found https://instagram.com/accounts/login/ Source: Files and Folders > Firefox Web History Located at: Table: moz_places(id: 34) Record Number 34	Pass
55-11	Instagram	Find viewed Instagram picture via Firefox	Evidence is Found https://instagram.com/p/3xtHtjPIG2/ Source: Files and Folders > Firefox Web History Located at: Table: moz_places(id: 33) Record Number 33	Pass

Test Scenarios - Internet Evidence Finder - hard drive- Facebook & Instagram on Chrome				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
56-2	Facebook	Find posted evidence on suspect's wall	No Evidence found	Fail
56-3	Facebook	Find Uploaded Picture	Evidence is found https://www.facebook.com/photo.php?fbid=107391949599925&set=a.106187259720394.1073741827.100009873604315&type=1&theater	Pass

			Source: Files and Folders > Chrome Current Session Located at: File Offset 117145 Record Number 432	
56-4	Facebook	Find post on friend's wall	No evidence found	Fail
56-5	Facebook	Find Instant messaging with friend	No evidence found	Fail
56-6	Facebook	Find video evidence post	Evidence is found https://www.facebook.com/100009873604315/videos/vb.100009873604315/107392542933199/?type=2&theater&notif_t=video_processed Source: Files and Folders > Chrome Current Session Located at: File Offset 417617 Record Number 436	Pass
56-7	Facebook	Find shared Instagram picture evidence	Evidence is found https://www.facebook.com/photo.php?fbid=106225229716597&set=a.106225223049931.1073741828.100009873604315&type=1&theater Source: Files and Folders > Chrome Current Session Located at: File Offset 495052 Record Number 439	Pass
56-8	Instagram	Find Instagram account of suspects logged in via Chrome	Evidence is Found https://instagram.com/smithvolkov/ Source: Files and Folders > Chrome Web History Located at: Table: urls(id: 35) Record Number 35	Pass
56-9	Instagram	Find viewed Instagram picture via Chrome	Evidence is Found https://instagram.com/p/3xtHtjPIG2/?taken-by=smithvolkov Source: Files and Folders > Chrome Web History Located at: Table: urls(id: 36) Record Number 36	Pass

Test Scenarios - Internet Evidence Finder - hard drive- Facebook & Instagram on IE				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
57-2	Facebook	Find posted evidence on suspect's wall	No evidence found	Fail
57-3	Facebook	Find Uploaded Picture	Evidence is Found Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11407100_107392949599825_1997037522158782039_n[1].jpg Potential Profile ID or Picture ID: 107392949599825 Record Number 19	Pass
57-4	Facebook	Find post on friend's wall	No evidence found	Fail
57-5	Facebook	Find Instant messaging with friend	No evidence found	Fail

57-6	Facebook	Find video evidence post	Evidence is Found https://www.facebook.com/100009873604315/videos/vb.100009873604315/107393532933100/?type=2&theater&notif_t=video_processed Source: Users\admin\AppData\Local\Microsoft\Internet Explorer\Recovery\Last Active Located at: File offset 207031 Record Number 512	Pass
57-7	Facebook	Find shared Instagram picture evidence	No evidence found	Fail
57-8	Instagram	Find Instagram account of suspects logged in via IE	No evidence found	Fail
57-9	Instagram	Find viewed Instagram picture via IE	Evidence is Found https://instagram.com/p/3xtHtjPIG2/ Source: Files and Folders > Internet Explorer 11 Main History - WebCache Located at: File offset 292452 Record Number 212	Pass

Test Scenarios - Internet Evidence Finder - hard drive- Twitter & Instagram on Firefox

Test Number /event #	Social network	Expected result	Source of evidence	Actual result
58-2	Twitter	Find posted evidence on Twitter	No evidence found	Fail
58-3	Twitter	Find uploaded photo in Twitter	Evidence is Found https://twitter.com/smithvolko1/status/610253537465925632/photo/1 Source:Files and Folders > Firefox Web History Located at: Table: moz_places(id: 41) Record Number 381	Pass
58-4	Twitter	Find tweets in friends wall	No evidence found	Fail
58-5	Twitter	Find Direct messaging with friend	No evidence found	Fail
58-7	Twitter	Find shared Instagram picture evidence	No evidence found	Fail
58-9	Instagram	Find viewed picture evidence in Instagram	Evidence is Found https://instagram.com/p/3xtNkYPIHN/ Source: Files and Folders > Firefox Web History Located at:Table:moz_places(id: 45) Record Number 45	Pass
58-10	Twitter	Find suspect's retweets	No evidence found	Fail

Test Scenarios - Internet Evidence Finder - hard drive- Twitter & Instagram on Chrome

Test Number /event #	Social network	Expected result	Source of evidence	Actual result
----------------------	----------------	-----------------	--------------------	---------------

59-2	Twitter	Find posted evidence on Twitter	No evidence found	Fail
59-3	Twitter	Find uploaded photo in Twitter	Evidence is Found https://pbs.twimg.com/media/CHgR34sUsAA-sLd.jpg Source:Files and Folders > Chrome Cache Records Located at: File Offset 3530752 Record Number 46	Pass
59-4	Twitter	Find tweets in friends wall	No evidence found	Fail
59-5	Twitter	Find Direct messaging with friend	No evidence found	Fail
59-6	Twitter	Find shared Instagram picture evidence	No evidence found	Fail
59-8	Instagram	Find viewed picture evidence in Instagram	No evidence found	Fail
59-9	Twitter	Find suspect's retweets	No Evidence Found	Fail

Test Scenarios - Internet Evidence Finder - hard drive- Twitter & Instagram on IE				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
60-2	Twitter	Find posted evidence on Twitter	No evidence found	Fail
60-3	Twitter	Find uploaded photo in Twitter	Evidence is Found https://twitter.com/smithvolko1/status/610256647156412416/photo/1 Source: Files and Folders > Internet Explorer 11 Main History - WebCache Located at: File offset 135799 Record Number 240	Pass
60-4	Twitter	Find tweets in friends wall	No evidence found	Fail
60-5	Twitter	Find Direct messaging with friend	No evidence found	Fail
60-6	Twitter	Find shared Instagram picture evidence	No evidence found	Fail
60-8	Instagram	Find viewed picture evidence in Instagram	Evidence is Found https://instagram.com/p/3xtNkYPIHN/ Source: Files and Folders > Internet Explorer 11 Main History - WebCache Located at: File offset 108504 Record Number 143	Pass
60-9	Twitter	Find suspect's retweets	No Evidence Found	Fail

Appendix 27 – Second Case Scenario: Analysis of RAM Using Internet Evidence Finder (Test Plan 11)

TEST PLAN 11 (Internet Evidence Finder)

Test Number: 011

Examiner: Saud Alshaifi

Test Title: Analysis of RAM acquired from the second case scenario, Suspect (Jason Lopiz), Examination and analysis using Internet Evidence Finder.

Test Date: 22/10/2015

Purpose and Scope

After finishing with examination and analysis of the first case scenario in test plans 9 & 10. This test plan aim to test Internet Evidence Finder for finding evidence from the second case scenario where the online social networks used are LinkedIn, and Bayt. According to the previous test conducted on test plan 3 & test plan 7. Belkasoft Evidence Center has found some evidence activities on both of the OSNSs by analysing RAM, IXTK on the other hand did not find any single evidence from the RAM. The purpose of this test is to indicate the tool's capabilities in terms of finding evidence from Bayt and LinkedIn via examining the suspect's RAM.

Requirements

- 1) The RAM image used for analysis in test plan 3 and test plan 7 should be recognized by Internet Evidence Finder.
- 2) Hashing algorithms need to be performed using IEF in order to confirm that the forensic image processed is an exact copy of the original Image.
- 3) After Verifying the hash value, IEF should maintain the integrity of the evidence.
- 4) Analysis should be conducted successfully.
- 5) IEF should be able to reconstruct the data or activities recovered after analysis, and report the evidence found from the second case scenario source RAM.

Description of Methodology

The methodology used in test plan 3 and test plan 7 is conducted in this test plan, as the same image is analysed but with different tool which is Internet Evidence Finder. After finishing with analysis of the first case scenario Test plan 9&10. The investigator should create a new case in IEF, and add the image source, and do the exact steps performed until the reporting phase.

Expected Results

- 1) It is expected that Internet Evidence Finder will recover the evidence posted or conducted on LinkedIn using the selected browsers.
- 2) It is expected that Internet Evidence Finder will recover the evidence posted or conducted on Bayt using the selected browsers.

Test Scenarios - Internet Evidence Finder – RAM – LinkedIn on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
61-2	LinkedIn	Find posted evidence on suspect's wall	No Evidence Found	Fail
61-3	LinkedIn	Find Uploaded Picture	No Evidence Found	Fail
61-4	LinkedIn	Find posted comment on picture	No Evidence Found	Fail
61-5	LinkedIn	Find picture likes	No Evidence Found	Fail
61-6	LinkedIn	Find sent messages	No Evidence Found	Fail

Test Scenarios - Internet Evidence Finder – RAM – LinkedIn on Chrome				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
62-2	LinkedIn	Find posted evidence on suspect's wall	No Evidence Found	Fail
62-3	LinkedIn	Find Uploaded Picture	Evidence is Found https://image-store.slidesharecdn.com/4db78fe0-b17c-44a5-b164-0d6be97727d5-original.jpeg Located At: Physical Sector 1609020 Record Number 23 & 1067	Pass
62-4	LinkedIn	Find posted comment on picture	No Evidence Found	Fail
62-5	LinkedIn	Find picture likes	No Evidence Found	Fail
62-6	LinkedIn	Find sent messages	No Evidence Found	Fail

Test Scenarios - Internet Evidence Finder – RAM – LinkedIn on IE				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
63-2	LinkedIn	Find posted evidence on suspect's wall	No Evidence Found	Fail
63-3	LinkedIn	Find Uploaded Picture	Evidence is Found https://image-store.slidesharecdn.com/71713020-5a66-4b25-a305-47a7bfc1f2e7-original.jpeg Located At: Physical Sector 2868652 Record Number 70 & 1126	Pass
63-4	LinkedIn	Find posted comment on picture	No Evidence Found	Fail
63-5	LinkedIn	Find picture likes	No Evidence Found	Fail
63-6	LinkedIn	Find sent messages	No Evidence Found	Fail

Test Scenarios - Internet Evidence Finder – RAM – Bayt on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
64-2	Bayt	Find question posted as evidence	No Evidence found	Fail
64-3	Bayt	Find recommendation made	No Evidence found	Fail
64-4	Bayt	Find answer to the question as evidence	No Evidence found	Fail
64-5	Bayt	Find Direct messaging with friend	No Evidence found	Fail

Test Scenarios - Internet Evidence Finder – RAM – Bayt on Chrome				
Test Number /event #	Social network	Expected result	Source of evidence	Actual result
65-2	Bayt	Find question posted as evidence	Evidence is Found http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?feed=top_stories Located At: Physical Sector 56603 Record Number 30	Pass
65-3	Bayt	Find recommendation made	Evidence is Found within Hex http://www.bayt.com/en/mymailbox-j/#inbox/p1/12686714/ Located At: Physical Sector 2091688 Record Number 5	Pass
65-4	Bayt	Find answer to the question as evidence	Evidence is Found http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?feed=top_stories#answer_706618 Located At: Physical Sector 56607 Record Number 19	Pass
65-5	Bayt	Find Direct messaging with friend	Evidence is Found within Hex. http://www.bayt.com/en/mymailbox-j/#inbox/p1/12686739/ Located At: Physical Sector 170738 Record Number 55 & 56 & 62	Pass

Test Scenarios - Internet Evidence Finder – RAM – Bayt on IE				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
66-2	Bayt	Find question posted as evidence	Evidence is Found http://www.bayt.com/en/specialties/q/205292/generate-question-as-evidence-in-bayt-using-ie/?first_p=1&fb_share=0 Located At: Physical Sector 56603 Record Number 8	Pass
66-3	Bayt	Find recommendation made	No Evidence found	Fail
66-4	Bayt	Find answer to the question as evidence	No Evidence found	Fail
66-5	Bayt	Find Direct messaging with friend	No Evidence found	Fail

Appendix 28 – Second Case Scenario: Analysis of Hard Drive Using Internet Evidence Finder (Test Plan 12)

TEST PLAN 12 (Internet Evidence Finder)

Test Number: 012

Examiner: Saud Alshaifi

Test Title: Internet Evidence Finder Test for the Second Case Scenario's HD, Suspect name: Jason Lopiz, OSNSs to be analysed: LinkedIn & Bayt

Test Date: 26/10/2015

Purpose and Scope

Test plan 12 is designed to test the capability of Internet Evidence finder for Finding evidence from LinkedIn and Bayt. In test plan 12 the same image that has been used in test plan 4 and test plan 8 which is called IMAGE_suspect2_harddrive.E01. This image acquired previously and the original evidence is stored in safe place. In test plan 4 the image is examined on Belkasoft Evidence Center, in test plan 8, Internet Examiner Toolkit were used to examine the image, and find evidence or (Controlled data simulated).

Requirements

- 1) Internet Evidence Finder should successfully recognize image type .E01 which is used in test plans (4 & 8)
- 2) The tool should be able to verify hash values
- 3) Internet Evidence Finder must protect the image from any alteration to the data.
- 4) The Image should be processed and ready for analysis, IEF should be able to find Evidence and data and view them for reconstruction
- 5) Internet Evidence Finder should be able to reconstruct the evidence simulated in the second case scenario, where the suspect is Jason Lopiz. IEF should find both LinkedIn and Bayt Activities as Evidence.

Description of Methodology

After finishing analysis of 2nd Case Scenario's RAM in Internet Evidence Finder, and Finishing off with its test plan 11. This test plan is created to examine IEF capabilities of Finding Evidence from LinkedIn and Bayt by examining the suspect's HD. This is very crucial for final findings in order to draw conclusion about the three digital forensic tools and to answer the research questions. This test plan is the last test plan to be conducted, the E01 forensic image will be processed and the investigator will look for artefacts and activities for collection of evidence and reconstruction.

Expected Results

- 1) It is expected that Internet Evidence Finder will recover the evidence posted or conducted on LinkedIn using the selected browsers.
- 2) It is expected that Internet Evidence Finder will recover the evidence posted or conducted on Bayt using the selected browsers.

Test Scenarios - Internet Evidence Finder – hard drive – LinkedIn on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
67-2	LinkedIn	Find posted evidence on suspect's wall	No Evidence found	Fail
67-3	LinkedIn	Find Uploaded Picture	Evidence is Found https://image-store.slidesharecdn.com/5ab72fca-35cb-4b9f-b1c1-0f1b22022243-original.jpeg Firefox Cache Records Record Number 223	Pass
67-4	LinkedIn	Find posted comment on picture	No Evidence found	Fail
67-5	LinkedIn	Find picture likes	No Evidence found	Fail
67-6	LinkedIn	Find sent messages	Evidence is Found From Firefox form History formhistory.sqlite Located At: Table: moz_formhistory(id: 3) Record Number 3	Pass

Test Scenarios - Internet Evidence Finder – hard drive – LinkedIn on Chrome				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
68-2	LinkedIn	Find posted evidence on suspect's wall	No Evidence found	Fail
68-3	LinkedIn	Find Uploaded Picture	Evidence is Found https://image-store.slidesharecdn.com/4db78fe0-b17c-44a5-b164-0d6be97727d5-original.jpeg From Chrome Web History Located At: Table: urls(id: 19) Record Number 19	Pass
68-4	LinkedIn	Find posted comment on picture	No Evidence found	Fail
68-5	LinkedIn	Find picture likes	No Evidence found	Fail
68-6	LinkedIn	Find sent messages	No Evidence found	Fail

Test Scenarios - Internet Evidence Finder – hard drive – LinkedIn on IE				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
69-2	LinkedIn	Find posted evidence on suspect's wall	No Evidence found	Fail
69-3	LinkedIn	Find Uploaded Picture	Evidence is Found https://image-store.slidesharecdn.com/71713020-5a66-4b25-a305-47a7bfc1f2e7-original.jpeg From Browser Activity Located At: File offset 7559888 Record Number 2515 & Found on WebCacheV01.dat Record Number 53	Pass
69-4	LinkedIn	Find posted comment on picture	No Evidence found	Fail
69-5	LinkedIn	Find picture likes	No Evidence found	Fail
69-6	LinkedIn	Find sent messages	No Evidence found	Fail

Test Scenarios - Internet Evidence Finder – hard drive – Bayt on Firefox				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
70-2	Bayt	Find question posted as evidence	Evidence is Found http://www.bayt.com/en/specialties/q/205279/question-as-evidence-in-bayt-using-firefox-test-post-1/?first_p=1&fb_share=0 Firefox Session Store Artefacts Located At: File offset 1635 Record Number 10	Pass
70-3	Bayt	Find recommendation made	No Evidence found	Fail
70-4	Bayt	Find answer to the question as evidence	Evidence is Found http://www.bayt.com/en/specialties/q/205279/question-as-evidence-in-bayt-using-firefox-test-post-1/?feed=top_stories#answer_706602 Firefox Session Store Artefacts Located At: File offset 3695 Record Number 14	Pass
70-5	Bayt	Find Direct messaging with friend	Evidence is Found From Firefox form History formhistory.sqlite Located At: Table: moz_formhistory(id:5) Record Number 5	Pass

Test Scenarios - Internet Evidence Finder – hard drive – Bayt on Chrome				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
71-2	Bayt	Find question posted as evidence	Evidence is Found http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?first_p=1&fb_share=0V User data Located At: File offset 298795 Record Number 2120	Pass
71-3	Bayt	Find recommendation made	Evidence is Found within hex. http://www.bayt.com/en/my-recommendations/ Located At: File offset 793757 Record Number 13	Pass
71-4	Bayt	Find answer to the question as evidence	Evidence is Found http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?feed=top_stories#answer_706618 User data/ Default Located At: File offset 929532 Record Number 2124	Pass
71-5	Bayt	Find Direct messaging with friend	Evidence is found within hex. http://www.bayt.com/en/mymailbox-j/#sent/p1/12686707/ Located At: File offset 1257500 Record#2128 & http://www.bayt.com/en/mymailbox-j/#inbox/p1/12686714/ Located At: File offset 1292049 Record Number 2130	Pass

Test Scenarios - Internet Evidence Finder – hard drive – Bayt on IE				
Test Number /event #	Social network	Expected result	Found Evidence	Actual result
72-2	Bayt	Find question posted as evidence	Evidence is Found http://www.bayt.com/en/specialties/q/205292/generate-question-as-evidence-in-bayt-using-ie/?first_p=1&fb_share=0 from WebCache.dat Located At: Table: Container_21 (EntryId: 19) Record Number 37	Pass
72-3	Bayt	Find recommendation made	No Evidence found	Fail
72-4	Bayt	Find answer to the question as evidence	No Evidence found	Fail
72-5	Bayt	Find Direct messaging with friend	No Evidence found	Fail

Appendix 29 – First Case Scenario: IEF Report for Evidence found on Facebook, Twitter & Instagram from RAM (Findings for Test Plan 9)



Case Info

Date Created: Oct 14, 2015 16:13:58

Case Number: 001

Evidence Number: **test1_Livememory_suspect:** *test1_Livememory_suspect.001 - Entire Disk (1.99 GB);*

pagefile.sys: PhysicalDrive0 - Partition 3 (Microsoft NTFS, 90.33 GB)
DATA [D:\] - test1 Memory acquisition\pagefile.sys;

Examiner: Saud Alshaifi

Notes: First case for Examination of Case Scenario One suspect's RAM & Pagefile

Chrome/360 Safe Browser/Opera Carved Web History

Record	URL	Last Visited Date/Time - (UTC)	Visit Count	Source	Located At	Evidence Number
29	https://instagram.com/p/3xtHtjPIG2/?taken-by=smithvolkov	15/06/2015 01:02:47 PM	1	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 90.33 GB) DATA [D:\] (User Selected) - [ROOT]\test1 Memory acquisition\pagefile.sys	File offset 622044113	pagefile.sys
30	https://instagram.com/smithvolkov/	15/06/2015 01:02:12 PM	2	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 90.33 GB) DATA [D:\] (User Selected) - [ROOT]\test1 Memory acquisition\pagefile.sys	File offset 622044188	pagefile.sys

Facebook Chat

Record	Sender Name	Sender ID	Message ID	Message Sent Date/Time - (UTC)	Message	Receiver ID	Source	Located At
1	Smith Volkov	Smith Volkov	mid.1433995250137:ec479273a86a32d831	15/06/2015 01:06:57 PM	I don't think so, I am still at uni WT building that I showed u before	n/a	pagefile.sys	File offset 264014383
2	Smith Volkov	Smith Volkov	mid.1433995250137:ec479273a86a32d831	15/06/2015 01:06:11 PM	now I am using another browser IE	n/a	pagefile.sys	File offset 264020527
3	Smith Volkov	Smith Volkov	mid.1433995250137:ec479273a86a32d831	15/06/2015 01:07:06 PM	so how was school today good?	n/a	pagefile.sys	File offset 264021295
4	Smith Volkov	Smith Volkov	mid.1433995250137:ec479273a86a32d831	15/06/2015 01:07:46 PM	I know you can do it.. I will teach you this weekend before the test	n/a	pagefile.sys	File offset 264028207
5	Hanan Alsalem	Hanan Alsalem	mid.1433995250137:ec479273a86a32d831	15/06/2015 01:07:52 PM	thank you 3>	n/a	pagefile.sys	File offset 264044197
6	Hanan Alsalem	Hanan Alsalem	mid.1433995250137:ec479273a86a32d831	15/06/2015 01:07:22 PM	yes, have speaking test today it was good\nnext week i have exam if i pass i go to upperintermediate	n/a	pagefile.sys	File offset 280677633
7	Hanan Alsalem	Hanan Alsalem	mid.1433995250137:ec479273a86a32d831	15/06/2015 01:06:23 PM	are you come home early tonight	n/a	pagefile.sys	File offset 298467527
9	n/a	100001368946250	mid.1433995250137:ec479273a86a32d831	15/06/2015 12:49:55 PM	that is so nice, so i be in you thesis haha good luck my cute husband	100009873604315	pagefile.sys	File offset 614132803
10	n/a	100001368946250	mid.1433995250137:ec479273a86a32d831	15/06/2015 12:59:02 PM	what you mean	100009873604315	pagefile.sys	File offset 662758390

Facebook URLs

Record	URL	Date/ Time - (UTC)	Artifact	Potential Activity	Source	Located At
5	https://www.facebook.com/photo.php?fbid=107391609599959&set=a.106225223049931.1073741828.100009873604315&type=1&theater		Browser Activity	Looking at Facebook photo with id: 107391609599959, album id: 106225223049931, and upload profile id: 100009873604315	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 70883
8	https://www.facebook.com/profile.php?id=100009873604315		Browser Activity	Unknown	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 258528
11	https://www.facebook.com/photo.php?fbid=107389486266838&set=a.106187259720394.1073741827.100009873604315&type=1&theater		Browser Activity	Looking at Facebook photo with id: 107389486266838, album id: 106187259720394, and upload profile id: 100009873604315	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 295573
18	https://www.facebook.com/100009873604315/videos/vb.100009873604315/107391359599984/?type=2&theater¬if_t=video_processed		Browser Activity	Unknown	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 452728
22	https://www.facebook.com/hanan.alsalem.58?fref=tl_fr_box&pnref=lhc.friends		Browser Activity	Looking at Facebook profile with profile id: hanan.alsalem.58	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 554940
43	https://www.facebook.com/messages/hanan.alsalem.58WdtR		Browser Activity	Looking at Facebook message with user id: hanan.alsalem.58WdtR	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 1295119
94	https://www.facebook.com/100009873604315/videos/vb.100009873604315/107392542933199/?type=2&theater¬if_t=video_processed	15/06/2015 01:01:10 PM	Chrome/360 Safe Browser/Opera Carved Web History	Unknown	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 90.33 GB) DATA [D:\] (User Selected) - [ROOT]\test1 Memory acquisition\pagefile.sys	File offset 327275040
98	https://www.facebook.com/photo.php?fbid=107391949599925&set=a.106187259720394.1073741827.100009873604315&type=1&theater	15/06/2015 12:56:43 PM	Chrome/360 Safe Browser/Opera Carved Web History	Looking at Facebook photo with id: 107391949599925, album id: 106187259720394, and upload profile id: 100009873604315	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 90.33 GB) DATA [D:\] (User Selected) - [ROOT]\test1 Memory acquisition\pagefile.sys	File offset 327275474
108	https://www.facebook.com/photo.php?fbid=106225229716597&set=a.106225223049931.1073741828.100009873604315&type=1&theater	15/06/2015 01:01:29 PM	Chrome/360 Safe Browser/Opera Carved Web History	Looking at Facebook photo with id: 106225229716597, album id: 106225223049931, and upload profile id: 100009873604315	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 90.33 GB) DATA [D:\] (User Selected) - [ROOT]\test1 Memory acquisition\pagefile.sys	File offset 621721119

Firefox FormHistory

Record	Field Name	Value	First Used Date/Time - (UTC)	Source	Located At	Evidence Number
1	Email	smithvolkov@hotmail.com	15/06/2015 12:39:33 AM	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 90.33 GB) DATA [D:\] (User Selected) - [ROOT]\test1 Memory acquisition\pagefile.sys	File offset 634707904	pagefile.sys

Firefox SessionStore Artifacts

Record	Title	URL	Source	Located At	Evidence Number
2	smithvolkov on Twitter: \"http://t.co/gXjQoLdhWq\"	https://twitter.com/smithvolko1/status/610253537465925632/photo/1	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 64538	test1_Livememory_suspect
7	Instagram photo by Smith Volkov "Invalid date at Invalid date"	https://instagram.com/p/3xtNkYPIHN/	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 774438	test1_Livememory_suspect
10	Instagram	https://instagram.com/smithvolkov/	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 1952081	test1_Livememory_suspect
11	Instagram	https://instagram.com/p/3xtHtjPIG2/?taken-by=smithvolkov	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 1952082	test1_Livememory_suspect

Identifiers

Record	Identifier	Column Name	Artifact	Artifact ID	Source	Located At	Evidence Number
6	Smith Volkov	Sender ID	Facebook Chat	1	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 90.33 GB) DATA [D:\] (User Selected) - [ROOT]\test1 Memory acquisition\pagefile.sys	File offset 264014383	pagefile.sys
7	Hanan Alsalem	Sender ID	Facebook Chat	5	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 90.33 GB) DATA [D:\] (User Selected) - [ROOT]\test1 Memory acquisition\pagefile.sys	File offset 264044197	pagefile.sys

Internet Explorer 10-11 Daily/Weekly History

Record	User	URL	Last Visited Date/Time	Access Count	Source	Located At	Evidence Number
9	admin	https://instagram.com/p/3xtHtjPIG2/	2015-06-15 13:09:25	1	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 764828	test1_Livememory_suspect

Social Media URLs

Record	Site Name	URL	Artifact	Located At	Artifact ID	Source	Evidence Number
4	Twitter	https://twitter.com/smithvolko1/status/610253303985745920	Browser Activity	Physical Sector 10205	36	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	test1_Livememory_suspect
47	Twitter	https://twitter.com/smithvolko1/status/610257403028738050/photo/1	Browser Activity	Physical Sector 474847	378	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	test1_Livememory_suspect
167	Twitter	https://twitter.com/smithvolko1/status/610256647156412416/photo/1	Internet Explorer 10-11 Daily/Weekly History	Physical Sector 1926361	43	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	test1_Livememory_suspect
255	Twitter	https://twitter.com/smithvolko1/status/610254995993178112	Browser Activity	Physical Sector 3065945	1677	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	test1_Livememory_suspect
258	Twitter	https://twitter.com/smithvolko1/status/610256537047576576	Browser Activity	Physical Sector 3065947	1680	test1_Livememory_suspect.001 - Entire Disk (1.99 GB) (Sector Level)	test1_Livememory_suspect

Appendix 30 – First Case Scenario: IEF Report for Evidence found on Facebook, Twitter & Instagram from HD (Findings for Test Plan 10)



Case Info

Date Created: Oct 19, 2015 18:21:43

Case Number: 002

Evidence Number: **IMAGE-suspect1-harddrive:** *IMAGE-suspect1-harddrive.E01 - Partition 1 (Microsoft NTFS, 100 MB) System Reserved, IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB), IMAGE-suspect1-harddrive.E01 - Unpartitioned Space;*

Examiner: Saud Alshaifi


Notes: Second case for Examination of Case Scenario One suspect's Hard Drive

Facebook URLs

Record	URL	Date/ Time - (UTC)	Potential Activity	Artifact	Located At	Source
432	https://www.facebook.com/photo.php?fbid=107391949599925&set=a.106187259720394.1073741827.100009873604315&type=1&theater		Looking at Facebook photo with id: 107391949599925, album id: 106187259720394, and upload profile id: 100009873604315	Chrome Current Session	File Offset 117145	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Current Session
436	https://www.facebook.com/100009873604315/videos/vb.100009873604315/107392542933199/?type=2&theater¬if_t=video_processed		Unknown	Chrome Current Session	File Offset 417617	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Current Session
439	https://www.facebook.com/photo.php?fbid=106225229716597&set=a.106225223049931.1073741828.100009873604315&type=1&theater		Looking at Facebook photo with id: 106225229716597, album id: 106225223049931, and upload profile id: 100009873604315	Chrome Current Session	File Offset 495052	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Current Session
512	https://www.facebook.com/100009873604315/videos/vb.100009873604315/107393532933100/?type=2&theater¬if_t=video_processed		Unknown	Browser Activity	File offset 207031	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Microsoft\Internet Explorer\Recovery\Last Active\{8871C2AB-12FD-11E5-B649-001B2498D131}.dat
541	https://www.facebook.com/photo.php?fbid=107389486266838&set=a.106187259720394.1073741827.100009873604315&type=1&theater	15/06/2015 12:45:15 PM	Looking at Facebook photo with id: 107389486266838, album id: 106187259720394, and upload profile id: 100009873604315	Firefox Web History	Table: moz_places(id: 27)	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\8ez4wa3i.default\places.sqlite
545	https://www.facebook.com/100009873604315/videos/vb.100009873604315/	15/06/2015 12:51:00 PM	Unknown	Firefox Web History	Table: moz_places(id: 31)	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All

	107391359599984/?type=2&theater¬if_t=video_processed					Files and Folders) - [ROOT]\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\8ez4wa3i.default\places.sqlite
792	https://www.facebook.com/photo.php?fbid=107391609599959&set=a.106225223049931.1073741828.100009873604315&type=1&theater		Looking at Facebook photo with id: 107391609599959, album id: 106225223049931, and upload profile id: 100009873604315	Firefox SessionStore Artifacts	Physical Sector 9809869	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (File Slack Space) - [ROOT]\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\8ez4wa3i.default\cache2\entries\41ED021D6E2AAE63301D86B38A760EE11FF60A95

Facebook Pictures

Record	Potential Profile ID or Picture ID	Image	Date/Time - (UTC)	Size (Bytes)	MD5 Hash	SHA1 Hash	Source
19	107392949599825		15/06/2015 01:03:40 PM	14808	65883aa22e1d89b17c7a326426e278d	dbd3e78b3e81701ec74a32b15f9a0d3325b918eb	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\56GGEP5W\11407100_107392949599825_1997037522158782039_n[1].jpg

Social Media URLs


Record	Site Name	URL	Date/Time - (UTC)	Artifact	Located At	Artifact ID	Source
381	Twitter	https://twitter.com/smithvolko1/status/610253537465925632/photo/1	15/06/2015 01:12:47 PM	Firefox Web History	Table: moz_places(id: 41)	41	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\8ez4wa3i.default\places.sqlite

240	Twitter	https://twitter.com/smithvolko1/status/610256647156412416/photo/1	2015-06-15 13:24:45 (local time)	Internet Explorer 10-11Daily/Weekly History	File offset 135799	19	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Microsoft\Windows\WebCache\V01.log
-----	---------	-------------------------------------------------------------------	----------------------------------	---------------------------------------------	--------------------	----	----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Firefox Web History

Record	URL	Last Visited Date/Time (UTC)	Title	Source	Located At	Evidence Number
33	https://instagram.com/p/3xtHtjPIG2/	15/06/2015 12:53:20 PM	Smith Volkov on Instagram: "this is instagram shared in facebook"	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\8ez4wa3i.default\places.sqlite	Table: moz_places(id: 33)	IMAGE-suspect1-harddrive
34	https://instagram.com/accounts/login/	15/06/2015 12:53:39 PM	Smith Volkov on Instagram: "this is instagram shared in facebook"	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\8ez4wa3i.default\places.sqlite	Table: moz_places(id: 34)	IMAGE-suspect1-harddrive
45	https://instagram.com/p/3xtNkYPIHN/	15/06/2015 01:15:30 PM	Instagram photo by Smith Volkov • Invalid date at Invalid date	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\8ez4wa3i.default\places.sqlite	Table: moz_places(id: 45)	IMAGE-suspect1-harddrive

Chrome Cache Records

Record	URL	Last Visited Date/Time - (UTC)	Content Size	Image	Source	Located At
46	https://pbs.twimg.com/media/CHgR34sUsAA-sLd.jpg	15/06/2015 01:18:46 PM	15133		Browser: Chrome website: Twitter Picture Evidence	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3
						File Offset 3530752

Chrome Web History

Record	URL	Last Visited Date/Time - (UTC)	Source	Located At	Evidence Number
35	https://instagram.com/smithvolkov/	15/06/2015 01:02:12 PM	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default\History	Table: urls(id:35)	IMAGE-suspect1-harddrive
36	https://instagram.com/p/3xtHtjPIG2/?taken-by=smithvolkov	15/06/2015 01:02:47 PM	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default\History	Table: urls(id:36)	IMAGE-suspect1-harddrive

Internet Explorer 10-11 Main History

Record	User	URL	Last Visited Date/Time	Access Count	Source	Located At	Evidence Number
143	admin	https://instagram.com/p/3xtNkYPIHN/	15/06/2015 01:29:44 PM	1	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Microsoft\Windows\WebCache\V01.log	File offset 108504	IMAGE-suspect1-harddrive
212	admin	https://instagram.com/p/3xtHtjPIG2/	15/06/2015 01:09:25 PM	1	IMAGE-suspect1-harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Microsoft\Windows\WebCache\V0100010.log	File offset 292452	IMAGE-suspect1-harddrive

**Appendix 31 – Second Case Scenario: IEF Report for Evidence found on
LinkedIn and Bayt from RAM (Findings for Test Plan 11)**



Case Info

Date Created: Oct 26, 2015 16:13:58

Case Number: 003

Evidence Number: **test2_Livememory_suspect2:** *test2_Livememory_suspect2.001*
- Entire Disk (1.99 GB); **pagefile.sys:** *PhysicalDrive0 -*
Partition 3 (Microsoft NTFS, 90.33 GB) DATA [D:] -
test2 Memory Acquisition\pagefile.sys

Examiner: Saud Alshaifi

Notes: Third case created for Examining RAM and the swap file for
Case Scenario 2 Suspect Jason Lopiz

Browser Activity

Record	URL	Source	Located At	Evidence Number
19	http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?feed=top_stories#answer_706618	test2_Livememory_suspect2.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 56607	test2_Livememory_suspect2
30	http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?feed=top_stories	test2_Livememory_suspect2.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 56603	test2_Livememory_suspect2
55	http://www.bayt.com/en/mymailbox-j/	test2_Livememory_suspect2.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 170738	test2_Livememory_suspect2
56	http://www.bayt.com/en/mymailbox-j/#inbox/p1/12686739/	test2_Livememory_suspect2.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 170738	test2_Livememory_suspect2
62	http://www.bayt.com/en/mymailbox-j/#[mailboxKeyword] #0	test2_Livememory_suspect2.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 170741	test2_Livememory_suspect2

Chrome/360 Safe Browser Carved Session/Tabs

Record	URL	Title	Source	Located At	Evidence Number
5	http://www.bayt.com/en/mymailbox-j/#inbox/p1/12686714/	My Mailbox Bayt.com	test2_Livememory_suspect2.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 2091688	test2_Livememory_suspect2

Chrome/360 Safe Browser/Opera Carved Web History

Record	URL	Visit Count	Evidence Number	Title	Source	Located At
23	https://image-store.slidesharecdn.com/4db78fe0-b17c-44a5-b164-0d6be97727d5-original.jpeg	2	test2_Livememory_suspect2	4db78fe0-b17c-44a5-b164-0d6be97727d5-original.jpeg (375x225)	test2_Livememory_suspect2.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 1609020



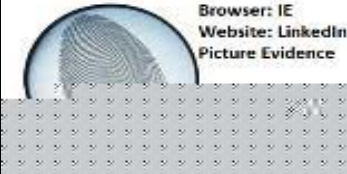
IE InPrivate/Recovery URLs

Record	URL	Source	Located At	Evidence Number
70	https://image-store.slidesharecdn.com/71713020-5a66-4b25-a305-47a7bfc1f2e7-original.jpeg	test2_Livememory_suspect2.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 2868652	test2_Livememory_suspect2

Internet Explorer 10-11 Daily/Weekly History

Record	User	URL	Last Visited Date/Time	Access Count	Located At	Source	Evidence Number
8	admin	http://www.bayt.com/en/specialties/q/205292/generate-question-as-evidence-in-bayt-using-ie/?first_p=1&fb_share=0	2015-06-23 20:50:41	2	Physical Sector 282554	test2_Livememory_suspect2.001 - Entire Disk (1.99 GB) (Sector Level)	test2_Livememory_suspect2

Pictures

Record	Image	Size (Bytes)	MD5 Hash	SHA1 Hash	Source	Located At
913		113423	9649ee522f27a9df9b9f0fb2719613c3	84ff62fa5ed500e2a88eaa8b4eab88043d05cb37	test2_Livememory_suspect2.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 1178873
1067		28635	f77f0d1e5656808488a4a8f2e4234eb2	660e796511606ee7c5496f8661209e4e52f169cc	test2_Livememory_suspect2.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 1550817
1126		352883	9f11e499e59c6c68c50a8e3438317a69	5b578d83bedeff37e1fb6f347a708c0ff5685c82	test2_Livememory_suspect2.001 - Entire Disk (1.99 GB) (Sector Level)	Physical Sector 1652097

**Appendix 32 – Second Case Scenario: IEF Report for Evidence found on
LinkedIn and Bayt from HD (Findings for Test Plan 12)**



Case Info

Date Created: Oct 29, 2015 16:13:58

Case Number: 004

Evidence Number: **IMAGE_suspect2_harddrive:** *IMAGE_suspect2_harddrive.E01 - Partition 1 (Microsoft NTFS, 100 MB) System Reserved, IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB), IMAGE_suspect2_harddrive.E01 - Unpartitioned Space;*


Examiner: Saud Alshaifi

Notes: Fourth case created for examining the hard drive for Case Scenario 2 Suspect Jason Lopiz

Browser Activity

Record	URL	Source	Located At	Evidence Number
2120	http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?first_p=1&fb_share=0V	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Last Session	File offset 298795	IMAGE_suspect2_harddrive
2124	http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?feed=top_stories#answer_706618	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Last Session	File offset 929532	IMAGE_suspect2_harddrive
2128	http://www.bayt.com/en/mymailbox-j/#sent/p1/12686707/	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Last Session	File offset 1257500	IMAGE_suspect2_harddrive
2130	http://www.bayt.com/en/mymailbox-j/#inbox/p1/12686714/	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Last Session	File offset 1292049	IMAGE_suspect2_harddrive
2515	https://image-store.slidesharecdn.com/71713020-5a66-4b25-a305-47a7bfc1f2e7-original.jpeg	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (Unallocated Clusters)	Physical Sector 7559888	IMAGE_suspect2_harddrive

Chrome Cache Records

Record	URL	Content Size	Source	Image	Evidence Number
200	http://img.b8cdn.com/images/uploads/user_photos/20/29424820_20150623073738.jpgg	24328	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Cache\f_000084	 A magnifying glass focusing on a fingerprint-like texture, with the text 'profile picture Bayt.com' overlaid.	IMAGE_suspect2_harddrive

Chrome Last Session



Record	URL	Title	Source	Located At	Evidence Number
13	http://www.bayt.com/en/my-recommendations/	My Recommendation - Bayt.com	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Last Session	File Offset 793757	IMAGE_suspect2_harddrive

Chrome Web History

Record	URL	Last Visited Date/Time (UTC)	Located At	Source	Title	Visit Count	Evidence Number
19	https://image-store.slidesharecdn.com/4db78fe0-b17c-44a5-b164-0d6be97727d5-	23/06/2015 03:09:56 PM	Table: urls(id: 19)	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData	4db78fe0-b17c-44a5-b164-0d6be97727d5-	2	IMAGE_suspect2_harddrive

	0d6be97727d5-original.jpeg			\Local\Google\Chrome\User Data\Default\History	original.jpeg (375x225)		
--	----------------------------	--	--	------------------------------------------------	-------------------------	--	--

Firefox Cache Records

Record	URL	Date/Time - (UTC)	MIME Type	Content Size (Bytes)	Image	Source	Evidence Number
223	https://image-store.slidesharecdn.com/5ab72fca-35cb-4b9f-b1c1-0f1b22022243-original.jpeg	23/06/2015 07:59:14 PM	image/jpeg	14698		IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\zjhbp3me.default\cache2\entries\2886F17FE270506CE798200878EBE450 DA40188C	IMAGE_suspect2_harddrive
654	https://media.licdn.com/mpr/mpr/shrink_100_100/AAEAQAIAAAAAAALsAAAAJGU0NjI4ZDRlTI1NZA tNGM0OS05NjY0LTZmOThhMWE3NDIkYg.jpg	23/06/2015 07:55:46PM	image/jpeg	3217		IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\zjhbp3me.default\cache2\entries\76DE241A22D11E65B08058BCCD40BA C50606FFB2	IMAGE_suspect2_harddrive

Firefox FormHistory

Record	Field Name	Value	Date Used Date/Time - (UTC)	ID	Source	Located At	Evidence Number
3	subject	Generate message to friend evidence in LinkedIn using Firefox test post 3	23/06/2015 07:57:10 PM	3	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\zjhbp3me.default\formhistory.sqlite	Table: moz_formhistory(id: 3)	IMAGE_suspect2_harddrive
5	subject	Generate message to friend evidence in Bayt using Firefox test post 4	23/06/2015 08:30:10 PM	5	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\zjhbp3me.default\formhistory.sqlite	Table: moz_formhistory(id:5)	IMAGE_suspect2_harddrive

Firefox SessionStore Artifacts

Record	Title	URL	Located At	Source	Evidence Number
10	Question as evidence in Bayt using Firefox test post 1? - Bayt.com Specialties	http://www.bayt.com/en/specialties/q/205279/question-as-evidence-in-bayt-using-firefox-test-post-1/?first_p=1&fb_share=0	File offset 1635	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\zjhbp3me.default\sessionstore-backups\previous.js	IMAGE_suspect2_harddrive
14	Question as evidence in Bayt using Firefox test post 1? - Bayt.com Specialties	http://www.bayt.com/en/specialties/q/205279/question-as-evidence-in-bayt-using-firefox-test-post-1/?feed=top_stories#answer_706602	File offset 3695	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\zjhbp3me.default\sessionstore-backups\previous.js	IMAGE_suspect2_harddrive
28	Specialties Ask Question - Bayt.com Specialties	http://www.bayt.com/en/specialties/ask-question/	Physical Sector 9113074	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (File Slack Space) - [ROOT]\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\zjhbp3me.default\cache2\entries\16AB6C12E842EDD52CA8B4A5AE6B0E DE567E81E6	IMAGE_suspect2_harddrive

Identifiers

Record	Identifier	Column Name	Artifact	Artifact ID	Source	Located At	Evidence Number
17	jasonlopiz@hotmail.com	Username	Chrome Logins	1	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Google\Chrome\User Data\Default>Login Data	Table: logins(row id: 1)	IMAGE_suspect2_harddrive

Internet Explorer 10-11 Daily/Weekly History

Record	User	URL	Last Visited Date/Time	Access Count	Located At	Source	Evidence Number
37	admin	http://www.bayt.com/en/specialties/q/205292/generate-question-as-evidence-in-bayt-using-ie/?first_p=1&fb_share=0	2015-06-23 20:50:41	2	Table: Container_21 (EntryId: 19)	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	IMAGE_suspect2_harddrive
53	admin	https://image-store.slidesharecdn.com/71713020-5a66-4b25-a305-47a7bfc1f2e7-original.jpeg	2015-06-23 20:16:53	3	Table: Container_21 (EntryId: 9)	IMAGE_suspect2_harddrive.E01 - Partition 2 (Microsoft NTFS, 148.95 GB) (All Files and Folders) - [ROOT]\Users\admin\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	IMAGE_suspect2_harddrive

Appendix 33 – Second Case Scenario: IEF Screenshots of Evidence Findings on suspect's RAM (Bayt)

Browser Activity:

★	#	URL
★	19	http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?feed=top_stories#answer_706618
★	30	http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?feed=top_stories
★	55	http://www.bayt.com/en/mymailbox-j/
★	56	http://www.bayt.com/en/mymailbox-j/#inbox/p1/12686739/
★	62	http://www.bayt.com/en/mymailbox-j/#[mailboxKeyword] #0

Internet Explorer History:

★	#	User	URL	Last Visited Da
★	8	admin	http://www.bayt.com/en/specialties/q/205292/generate-question-as-evidence-in-bayt-using-ie/?first_p=1&fb_share=0	2015-06-23 20:

Direct Message sent using Chrome:

```

2D 00 2D 00 2D 00 0A 00 0A 00 47 00 65 00 6E 00 65 00 72 00
61 00 74 00 65 00 20 00 6D 00 65 00 73 00 73 00 61 00 67 00
65 00 20 00 74 00 6F 00 20 00 66 00 72 00 69 00 65 00 6E 00
64 00 20 00 65 00 76 00 69 00 64 00 65 00 6E 00 63 00 65 00
20 00 69 00 6E 00 20 00 42 00 61 00 79 00 74 00 20 00 75 00
73 00 69 00 6E 00 67 00 20 00 43 00 68 00 72 00 6F 00 6D 00
65 00 20 00 74 00 65 00 73 00 74 00 20 00 70 00 6F 00 73 00
74 00 20 00 34 00 00 00 72 00 00 00 68 00 74 00 74 00 70 00

```

```

-.-.-.-.-G.e.n.e.r.
a.t.e..m.e.s.s.a.g.
e..t.o..f.r.i.e.n.
d..e.v.i.d.e.n.c.e.
.i.n..B.a.y.t..u.
s.i.n.g..C.h.r.o.m.
e..t.e.s.t..p.o.s.
t..4...h.t.t.p.

```

Recommendation made using Chrome Recovered

★	#	User	URL	Last Visited Da
★	5		http://www.bayt.com/en/mymailbox-j/#inbox/p1/12686714/	

Details	Hex	Text
1070945400	72 00 6F 00 74 00 65 00 3A 00 0A 00 2D 00 2D 00 2D 00 2D 00	r.o.t.e.i.....
1070945420	2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00D.e.
1070945440	2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 0A 00 0A 00 44 00 65 00D.e.
1070945460	61 00 72 00 20 00 53 00 61 00 75 00 64 00 2C 00 59 00 6F 00	a.r..S.a.u.d..Y.o.
1070945480	75 00 20 00 68 00 61 00 76 00 65 00 20 00 72 00 65 00 63 00	u..h.a.v.e..r.e.c.
1070945500	65 00 69 00 76 00 65 00 64 00 20 00 61 00 20 00 72 00 65 00	e.i.v.e.d..a..r.e.
1070945520	63 00 6F 00 6D 00 6D 00 65 00 6E 00 64 00 61 00 74 00 69 00	c.o.m.m.e.n.d.a.t.i.
1070945540	6F 00 6E 00 20 00 66 00 72 00 6F 00 6D 00 20 00 4A 00 61 00	o.n..f.r.o.m..J.a.
1070945560	73 00 6F 00 6E 00 20 00 6C 00 6F 00 70 00 69 00 7A 00 20 00	s.o.n..l.o.p.i.z..
1070945580	70 00 65 00 6F 00 70 00 6C 00 65 00 2E 00 62 00 61 00 79 00	p.e.o.p.l.e..b.a.y.
1070945600	74 00 2E 00 63 00 6F 00 6D 00 2E 00 20 00 54 00 68 00 69 00	t...c.o.m...T.h.i.
1070945620	73 00 20 00 72 00 65 00 63 00 6F 00 6D 00 6D 00 65 00 6E 00	s...r.e.c.o.m.m.e.n.
1070945640	64 00 61 00 74 00 69 00 6F 00 6E 00 20 00 69 00 73 00 20 00	d.a.t.i.o.n..i.s..
1070945660	6E 00 6F 00 77 00 20 00 64 00 69 00 73 00 70 00 6C 00 61 00	n.o.w..d.i.s.p.l.a.
1070945680	79 00 65 00 64 00 20 00 6F 00 6E 00 20 00 79 00 6F 00 75 00	y.e.d..o.n..y.o.u.
1070945700	72 00 20 00 43 00 56 00 2E 00 4A 00 61 00 73 00 6F 00 6E 00	r..C.V..J.a.s.o.n.
1070945720	20 00 6C 00 6F 00 70 00 69 00 7A 00 27 00 73 00 20 00 72 00	..l.o.p.i.z..s..r.
1070945740	65 00 63 00 6F 00 6D 00 6D 00 65 00 6E 00 64 00 61 00 74 00	e.c.o.m.m.e.n.d.a.t.
1070945760	69 00 6F 00 6E 00 3A 00 47 00 65 00 6E 00 65 00 72 00 61 00	i.o.n...G.e.n.e.r.a.
1070945780	74 00 65 00 20 00 72 00 65 00 63 00 6F 00 6D 00 6D 00 65 00	t.e..r.e.c.o.m.m.e.
1070945800	6E 00 64 00 61 00 74 00 69 00 6F 00 6E 00 20 00 65 00 76 00	n.d.a.t.i.o.n..e.v.
1070945820	69 00 64 00 65 00 6E 00 63 00 65 00 20 00 69 00 6E 00 20 00	i.d.e.n.c.e..i.n..
1070945840	42 00 61 00 79 00 74 00 20 00 75 00 73 00 69 00 6E 00 67 00	B.a.y.t..u.s.i.n.g.
1070945860	20 00 43 00 68 00 72 00 6F 00 6D 00 65 00 20 00 74 00 65 00	..C.h.r.o.m.e..t.e.
1070945880	73 00 74 00 20 00 70 00 6F 00 73 00 74 00 20 00 32 00 72 00	s.t..p.o.s.t..2.r.

Appendix 34 – Second Case Scenario: IEF Screenshots of Evidence Findings on suspect's HD (LinkedIn and Bayt)



Browser Activity:



★	#	URL
★	2.	http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?first_p=1&fb_share=0V
★	2.	http://www.bayt.com/en/specialties/q/205284/generate-question-as-evidence-in-bayt-using-chrome-test-post-1/?feed=top_stories#answer_706618
★	2.	http://www.bayt.com/en/mymailbox-j/#sent/p1/12686707/
★	2.	http://www.bayt.com/en/mymailbox-j/#inbox/p1/12686714/
★	2.	https://image-store.slidesharecdn.com/71713020-5a66-4b25-a305-47a7bfc1f2e7-original.jpeg

Chrome Web History:

★	#	URL	Located At
★	19	https://image-store.slidesharecdn.com/4db78fe0-b17c-44a5-b164-0d6be97727d5-original.jpeg	Table: urls(d: 19)

Chrome Cache Records:

Go To #:  Default Encoding Search: 

	#	URL	File Type	Content Size	Source
	200	http://img.b8cdn.com/images/uploads/user_photos/20/29424820_20150623073738.jpg	jpeg	24328	IMAGE_su...

Firefox Cache Records:

★	#	URL	MIME Type
★	2.	https://image-store.slidesharecdn.com/5ab72fca-35cb-4b9f-b1c1-0f1b22022243-original.jpeg	image/jpeg
★	6.	https://media.licdn.com/mpr/mpr/shrink_100_100/AEEAAQAAAAAALsAAAAJGU0NjI4ZDRlT1NzAtNGM0OS05NjY0LTZmOThhMWE3NDkYg.jpg	image/jpeg

Firefox Form History:

★	#	Field Name	Value	Times Used	ID
★	3	subject	Generate message to friend evidence in LinkedIn using Firefox test post ...	1	3
★	5	subject	Generate message to friend evidence in Bayt using Firefox test post 4	1	5

Firefox Session Store Artefacts:

★	#	Title	URL
★	10	Question as evidence in Bayt using Firefox test post 1? ...	http://www.bayt.com/en/specialties/q/205279/question-as-evidence-in-bayt-using-firefox-test-1?
★	14	Question as evidence in Bayt using Firefox test post 1? ...	http://www.bayt.com/en/specialties/q/205279/question-as-evidence-in-bayt-using-firefox-test-1?
★	28	Specialties Ask Question - Bayt.com Specialties	http://www.bayt.com/en/specialties/ask-question/

Internet Explorer History:

★	#	User	URL	Access Count
★	37	admin	http://www.bayt.com/en/specialties/q/205292/generate-question-as-evidence-in-bayt-using-ie/?first_p=1&fb_shar...	2
★	53	admin	https://image-store.slidesharecdn.com/71713020-5a66-4b25-a305-47a7bfc1f2e7-original.jpeg	3

Chrome Last Session:

Default Encoding ▾ Search:

★	#	URL	Last Visited Date/Ti...	Title
★	12	http://people.bayt.com/saud-alshaifi/#submit-alert-message		Saud Alshaifi - Public ...
★	13	http://www.bayt.com/en/my-recommendations/		My Recommendations ...

Recovered Bayt Message to a friend using Chrome:

00 20 00 32 00 33 00 2D 00 30 00 36 00 2D 00 32 00 30 00 31 00 35 00 20 00	2 3 0 6 2 0 1 5
30 00 38 00 3A 00 34 00 33 00 2C 00 20 00 53 00 61 00 75 00 64 00 20 00 41	0 8 4 3 S a u d A
00 6C 00 73 00 68 00 61 00 69 00 66 00 69 00 20 00 77 00 72 00 6F 00 74 00	l s h a i f i w r o t
65 00 3A 00 0A 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D	e t t t t t t t t t t t
00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 2D 00 0A 00 0A 00	t t t t t t t t t t t t
47 00 65 00 6E 00 65 00 72 00 61 00 74 00 65 00 20 00 6D 00 65 00 73 00 73	G e n e r a t e m e s s
00 61 00 67 00 65 00 20 00 74 00 6F 00 20 00 66 00 72 00 69 00 65 00 6E 00	a g e t o f r i e n d
64 00 20 00 65 00 76 00 69 00 64 00 65 00 6E 00 63 00 65 00 20 00 69 00 6E	d e v i d e n c e i n
00 20 00 42 00 61 00 79 00 74 00 20 00 75 00 73 00 69 00 6E 00 67 00 20 00	B a y t u s i n g
43 00 68 00 72 00 6F 00 6D 00 65 00 20 00 74 00 65 00 73 00 74 00 20 00 70	C h r o m e t e s t p
00 6F 00 73 00 74 00 20 00 34 00 00 00 1E 00 00 00 65 00 6D 00 61 00 69 00	o s t 4 e m a i
6C 00 73 00 43 00 68 00 65 00 63 00 6B 00 4C 00 69 00 73 00 74 00 00 00 10	l s C h e c k L i s t
00 00 00 63 00 68 00 65 00 63 00 6B 00 62 00 6F 00 78 00 02 00 00 00 31 00	c h e c k b o x 1
00 00 06 00 00 00 6F 00 66 00 66 00 00 00 1E 00 00 00 65 00 6D 00 61 00 69	o f f e m a i
00 6C 00 73 00 43 00 68 00 65 00 63 00 6B 00 4C 00 69 00 73 00 74 00 00 00	l s C h e c k L i s t

Recommendation made using Chrome Recovered from HD:

★ 13 http://www.bayt.com/en/my-recommendations/ My Recommendations -Not Found

Go To Page: Showing results 1 - 2 of 2

Details	Hex	Text
0621252	65 00 78 00 74 00 02 00 00 00 31 00 00 00 22 00 00 00	e . x . t 1 . . . " . . .
0621270	73 00 61 00 6C 00 65 00 73 00 20 00 74 00 65 00 61 00	s . a . l . e . s . . t . e . a .
0621288	6D 00 20 00 6D 00 65 00 6D 00 62 00 65 00 72 00 00 00	m . m . e . m . b . e . r . . .
0621306	1A 00 00 00 72 00 65 00 6C 00 61 00 74 00 69 00 6F 00 r . e . l . a . t . i . o .
0621324	6E 00 5F 00 72 00 65 00 63 00 5F 00 00 00 14 00 00 00	n _ r . e . c . _
0621342	73 00 65 00 6C 00 65 00 63 00 74 00 2D 00 6F 00 6E 00	s . e . l . e . c . t . - . . . o . n .
0621360	65 00 02 00 00 00 32 00 00 00 00 00 00 00 02 00 00 00	e 2
0621378	30 00 00 00 28 00 00 00 72 00 65 00 63 00 6F 00 6D 00	0 . . (. . . r . e . c . o . m .
0621396	6D 00 65 00 6E 00 64 00 61 00 74 00 69 00 6F 00 6E 00	m . e . n . d . a . t . i . o . n .
0621414	5F 00 74 00 65 00 78 00 74 00 5F 00 10 00 00 00 74 00	_ . t . e . x . t . _ t .
0621432	65 00 78 00 74 00 61 00 72 00 65 00 61 00 02 00 00 00	e . x . t . a . r . e . a
0621450	31 00 00 00 82 00 00 00 47 00 65 00 6E 00 65 00 72 00	1 G . e . n . e . r .
0621468	61 00 74 00 65 00 20 00 72 00 65 00 63 00 6F 00 6D 00	a . t . e . _ . r . e . c . o . m .
0621486	6D 00 65 00 6E 00 64 00 61 00 74 00 69 00 6F 00 6E 00	m . e . n . d . a . t . i . o . n .
0621504	20 00 65 00 76 00 69 00 64 00 65 00 6E 00 63 00 65 00	. . e . v . i . d . e . n . c . e .
0621522	20 00 69 00 6E 00 20 00 42 00 61 00 79 00 74 00 20 00	. . i . n . _ . B . a . y . t . .
0621540	75 00 73 00 69 00 6E 00 67 00 20 00 43 00 68 00 72 00	u . s . i . n . g . _ . C . h . r .

Appendix 35 –SQL Statements Used to Search For Evidence in Internet Examiner Toolkit

1. Facebook Artefacts :

```
SELECT * FROM Records WHERE HideRecord = 0 AND ((OptionalFilterKeywords LIKE '%Social Networking%' AND OptionalFilterKeywords LIKE '%Facebook%') OR (ArtifactCategory = 'Social Networking' AND ArtifactBrand = 'Facebook')) ORDER BY ActivityTimeLocal ASC
```

2. Facebook Chat messages:

```
SELECT * FROM Records WHERE HideRecord = 0 AND ((OptionalFilterKeywords LIKE '%Social Networking%' AND OptionalFilterKeywords LIKE '%Facebook%' AND OptionalFilterKeywords LIKE '%Chat Message%') OR (ArtifactCategory = 'Social Networking' AND ArtifactBrand = 'Facebook' AND ArtifactType = 'Chat Message')) ORDER BY ActivityTimeLocal ASC
```

3. Facebook Email Messages:

```
SELECT * FROM Records WHERE HideRecord = 0 AND ((OptionalFilterKeywords LIKE '%Social Networking%' AND OptionalFilterKeywords LIKE '%Facebook%' AND OptionalFilterKeywords LIKE '%Email Message%') OR (ArtifactCategory = 'Social Networking' AND ArtifactBrand = 'Facebook' AND ArtifactType = 'Email Message')) ORDER BY ActivityTimeLocal ASC
```

4. Facebook photo URLs

```
SELECT * FROM Records WHERE HideRecord = 0 AND ((OptionalFilterKeywords LIKE '%Social Networking%' AND OptionalFilterKeywords LIKE '%Facebook%' AND OptionalFilterKeywords LIKE '%Photo Url%') OR (ArtifactCategory = 'Social Networking' AND ArtifactBrand = 'Facebook' AND ArtifactType = 'Photo Url')) ORDER BY ActivityTimeLocal ASC
```

5. Facebook Wall posts

```
SELECT * FROM Records WHERE HideRecord = 0 AND ((OptionalFilterKeywords LIKE '%Social Networking%' AND OptionalFilterKeywords LIKE '%Facebook%' AND OptionalFilterKeywords LIKE '%Wall Post%') OR (ArtifactCategory = 'Social Networking' AND ArtifactBrand = 'Facebook' AND ArtifactType = 'Wall Post')) ORDER BY ActivityTimeLocal ASC
```

6. Facebook Profiles

```
SELECT * FROM Records WHERE HideRecord = 0 AND ((OptionalFilterKeywords LIKE '%Social Networking%' AND OptionalFilterKeywords LIKE '%Facebook%' AND OptionalFilterKeywords LIKE '%Profile%') OR (ArtifactCategory = 'Social Networking' AND ArtifactBrand = 'Facebook' AND ArtifactType = 'Profile')) ORDER BY ActivityTimeLocal ASC
```

7. Twitter Tweets:

```
SELECT * FROM Records WHERE HideRecord = 0 AND ((OptionalFilterKeywords LIKE '%Social Networking%' AND OptionalFilterKeywords LIKE '%Twitter%' AND OptionalFilterKeywords LIKE '%Tweet%') OR (ArtifactCategory = 'Social Networking' AND ArtifactBrand = 'Twitter' AND ArtifactType = 'Tweet')) ORDER BY ActivityTimeLocal ASC
```

8. Twitter Photo URLs:

```
SELECT * FROM Records WHERE HideRecord = 0 AND ((OptionalFilterKeywords LIKE '%Social Networking%' AND OptionalFilterKeywords LIKE '%Twitter%' AND OptionalFilterKeywords LIKE '%Photo Url%') OR (ArtifactCategory = 'Social Networking' AND ArtifactBrand = 'Twitter' AND ArtifactType = 'Photo Url')) ORDER BY ActivityTimeLocal ASC
```

9. Firefox:

```
SELECT * FROM Records WHERE HideRecord = 0 AND ((OptionalFilterKeywords LIKE '%Browser Activity%' AND OptionalFilterKeywords LIKE '%Firefox%') OR (ArtifactCategory = 'Browser Activity' AND ArtifactBrand = 'Firefox')) ORDER BY ActivityTimeLocal ASC
```

10. Chrome

```
SELECT * FROM Records WHERE HideRecord = 0 AND ((OptionalFilterKeywords LIKE '%Browser Activity%' AND OptionalFilterKeywords LIKE '%Google Chrome%') OR (ArtifactCategory = 'Browser Activity' AND ArtifactBrand = 'Google Chrome')) ORDER BY ActivityTimeLocal ASC
```

11. Internet Explorer

```
SELECT * FROM Records WHERE HideRecord = 0 AND ((OptionalFilterKeywords LIKE '%Browser Activity%' AND OptionalFilterKeywords LIKE '%Internet Explorer%') OR (ArtifactCategory = 'Browser Activity' AND ArtifactBrand = 'Internet Explorer')) ORDER BY ActivityTimeLocal ASC
```

12. LinkedIn

```
SELECT * FROM Records WHERE HideRecord = 0 AND ((OptionalFilterKeywords LIKE '%Social Networking%' AND OptionalFilterKeywords LIKE '%LinkedIn%') OR (ArtifactCategory = 'Social Networking' AND ArtifactBrand = 'LinkedIn')) ORDER BY ActivityTimeLocal ASC
```