# Social Network Forensics: Evidence Extraction Tool Capabilities

JUNG SON

MNZCS, Postgrad Dip. Computing (UNITEC, NZ), Dip. InfoTech (AUT, NZ), Cert. Computing (AUT, NZ)

A thesis submitted to the graduate faculty of Design and Creative Technologies
AUT University
in partial fulfilment of the
requirements for the degree of
Masters of Forensic Information Technology

School of Computing and Mathematical Sciences

Auckland, New Zealand

2012

# 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.

.....

Signature

# Acknowledgements

The thesis was completed at the Faculty of Design and Creative Technologies in the school of Computing and Mathematical Sciences at AUT University, New Zealand. This research task has been completed with the insight, support, practical assistance and guidance from many people:

Firstly, I would like to thank my family. My master's degree journey has been possible and even pleasurable due to the enthusiasm and goodwill of all my extended family. In particular, my wife Hi Sung has been unfailingly cheerful in organising her availability to suit my study commitments. My parents, Tiger and Jenny, and brother, Sam, have provided much-needed additional mental support, along with their interest and encouragement.

I have been lucky with an exemplary supervision experience through out my master's degree programme at AUT University. I would like to show my gratitude to my supervisor Dr Brian Cusack. Dr Cusack has guided me with precision, encouragement, humour and compassion. He provided me with a clear framework for the thesis construction, and supports me with tools and intellectual space to bring my ideas alive. I would also like to show my gratitude to the software vendors who provided free trial access to their software with extended period of time, including: John Bradley at SiQuest Corporation, Jad Saliba from JADsoftware. Their generous contributions have been invaluable to me and this research would not have been possible without this resource. My dear colleagues have had to tolerate my unavailability for much of the past one year, and to fit in with my very limited social/work calendar. My heartfelt thanks to my boss Rob Martindale, who has provided his professional interest, unconditional support, and encouragements.

I would like to extend my gratitude to my quality reviewer Peter Wilson. In writing my thesis, I have received generous advice from Peter Wilson, who agreed to provide me with assistant in proof reading of my lengthy thesis with helping track down grammatical errors. Peter provided stimulating discussions, challenging questions, and many exciting debates in my chosen area of Social Network Forensic research.

Lastly, thank you to my fellow student Tom Laurenson for his friendship, inspiration and continued ideas and enthusiasm.

# Abstract

The introduction of Social Networking Sites (SNSs) in recent years caused an explosion in consumer participation and these sites now attract hundreds of millions of users from around the world. Likewise, blogs and wikis are increasingly popular Web 2.0 venues that can evolve into formal communities of interest, providing significant knowledge-sharing and learning opportunities. Used appropriately, these venues therefore represent a valuable public space. Unfortunately, because a majority of the users of these sites are young people, the sites also tend to attract online predators and others who would exploit the sites. It is opportune to review and test the capability of different Digital Forensic tools that have practical application in the extraction of potential evidence from SNSs such as Facebook™, Twitter™, LinkedIn and Google+™, in the event of criminal activity.

This research evaluates evidence extraction tools in a systematic and forensically sound manner and based on the findings of the literature review in this research, to measure the capability of extracting evidence from SNSs in different test scenarios. The research question underpinning this research asks whether the existing digital forensic tools have enable forensic investigators to enhance investigative process, and what features there are in each tool that can collect evidence from SNSs. This research will explore evidence extraction tool capabilities by posing the following main research question:

***What are the capabilities of the 3 chosen tools to collect and analyse evidence from Social Networking Sites in a digital forensic investigation?***

There are volumes of blog articles and ACM publications on social network technologies that reflect research in a full range of related topics. However, although there is a large body of literature on social networks generated since 2009, there are only a few articles on forensics in SNSs. The available literature is concerned with the impact of social networking on society in general, rather than how to find evidence from social networking sites.

In the proposed research, a samples of three software tools are evaluated for capability after a thorough review from literature about the available tools. A simulated social networking site is constructed in a controlled environment, and then

stress-tested. The three selected tools are used to extract social network chat or web pages from allocated space on a hard disk partition, from unallocated space, and generated log data. Each tool is assessed for scope and capability. Advice on best practice for compliance with forensic data acquisition principles can be made based on performance. These outcomes can contribute to gaps in the current literature on conducting digital forensics investigation for SNSs.

The research found that evidence extraction from SNSs is complex as evidence is typically not saved on the hard drive, and artifacts are stored in many different places, depending on a number of variables. Given that the data exchange in question creates largely volatile data for which no guarantee of later data retrieval is given, all tools attempting to recover SNS data as evidence meet this condition as a fundamental constraint. There is no guarantee of the survivability of data created during user interaction with SNSs. Field testing results shows that some tools can extract Facebook Chat messages but no other details, some tools could recover send dates and times for chat messages as well as users ID, and detailed messages. The research testing results provide an understanding of the capability of the evidence extraction tools. The findings help the forensic examiner determine the accuracy and effectiveness they can expect when they need to use a particular tool.

The tools evaluated in this research, for their strengths and weaknesses, can dramatically improve the efficiency of a knowledgeable forensic examiner. The research findings presented may be valuable for law enforcement agents and digital forensic investigators in identifying current issues and limitations of the tools, and for software vendors to recognise the limitations of the tools, so that they can improve the tools for better extraction capability. It is hoped that the research findings may contribute to the future development of a social network artifact extraction tool, or to the enhancement of existing tools.

# Table of Contents



# Chapter One - Introduction



# Chapter Two - Literature Review

# Chapter Three - Research Methodology



# Chapter Four - Research Findings

## Chapter Five - Discussion



## Chapter Six - Conclusion



## Appendix

# List of Tables

# List of Figures

# List of Abbreviations

| | |
|---|---|
| AHP | Analytic Hierarchy Process |
| ATA | Advanced Technology Attachment |
| CD | Compact Disc |
| CFTT | Computer Forensic Tool Testing |
| CPU | Central Processing Unit |
| DCO | Device Configuration Overlay |
| DDR | Double Data Rate |
| DFF | Digital Forensics Framework |
| EXT2 | Second Extended Filesystem |
| FAT | File Allocation Table |
| FTK | Forensic Took Kit |
| GB | Gigabyte |
| GHz | Gigahertz |
| GPS | Global Positioning System, Global Positioning System |
| HDD | Hard Disk Drive |
| HKBS | Hybrid Knowledge Based System |
| HPA | Host Protected Area |
| HTML | Hypertext Markup Language |
| IDE | Integrated Drive Electronics |
| IE | Internet Explorer |
| IEC | International Electro technical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IEF | Internet Evidence Finder |
| IP | Internet Protocol |
| ISO | International Organization for Standardisation |
| JSON | JavaScript Object Notation |
| MD5 | Message Digest algorithm 5 |
| NIJ | National Institute of Justice |
| NIST | National Institute of Standards and Technology |
| NTFS | New Technology File System |
| PARD | Photograph Aspect Ratio Differential |
| PC | Personal Computer |

| | |
|---|---|
| PDAs | Personal Digital Assistants |
| RAM | Random Access Memory |
| RMC | Recover My Chat |
| RPM | Revolutions Per Minute |
| SANS | SysAdmin, Audit, Network, Security |
| SATA | Serial Advanced Technology Attachment |
| SHA1 | Secure Hash Algorithm version 1 |
| SNSs | Social Networking Sites |
| SQL | Structured Query Language |
| SWGDE | Scientific Work Group on Digital Evidence |
| TCP | Transmission Control Protocol |
| TIM | Tableau Imager |
| UAC | User Access Control |
| UFS | Unix File System |
| URL | Uniform Resource Identifier |
| USB | Universal Serial Bus |
| UTC | Coordinated Universal Time |
| VFAT | Virtual File Allocation Table |
| WSM | Weighted Scoring Method |

# Chapter One

# INTRODUCTION

## 1.0 BACKGROUND

Social Networking websites are widely used for people to openly exchange ideas and to interact publicly in cyber space. It would seem that the introduction of Social Networking Sites (SNSs) tapped into the human desire to be able to communicate with other like-minded individuals in a convenient and reasonably safe fashion, a desire that has manifest in young people in particular. For instance, according to Van Tassel (2006), "The popularity of social network sites demonstrates the power of user-created content. Social networking sites are mainly populated by young people in their teens and twenties" (p. 181). There is also a higher level of content oversight provided in most SNSs compared to other Web 2.0 venues such as blogs and wikis. In this regard, Van Tassel adds that, "User-generated content destinations require some administration. The procedures and rules for posting material must be clear, prominently displayed and strongly enforced, usually by paid moderators. Sites for the general public must often guard against pornography and offensive graphics and language" (p. 181).

SNSs were initially used for the purpose of promoting friendship. However, since networked computers allow social networks to expand and grow in ways that were previously unanticipated, more criminals utilise SNSs to achieve their goals (Coyle & Vaughn, 2008). This indicates that the SNSs are host to many people who pose a threat to security and legitimate use of online social networking services (Coyle & Vaughn, 2008). Notwithstanding their potential for misuse in these and other ways, it is clear that SNSs are going to continue to increase in popularity, at least for the foreseeable future. To put the explosive growth of SNSs in perspective, literature review conducted in this research noted that more than two in five online New Zealanders (42%) are interacting with companies via social networking sites and 79% of 1.8 million New Zealand social networkers call Facebook their main social networking site (Sultana, 2010).

More recently, social networking websites have become accessible not only via a web browser, but also by mobile devices such as PDAs and smartphones. In this

case, using conventional digital forensic tools for collecting and analysing evidence is not appropriate. Criminal investigation can be complicated if the crime involves social networking technology because information can be posted on a number of different social network spaces, and if evidence found from these SNSs is not collected in the most timely and efficient way, other complications can be caused such as wrongful convictions.

While the increase in the number of users in SNSs has resulted in an increased number of crimes, there are limited studies focused on identifying the existing tools capability of extracting evidence from SNSs. It is also noted from the literature review that there is no accepted model for professional standards or any standardised tools that the investigator can use in this area. Section 2.6 discusses the details of issues and problems in digital forensics investigations in social network environments.

The aim of this research is to evaluate existing digital forensic tool extraction capability from SNSs with the test scenarios developed herein. The test scenarios developed in this research tries to retrieve the information posted on SNSs from the target hard disk. However, as information is posted in the Internet space, the information is volatile and it is commonplace that the investigator finds a challenging task in gathering evidence from computer systems. Retrieving artifacts from SNSs is a relatively complex task as artifacts are stored dependant on a number of variables, or may not be stored on users' hard disk at all. Thus, there are the prospects that a digital forensic investigator may miss evidence and that there is insufficient evidence extracted to support the case. To assist in avoiding this scenario, this research aims to assist forensic investigators to identify existing tools capability to extract SNSs related evidence that resides on user's hard disk. All research has been carried out in the interest of gaining a better understanding of the capability of extraction tools that can retrieve the information posted on SNSs. This includes testing tools against to 11 field test scenarios and aims to answer the research question proposed in Section 3.2. The proposed research question to be addressed in the research is:

> ***What are the capabilities of the 3 chosen tools to collect and analyse evidence from Social Networking Sites in a digital forensic investigation.***

## 1.1 MOTIVATION

The background to this research is briefly discussed in Section 1.0 in order to understand the importance of the chosen research areas. This section discusses the motivation of the author ranging from the popularity of SNSs to the lack of supported digital forensic tools available to conduct investigation on SNSs.

Digital forensic investigators are relying on digital forensic tools to extract evidence from digital devices in order to examine evidence more effectively and in a forensically sound manner (Pollitt, 2008). Following the trend in demand, tools and techniques in digital forensics have been developed in recent years due to an increase in the number of digital crimes. Even though there are many digital forensic tools developed to extract evidence from digital devices, these tools do not yet appear to support extracting evidence from SNSs such as Facebook, Twitter, LinkedIn, and Google plus. This is because SNSs are a very new field in digital forensics, and it is different from extracting normal fixed file data from hard drives, as some, and perhaps the majority of information posted on SNSs are kept on the server rather than the user's computer.

It is noted from the literature review that extracting information posted on SNSs is not widely supported by existing digital forensic tools as of yet. Some of the common SNSs artifacts that could be extracted from users computer includes: Online chat messages, wall post, status update, pictures, videos, GPS information, email, and web browsing history. Because of the digital landscape is highly changeable, with new emerging technologies like SNSs, digital forensic investigators have to start moving beyond just getting evidence extraction from data saved on a suspect's computer. In order to do this, it is important to develop new digital forensic tools and techniques. It is also important to provide mitigation for missing data from the extraction process. Significant gaps in the amount of data may result, as information posted on SNSs as data is not saved on the users' computer. Investigators used to be able to reconstruct data relatively easy in traditional digital forensics because data is not actually deleted in most cases. However, performing digital forensics in SNSs is a difficult task due to the limited sources of evidence available, and the investigator may only reconstruct evidence from fragments of data remaining on the hard drive.

Presenting extracted data from SNSs is another challenge for the digital forensics investigator. Even though tools can extract Internet artifacts, there are some technical constraints for presenting fragmented of data. The task is so demanding that investigators struggle to transform the data into a human readable format that can be presented in a court of law (Golden G. Richard & Roussev, 2006). There is no doubt that the tools' capability of providing a snapshot of the data from different perspectives is arbitrarily driven by what the investigator wants to look at. The investigator has options within the tools configuration to provide extraction findings from SNSs as well as formatted and easily digested summaries with some of the tools, whereas investigator spend most of the time putting the data into the correct format and then analyse the extracted data.

In summary, the preceding discussion illustrates the demand for evidence extraction tools that can extract artifact from SNSs. Social network form a massive part of todays, and the futures digital landscape, and is represented in a variety of forms especially via SNSs like Facebook, Twitter, LinkedIn, and Google Plus. The increasing popularity of social networks has started to provide evidence that can be used in digital forensic investigation (Haggerty, 2010). When social networking sites and other Web 2.0 venues are exploited for identity theft, fraud or sexual predation, there is a need for effective forensics tools that can be used to identify the perpetrator(s) and collect the evidence needed for prosecution, a need that directly relates to the main research question proposed in this research.

## 1.2 STRUCTURE OF THESIS

This paper is composed of 6 chapters. Chapter 1 "Introduction", Chapter 2 "Literature review", Chapter 3 "Research Methodology", Chapter 4 "Research Findings", Chapter 5 "Discussion", and Chapter 6 "Conclusion". Chapter One introduces the importance of the research topic, and background of the research as well as motivations for this research.

Chapter 2 presents a literature review, and recent studies in the digital forensics area particularly in Social Network. Literature topics reviewed in Chapter 2 include: characteristics of SNSs, overview of digital forensics environments, digital evidence, evidence extraction tools, ethical issues in digital forensics especially in the field of

SNSs, and issues and problems in Social network forensics. The Social Networking Sites (SNSs) are introduced and explained at the beginning of the chapter. Characteristics of SNSs are explored to help the researcher to understand the implications of Social Network forensics. The review of the digital forensics environment alerts the importance of digital forensics investigation processes. It also reviews the definition of the 4 components of digital forensics reviewed in this chapter, and explains the differences between digital forensics, network forensics, social network forensics, and web browser forensics. The chapter then reviews currently available market leading digital forensic tools, to understand the trends in development of digital forensics tools. Chapter 2 concludes with a summary of ethical issues and problems associated with social network forensics, and seek a way to mitigate ethical concerns in the area of social network forensics investigation.

In Chapter 3, a number of similar approaches in the chosen research field are reviewed and evaluated. Chapter 3 begins with a review of five similar approaches to develop research methodology for this research in order to be used as guidance for field-testing phase. These similar approaches are on the topics of: General approach for testing computer forensic tools, Tools testing and analytical methodology, validation of forensic computer software, data recovery function testing for digital forensic tools, and framework for evaluation and selection of the software. Reviewing studies conducted by scholars in similar research fields helped to identify a research model that can be adapted for this research, to answer the research questions proposed in the previous chapter. Research design with four steps of research testing phase is developed, and a data map is presented to outline the process of research. Expected outcome and any limitations of this research have been identified at an early stage to mitigate the possible impacts on field-testing activities.

Chapter 4 reports the research findings from the research design model and data collection phases outlined in Chapter 3. Any changes made during the field-testing phase are acknowledged and explained in the beginning of the chapter 4. Collected data from the research-testing phase are analysed and the summary of findings is presented in a tabular and graphic format.

Chapter 5 discusses key findings and the analysis result presented in Chapter 4. Based on the findings summary provided in chapter 4, the research questions and sub-questions discussed in chapter 3 are addressed. Validity of proposed hypotheses is checked based on discovery from the field test finding results. Significant findings identified in chapter 4 provide comprehensive discussion on the strength, weakness, and limitations of each tool.

Chapter 6 summarises the research findings. The research question and sub-questions identified in chapter 3 are answered in chapter 6. The chapter concludes the discussion by providing possible future development opportunities and seeks possible areas for future research, followed by the conclusion of the thesis.

The appendices are provided at the end of the thesis as supplementary information. Appendices include testing environment information, generated baseline data, field finding procedures and set of results from testing phase.

# Chapter Two

# LITERATURE REVIEW

## 2.0 INTRODUCTION

The forensic field is constantly changing, with the rapid development of technologies. Traditional forensic science has provided a foundation for legal proceedings for more than 100 years (Pollitt, 2008). This traditional forensic science has influenced a number of areas due to the increasing number of computer crimes. Digital forensics practitioners can learn much from the traditional forensic process. According to Casey (2004), some of the earliest recorded computer crimes occurred as far back as in 1969 and 1970. Digital forensic investigators applied traditional science in order to investigate computer related crimes. Due to the largely intangible nature of the evidence (something that cannot be precisely measured or assessed in human term), there were legal struggles law protecting physical asset (Forbes, 2011). The distinction between digital forensics and traditional forensics started to become apparent the late 1980s responding to the growth of computer crimes (Casey, 2004, p. 25). Since then, digital forensics has always referred to a method of collecting criminal evidence from any digital medium, in order to present it in a court of law. In the early digital forensics stage, investigators used the suspects' computers itself to obtain evidence. However the integrity of the evidence may be lost during the investigation process as the computer itself could alter the evidence. It is no longer practical to use the suspects' computer to obtain evidence. As a result, a number of digital forensic tools have been developed to help investigators do their work effectively and in a forensically sound manner. There are no standard tools for collecting or processing evidence from social networking environments. Even though there are a number of vendors now offering forensic tools, forensic investigators may face problems choosing the right tools when they may not fully understand the tools.

The research objective of Chapter 2 is to critically review the recent literature related to the three study areas; namely Social Networking Sites (SNSs), digital forensics, and evidence collection tools. Literature on SNSs and digital forensics will be reviewed in chapter two, to form a contextual basis for the research as a whole.

Firstly, an acceptable definition of the term 'social networking sites' must be derived, and why people use them. The link is then made to the second topic, that of digital forensics and the need to follow standardised processes in acquisition, preservation, analysis, and reporting of evidence from social networking sites. The literature review not only serves to find information about existing technologies, but also identifies possible issues from where potential research questions may derived. Section 2.1 introduces:

The term of Social Networking Sites (SNSs)
Statistical usage record of these SNSs
Why SNSs are an important in digital forensics
How SNSs can be misused or targeted

A section 2.2 discusses the digital forensics environments as well as defines digital evidence and the processes of digital investigation in digital forensics. A number of digital forensics tools are reviewed and evaluated in depth in Section 2.3 to 2.4. Ethical issues related to digital forensics and Social network forensics are discussed in the Section 2.5. Finally, the issues and problems related to Social Network Forensics that were encountered in the literature review will be identified and discussed in Section 2.6, which will demonstrate the relevance of this research.

## 2.1 SOCIAL NETWORKING SITES

At the most basic level, social networking sites are simply online forums in which users come together at their convenience to share information in the form of digital text, graphics, links and so forth, empirical observations, or sometimes just to chat. A useful definition of social networking sites provided by Carter, Foulger and Ewbank states that these 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"* (2008, p. 682).

Web 2.0 includes those social networking sites as well as Blogs and Wikis, and Sites such as an Online Learning Management System also has components of Web 2.0.

According to Millard & Ross (2006), Web 2.0 is the popular name of a new generation of web applications: Sites that emphasis openness, community and interaction (Millard & Ross, 2006).

While social networking sites and Web 2.0 in general typically feature the ability to post information for others to view permanently, there are also sites that feature chat rooms and other forums where posts may be quickly deleted. Nevertheless, this information still leaves a record. In this regard, Carter et al note that, "These sites are not unlike the old-fashioned 'party line' telephones, but they leave a more permanent record of the conversations" (2008, p. 682). The type of data that is generated in a social networking site is impressive. For example, Carter et al. add that, "Most social networking sites include the ability to conduct live chats, send e-mails, upload videos, maintain a blog or discussion group, and share files. Users can also post links to pictures, music, and video, all of which have the potential to create a virtual identity" (2008, p. 682).

One of the more compelling features of social networking sites is their ease of use. Registering is a simple and guided affair involving little more than creating an account and a user profile. Once these steps are completed, the site is open ground for exploration, posting of user-generated content and the creation of countless online relationships with others who share similar interests and views (Carter et al., 2008). Most larger social networking sites such as Facebook provide their users with various privacy setting levels that allow only certain people access to user pages. In this regard, Carter and her associates report that, "A mutual relationship between users called 'friending' links profiles together, creating the backbone of the website's social network. If the profile is set to private, then only 'friends' can view the entire page" (2008, p. 682). Other sites use similar features to restrict who is allowed access to user-generated content and for viewing an individual's profile (Carter et al., 2008). Beyond these minimal requirements, social networking sites are wide open in terms of content, limited only by the agreed upon protocols and manners established for the venue. By July 2006, there were already more than 140 different social networking sites available on the World Wide Web, with hundreds of millions of users (Anklam, 2007).

The Internet has become a very important role in our daily communication. It is now beyond a mere information gathering tool. It is now a space for learning and sharing information. Social Networking Sites (SNSs) are enabling us to communicate with others via Internet and share common interests in hobbies, religion, or politics. Definition of SNSs are summarised as below.

**Table 2.1: Definition of Social Media & Networking Sites**

| Source | Definition |
|---|---|
| Boyd & Ellison (2007) | 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. |
| Ahn, Han, Kwak, Moon & Jeong (2007) | Provide an online private space for individuals and tools for interacting with other people in the Internet.<br>Provide users with an online presence that contains shareable personal information, such as a birthday, hobbies, preferences, photographs, and writings. |
| Chen, Geyer, Dugan, Muller & Guy (2009) | Allow users to articulate their social networks by adding other users to their "friend lists". |
| Safko & Lon (2009) | SNSs are part of Social media and it refers to activities, practices, and behaviours among communities of people who gather online to share information, knowledge, and opinions using conversational online media. SNSs make it possible to create and easily transmit content in the form of words, pictures, videos, and audios. |
| Mangold & Faulds (2009) | A wide range of online, word-of-mouth forums including blogs, discussion boards and chat rooms, consumer product or service ratings websites and forums, Internet discussion boards and forums. |

### 2.1.1 Characteristics of Social Networking Sites

"Social networking sites (SNS)" means web-based online media platform services that allow for social interaction, allowing the creation and exchange of user-generated content (Boyd & Ellison, 2007). Boyd and Ellison stated that social networking sites enable users to articulate and make visible their social networks and this can result in connections between individuals that would not otherwise be made. SNSs are part of social media and it is based on Web 2.0 based websites. As summarised in Table 2.1, SNSs have in common five main characteristics, which are - Participation, Community, Public access, Communication and Connections.

**Table 2.2: Characteristics of Social Networking Sites**

| Category | Description |
|---|---|
| Participation | Social networking sites encourage participation and promote feedback from site users. |
| Community | People can create their own community and share their common interests. This community can be a place to share information and gather information. |
| Public | Most Social Networking Sites enables user feedback and contribution in a way user can interact with others publically. Thus, there are fewer barriers to access and use of these sites. |
| Communication | While traditional media provide one-way communication, SNSs provide two-way communication. |
| Connection | Most of Social Networking Sites getting popular by having more users and users connection to other members of the site. Sites also help you get in touch with those people whom you no longer meet in your everyday life. |

In summary, SNSs are allowing social activities in Web 2.0-based websites. SNSs are rapidly growing, and spread quickly because of their characteristics and the development of cutting edge technologies such as smartphones. In other words, SNSs induce large numbers of people to create and share information, provide a place where people can express their own feelings, and enables people to check and update information anytime without geographical barriers. These characteristics of SNSs induce people to use SNSs often, and it is expected that this trend will most likely to continue (Boyd & Ellison, 2007). As more people in the world's Internet population

visit social networking sites, this also indicates that evidence we can collect from these websites is likely to grow as time spent on social networking sites is growing more. The most popular social networking websites used at the time of writing include - Facebook, Twitter, LinkedIn, MySpace and Google Plus.

**Table 2.3: Popular Social networking websites.**

| Site Name | Key Features |
|---|---|
| Facebook | Make friends, Upload photos, post videos, get news, tag friends, view friend's status. |
| Twitter | Keep people informed on what you are up to. Updating personal status with limited characters and following others. |
| LinkedIn | Build professional network, update career profile. LinkedIn is a business-oriented social networking site. |
| MySpace | Create a profile page that people can use to meet new friends. User can post videos, movies, news, and blog. |
| Google Plus | Social networking site provided by Google. It provides similar features like Facebook – connect friends, share photos and video and view friend's status. |

### 2.1.2 The modern media of Social Networking Sites and cultural factors

SNSs have played an important role to lead political and social culture of communications along with offline areas. For example, U.S. White House posted Obama's public schedule for press conference and TV interview schedule on Twitter prior to deployment on news media, U.S. General Accounting Office (GAO) and the Department of Defence also promote communication between people via social networking sites.

In the course of the 2008 U.S. Presidential election, Barack Obama's presidential campaign showed an example of using social networking sites. The campaign showed a case where the centre of public opinion formation has shifted from existing mass media to open Internet-based social networking sites. Obama has taken 'grassroots' campaigning into the digital age by using Web 2.0 and using it as a central communication tool of his presidential campaign. For example, he utilised his 1,450,000 Twitter followers by setting up a page in Facebook and in MySpace and posting his policies, his growth process, and information about the vice president.

He made sure his speeches sound good on the YouTube website. He has not only posted his own speech on YouTube but also posted his supporters video and gathered more than 300 million supporters by having supporter button on the YouTube site. A book published by New Riders, 2009, reported that Obama's YouTube video generated 3.4 million views in the first ten days alone (Rahaf & Harfoush, 2009). He also used an online-based fund-raising strategy. Barack Obama raised 6.5 million online donors and raised $300 million dollars online.

Social networking sites facilitate the concept of social relationships on the Internet, which enables us to have variety of connections, and share information across geographical and language boundaries, connecting people around the world. This presidential campaign from U.S. shows how powerful this social networking site can be. As illustrated superbly by the Obama's presidential campaign in 2008, social networking sites will not only impact the adoption and being embraced by most organizations, but that its reach and ubiquity will be much more far-reaching. Social networking site brought us some concerns such as invasion of privacy as it is created based on mutual trust and an open structured system on a public facing websites. Today, it is clear that social networking sites are growing in popularity and breadth of content, making the need for sophisticated forensics tools that can document evidence of online criminal activities in these venues all the more important.

### 2.1.3 Social Networking Site Usage by Country

Through Social Networking sites such as Facebook, Twitter and Google Plus, communication flows freely and we can share information easily. It is different from old days one-way communication method and this difference made many changes in daily life. When formed specifically to acquire information, the power of those who distribute the information will be greatly enhanced in the communication process. This phenomenon still applies to the field of digital forensics. Thus, it would be beneficial to compare social networking sites usage by different countries such as New Zealand, U.S.A and South Korea, where their cultural and jurisdictional background is different. This comparison will show us what is the most dominant social networking sites in each countries and also indicate us how and why people use social networking sites.

#### 2.1.3.1 New Zealand

Social networking site has been also widely used in New Zealand. A report released by the New Zealand parliament states that the majority of New Zealand members of Parliament have at least one online social networking site account (Busby & Bellamy, 2011). According to Montalk (2011), Facebook is the most popular of the social networking sites with New Zealand MPs, with all members of ACT and the Greens having legitimate accounts, followed by about 95 per cent of Labour MPs (De Montalk, 2011).

Recently, The University of Auckland and AUT University launched their official Facebook sites and the New Zealand Prime Minister, John Key, opened a new political front, with the launch of his official Facebook site. This trend is not limited to organisation or politicians. Statistics New Zealand conducted a survey in 2009 to check household use of Information and Communication Technology. In this survey, thirty-seven per cent of respondents reported that they used the Social Networking Sites (Bascand, 2010). This trend is increasing for New Zealanders at a rapid rate, with social networking sites such as Facebook and Twitter. According to a recent study conducted by AC Nielsen, more than two in five online New Zealanders (42%) are interacting with companies via social networking sites and 79% of 1.8 million New Zealand social networkers call Facebook their main social networking site (Sultana, 2010). The trend upwards increased to 37% in 2009 from 17% a year earlier.

#### 2.1.3.2 USA

Social networking sites (SNSs) have been most widely spread in the United States of America. Currently about 65% of the Internet population uses social networking sites, and the world's most famous sites such as Facebook and Twitter were created from the U.S. There are more than 400 million users worldwide, and 130 million (30%) of these users are Americans. Because there are so many users in SNSs, a lot of businesses view SNS's as a marketing and advertisement opportunity and SNSs become beyond the means of a simple advertisement and go further to the means of information distribution tool from the trusted source.

As of September 2009, Internet advertising market took 20.3% of online advertisement spending and eMarketer has come predicted that U.S. based marketers will spend $3.08 billion dollars in advertising on SNSs in 2011.

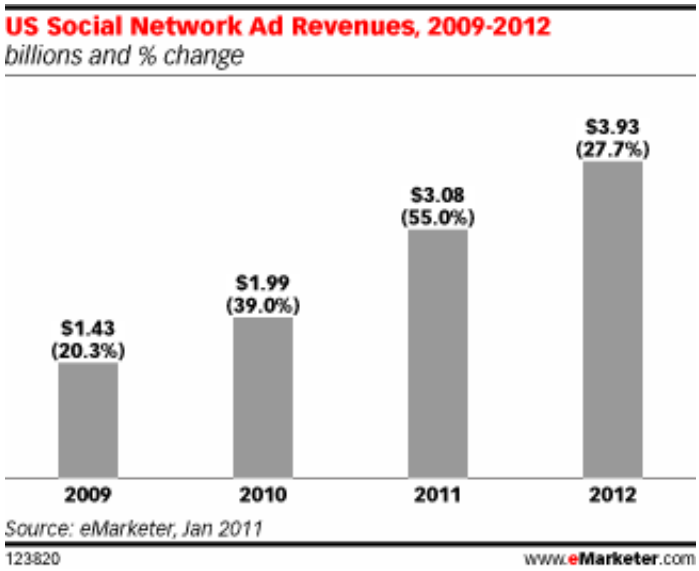



**Figure 2.1: US Social network advertising revenues, 2009-2012 (eMarketer, 2011)**

#### 2.1.3.3 South Korea

South Korea's Internet population has been steadily increasing in recent years. By May 2010, approximately 77.8 per cent of South Korea's 49 million people were using the Internet, according to new government figures reported by statistics Korea (Statistics Korea, 2009). South Korea has become one of the most connected countries in the world, and 61.3% of Internet users are using SNSs at least once a month while 71% of people think SNSs are very important communication tool. Most people use SNSs to keep in touch with their friends and about 87.9% of users have experienced forming new relationships via SNSs.

More people in South Korea are familiarising themselves with the popular social networking sites such as the global Facebook, Twitter and Linked In as well as the locally developed and most well known sites like Cyworld and Me2day with a rising number of those owning a smartphone. The most famous SNS in South Korea is called Cyworld, which is the largest and oldest online social networking service in South Korea (Ahn, Han, Kwak, Moon, & Jeong, 2007). Cyworld has about 24 million registered users and it has expanded to the global market including China and Japan. Like the U.S, SNSs have become one of the significant communication channels for

politicians, primarily because of the power of relational networking (Park & Kluver, 2009). The South Korean Government recently launched a site on the Me2day social networking site and publishes a variety of content, including national news, presidential photos, speeches and other multimedia content.

## 2.2 OVERVIEW OF DIGITAL FORENSICS ENVIRONMENT

The origin of Forensic can start from the practice of forensic medicine meaning "of or used in law courts" (Oxford Dictionary1999, p. 305). One of the classic examples of forensic tasks is identifying fingerprints. The term "Forensic" has become more familiar to the IT community and law enforcement, as the number of criminal activities using computer has increased (Reith, Carr, & Gunsch, 2002, p. 10). Thus, the new term 'Computer Forensics' has been introduced and more recently it is referred to as digital forensics. Recently, the term has subdivided into network forensics, Internet forensics, and Social Network Forensics.

With the rapid growth of social networking sites, most business and government organisations are now putting their activities on social networking sites. Thus, having a Facebook page and Twitter account is becoming a more common concept in both private and public sectors. In this context, sensitive information such as personal, organisational, political and financial information can be posted or viewed widely. This sometimes can lead to illegal activities such as infringement of personal privacy. Due to the advent of computer crimes via these SNSs, social network forensics as a means of crime prevention has become a useful technology and SNSs can be a rich resource for forensic investigations. Therefore, it is critical that in the course of investigating crimes, there is a digital forensics expert to present scientific evidence with a systematic procedure that is legally proven and scientifically sound. Digital evidence gathered from social networking sites is subject to scrutiny, in particular regarding viability, and thus standard investigation processes must be followed.

The following section gives a brief introduction to digital forensics, network forensics and social network forensics. Currently available digital forensics investigation procedures and standards guides will be reviewed and a recommendation will be made for conducting social network forensic investigations. It is followed by comparison of different digital forensic tools that are relevant to this research.

### 2.2.1 Digital Forensics

Digital forensics can have many definitions as the definition can change as the perception of digital forensics changes. However, the meaning of digital forensics can have some common elemental components. McKemmish (1999) defined digital forensic as "the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable" (McKemmish, 1999). Berghel (2003) makes a similar definition to McKemmish. He defines digital forensics as: "preservation, identification, extraction, documentation, and interpretation of computer data" (Berghel, 2003). Furthermore, Venter, Labuschagne, & Eloff (2007, p. 1) defines digital forensics as the application of computer investigation and analysis techniques to determine potential evidence.

Traditional computer forensics involves collecting data from an electronic device where the data is going to be used in some kind of investigation or for law enforcement. Instead of just copying individual files, the digital forensics examiner creates what is called an image (bit-by-bit copy). This is a complete image of the whole hard drive store of information from a computer. The investigator can take that out of the computer and analyse the data image to find specific information, which can be files and folders or email conversations, but also Meta data, where computer stores information about the files themselves. For example, the data stamp for the file creation, when it was modified, who accessed the file last. Digital forensics investigators not only find the active files, but are also able to find deleted files, password protected files or overwritten files and these are the treasure of trove.

### 2.2.2 Network Forensics

Traditional computer forensics mainly deals with static data. For example, a hard drive, CD, or a Flash drive, where data recovery is needed. There are a number of tools to help digital forensic investigators recover and reconstruct evidence data from any particular medium. In network environments, data is transferred from one computer to another and this is when we need to use network forensic procedures when collecting evidence.

Meghanathan, Allam, & Moore (2009, p. 14) stated that network forensics deals with the capture, recording and analysis of network events in order to discover

evidential information about the source of security attacks for a court of law. Network forensics deals with ephemeral data and is critical as there are so many thousands of people creating and distributing viruses, spyware and malware via network. Berghel (2003) stated that the computer forensics investigator can have 'something to seize and investigate', whereas the network/internet forensics specialist only has something to investigate from the network packet filters, firewalls and wireless frames (Berghel, 2003).

The Digital Forensics investigator needs to have the ability to determine the scope of network related incidents very quickly, and 'rewind' the breach so that they can identify where to look for the potential evidence. Network forensic investigator might require the same skill set as hackers in order to identify what has happened and why it has happened, and also to identify the motivation for the crime. Being able to track and identify network events, or events between systems is becoming a more important skill in the network forensics field. Berghel's statement is apt:

> *"This is the time to change our focus from the negative (hacker) to the positive (Internet Forensics specialist) dimension of this exciting new discipline" (Berghel, 2003).*

As network forensics continues to grow and to gain acceptance among the both the IT industry and law enforcement, Digital Forensic investigators need to watch for network activities adequately and effectively in order to understand possible attacks and collect evidence from these attacks.

### 2.2.3 Social Network Forensics

Social networking sites are an important communication medium. Just like emails and instant messaging, social networking sites are excellent place for companies, businesses and governments to interact with the public and their customers. These social networking sites become an important communication medium for many organisations and people. Currently there are many criminal cases that are related to social networking sites or the use of social networking sites in order to commit crime. Chua (2009) stated that "The distribution of malware on social networking sites first occurred in small amounts towards the end of 2007, but that trend appears to be on the rise" (Chua, 2009). Further to this, he predicted that this trend is expected to increase

every month and is only going to continue. For example, Facebook is only going to be used more and Web 2.0 based websites, such as blogs and wikis, will only become more important in any cases in the digital forensics area. Haggerty (2010) stated that:

> *"Social network analysis may not provide tangible evidence to be used in a court of law per se, but will identify intangible evidence such as other suspects, potential sources of evidence or the suspect's level of involvement in a crime or malicious event" (Haggerty, 2010).*

With the popularity of social media, many people are willingly publicising where they live, their religion, their medical status, their friends, personal email addresses, phone numbers, photos of themselves and status updates, which informs people where they are and what they doing. Criminals can use these social networking sites to commit crimes. For example, a terrorist group may use a social networking site such as Google Plus (location-based social networking website) to identify popular locations for bombing, while drug dealers can use social networking sites in order to communicate with other dealers or their customers.

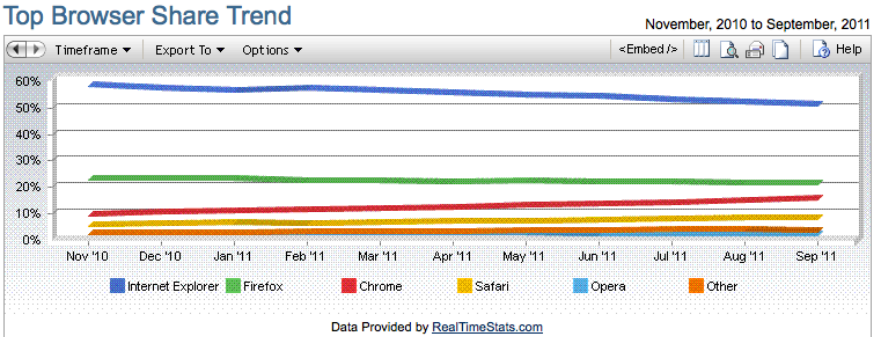
There is lack of definition in social network forensics as the field is not sufficiently familiar to the IT Community and it is new area to the law enforcement and computing domain. The term Digital Forensics is widely known and has been used for many court cases. A Google search produced 2,150,000 results for "digital forensics" and 97,100 results for "social network forensics". This simple search result indicated that the term "social network forensics" is not often used as the term "Digital Forensics" as of today. Social network forensics came after the revolution of social networking sites but the term social network forensics does not have accepted definition. However, social network forensics will be a major focus of Digital Forensics in the future, and it will be a major part of today's and the future digital landscape (Haggerty, 2010).

Digital Forensics has been developed in recent years and it has been widely used for computer crime investigation and tested in a court of law. Social network forensics can learn much from this process, as social network forensics is part of digital forensics, which deals with digital evidence gathered from social networking sites. In any digital forensic cases, investigators must follow the process that ensure the evidence is legally acceptable, and present all digital evidence in a forensically sound manner (McKemmish, 2008).

### 2.2.4 Web Browser Forensics

Ravi Kumar Jain (2007, p. 52) define web Internet forensics as the combination of advanced computing techniques and human intuition to uncover clues about people and computers involved in Internet crime. The web browser is defined as the navigation and rendering tool for the Web (Berghel, 2008). Therefore, web browser forensic can be considered as a part of Internet forensics, which is focused on the web browser's history, cache, and cookie information in particular.

As the Internet is widely used, a criminal suspect may use a web browser to connect to the Internet, and being able to find any evidence left by web browsing activity is a crucial component of digital forensic investigation. All of the well-known web browsers such as Mozilla Firefox, Google Chrome, Apple Safari, and Microsoft Internet Explorer saves users' activities in a cache, in the internet history list and in cookies in order to improve the user experience and save browsing time (Daniel & Daniel, 2012). Figure 2.2 shows the top 5 web browsers in market share as at 23rd October 2011.




| Month | Internet Explorer | Firefox | Chrome | Safari | Opera | Other |
|---|---|---|---|---|---|---|
| November, 2010 | 58.45% | 22.77% | 9.26% | 5.21% | 2.17% | 2.14% |
| December, 2010 | 57.09% | 22.81% | 9.98% | 5.57% | 2.21% | 2.34% |
| January, 2011 | 56.00% | 22.75% | 10.70% | 6.03% | 2.25% | 2.27% |
| February, 2011 | 56.77% | 21.74% | 10.93% | 5.76% | 2.12% | 2.67% |
| March, 2011 | 55.93% | 21.80% | 11.57% | 6.00% | 2.12% | 2.58% |
| April, 2011 | 55.11% | 21.63% | 11.94% | 6.51% | 2.11% | 2.70% |
| May, 2011 | 54.28% | 21.71% | 12.52% | 6.54% | 2.01% | 2.93% |
| June, 2011 | 53.68% | 21.68% | 13.11% | 6.80% | 1.70% | 3.02% |
| July, 2011 | 52.72% | 21.47% | 13.49% | 7.37% | 1.62% | 3.33% |
| August, 2011 | 51.59% | 21.03% | 14.46% | 7.71% | 1.58% | 3.62% |
| September, 2011 | 50.97% | 21.06% | 15.17% | 8.03% | 1.58% | 3.18% |

**Figure 2.2: Web Browser market share trend (Net application, 2011)**

Ravi Kumar Jain (2007, p. 52) also noted that a web browser creates log files, stores data in cache files, and stores cookies on a user's computer, which can be used as a computer forensics tool. He stresses that the web browser is one of the most extensively used forensic tools in investigating cyber crimes.

As each of the well-known browsers stores web access activities in their own native format in different locations, the activities related to SNSs are found in different locations according to the operating system and the version of the web browsers. As stated by Oh, Lee, & Lee (2011), tracing evidence of web browser use is an important process for digital forensic investigation and this will certainly become more important for tracking evidence from web related crimes, including SNS activities. Using appropriate tools to extract evidence from web browsers will certainly be useful in SNS investigation. It allows fast analysis and extraction of significant evidence from the suspected criminals web browsers activities.

### 2.2.5 Digital Evidence

While fingerprints and DNA are used as evidence in traditional forensics, digital evidence is used for digital forensics. Digital evidence can be called a 'Digital fingerprint' as computer systems and most of web browsers such as Internet Explorer and Firefox stores unique information that can be tracked by digital forensics investigators. Digital evidence comes from a variety of sources such as computers, memory sticks, mobile phones, emails, web sites and social networks. This evidence has been offered in an increasing number of criminal court cases recently (Brown, 2009). NIJ (2008) defines the "digital evidence" in the following manner:

> "*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).

This is consistent with Casey's definition of digital evidence. Casey (2004) has adapted from Chisum (1999) and defined digital evidence as:

> *"any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi"* (Casey, 2004, p. 12).

Another definition for digital evidence has been provided by SWGDE (Scientific Working Groups on Digital Evidence). SWGDE (2007) stated that "Digital Evidence is any information of probative value that is either stored or transmitted in a binary form," the word "binary" has been changed to "digital" at later stage.

Devices such as iPhone, digital camera, and computers, can also be connected to number of social networking sites. All of these things are digital devices and they contain evidence. The digital evidence includes digital audio/video, system logs, access logs, incidents, network packets transmitted via network and other records of what occurred in particular incidents. This evidence is often involved with computer intrusions, identify theft, fraud cases, child pornography, and intellectual property theft. As people use more digital devices and we can find more evidence from those devices, digital evidence is considered very important evidence and is encountered more each day by forensic investigators as well as lawyers and law enforcement agencies.

Digital evidence has to meet various criteria in order to be accepted and gain weight in court cases. This is because digital information has a number of characteristics and it can be sometimes complicated to present as evidence. The following section introduces some characteristics and problems of digital evidence.

#### 2.2.5.1 Characteristics and issues of digital evidence

Digital evidence can be changed, which is different from DNA. Thus, most guidelines highlighted that evidence must not contaminated during the course of collection. Once the digital evidence has been tampered with, the integrity of the evidence derived thereby vanishes. However, this may require a high level of computer knowledge to understand the concept, and most judges would not be able to recognise whether the original evidence has been changed during the examination. This is consistent with Casey's (2000) argument that digital evidence can easily be overlooked. Casey (2000) stated that:

> "*When several computers are involved, it is easy to overlook important digital evidence, neglect to collect digital evidence properly and document the investigation inadequately"* (Casey, 2000, p. 174).

This means innocent people may be convicted by overlooking data, or an incorrectly analysed report by an unprofessional forensic examiner could hold inappropriate weight.

Privacy is another issue in digital evidence. As the forensic expert is expected to collect and analyse the information, they have a chance to see clients' private or

secret information while they are performing the investigation. However when it comes to the courtroom and if they need to report the findings as an expert witness, they will not be able to keep the secrecy and privacy of the clients' information in order to prove a crime (McCarthy, 2009).

Digital evidence has many challenges due to its characteristics. Casey (2004) summarised characteristics and challenges of digital evidence and they are shown in table 2.4.

**Table 2.4: Challenging aspects of digital evidence (Adapted from Casey, 2004, p.16; NIJ, 2008, p.ix)**

| Digital evidence challenges | Details of challenging aspects of digital evidence |
|---|---|
| 1. Digital evidence is messy | Digital evidence is messy, slippery form of evidence that can be very difficult to handle. |
| 2. Duplicability and Modifiability | Digital evidence can be manipulated so easily raises new challenges for digital investigators. Digital evidence can be easily altered, damaged or destroyed during the collection process. |
| 3. Impossible to create complete reconstruction | Digital evidence is generally an abstraction of some event or digital object. Therefore, all of the puzzle pieces are never available, which makes it impossible to create a complete reconstruction of crime, |
| 4. Digital evidence is circumstantial | Digital evidence is usually circumstantial and this makes difficult to attribute computer activity to an individual. Therefore, digital evidence can only be a part of a solid investigation process. |
| 5. Changes of technology | With the rapid development of technologies, there are always new attacks and different way of committing the crime using new technologies. Digital investigators must follow the trend of technology and understand the attackers behaviour accordingly with cutting-edge technologies. |
| 6. Time Sensitive | Digital evidence is very time sensitive. For example, investigation into intellectual property theft case is generally time sensitive, as time of theft is crucial information. |
| 7. Cross geographical and jurisdictional borders | Internet/network crime often involves international components and evidence may come from different countries. Geographical and Jurisdictional differences between each country will make digital investigation process much cumbersome. |

Government, technicians and law enforcement have developed techniques and standards about digital forensics in order to prevent those characteristic issues with digital evidence. As a classic example, NIJ (National Institute of Justice) from U.S. Department of Justice has been producing number of guidelines and reports related to this matter (NIJ, 2008).

### 2.2.6 Investigative Processes and Standardisations

Investigation processes for digital evidence can be divided into number of steps and there are number of scholars proposed investigative process model. U.S. Department of Justice published an investigative process model in the electronic crime scene investigation. According to guide to first responders, the process consists of four major phases: collection, examination, analysis and reporting (NIJ, 2008).

Similar investigative process framework has been proposed by Beebe & Clark. They divided process in to following 6 phases: preparation phase, incident response phase, data collection phase, data analysis phase, presentation of findings phase, and incident closure phase (Beebe & Clark, 2005). There are number of publications and research papers, which proposed new investigation process model or frameworks. The process model varies case by case and it seems that there are no consistencies in digital forensics investigation process as many scholars have proposed different investigation process. However, most part of the processes or frameworks is overlapping with other investigation related discipline areas and the basic, crucial components of digital forensic investigation processes can be identified from all proposed investigation models.

Examples of previous digital forensics investigation process models are presented in Table 2.5. Seven sample investigative process models were chosen for detailed study and the common investigative process has been highlighted with bold border with bold font. From this table, it is acknowledged that there are five common steps in digital forensics investigation, namely Step 1 – Preparation, Step 2- Data Collection, Step 3 – Data Analysis, Step 4- Findings presentation/Reporting and Step 5- Incident closure.

**Table 2.5: Previous Digital Forensics Investigation Models/Frameworks (Author) (Adapted and updated from Beebe & Clark, 2005, P.154)**

| Author / Processes | Palmer (2001) DFRWS model | Carrier & Spafford (2003) | Casey and Palmer (2004) | Beebe & Clark (2005) | Hershensohn (2005) | Kohn et al. (2006) | NIJ (2008) |
|---|---|---|---|---|---|---|---|
| Readiness | | ✓ | | | | | |
| Identification | ✓ | | | | | | |
| Deployment | | ✓ | | | | | |
| Incident alerts or accusation | | | ✓ | | | | |
| **Preparation** | | | | ✓ | ✓ | ✓ | |
| Assessment of worth | | | ✓ | | | | |
| Incident Response | | | ✓ | ✓ | | | |
| Incident/crime scene protocols | | | ✓ | | | | |
| Recovery | | | ✓ | | | | |
| Harvesting | | | ✓ | | | | |
| Reduction | | | ✓ | | | | |
| Documentation | | ✓ | | | | | |
| Survey | | ✓ | | | | | |
| **Data Collection** | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| Preservation | ✓ | ✓ | ✓ | | | | |
| **Data Analysis** | ✓ | | ✓ | ✓ | ✓ | | ✓ |
| Organisation and search | | | ✓ | | | | |
| Authentication | | | | | ✓ | | |
| Examination | ✓ | | | | | | ✓ |
| Reconstruction | | ✓ | | | | | |
| **Findings presentation / Reporting** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Persuasion and testimony | | | ✓ | | | | |
| Preview | | ✓ | | | | | |
| Decision | ✓ | | | | | | |
| Incident closure | | | | ✓ | | | |
| **Number of Phases** | **7** | **9** | **12** | **6** | **5** | **3** | **4** |

This findings are very similar with Selamat, Yusof, & Sahib (2008)'s result. They have identified existing investigation frameworks and merged the same activities or processes that provide the same result into following 5 common phases:

**Table 2.6: Summarisation of the output mapping (Selamat, Yusof, & Sahib, 2008)**

| Phase | Phase Name | Output |
|---|---|---|
| Phase 1 | Preparation | Plan, Authorization, Warrant, Notification, Confirmation |
| Phase 2 | Collection and Preservation | Crime type, Potential Evidence Sources, Media, Devices, Event |
| Phase 3 | Examination and Analysis | Log Files, File, Events log, Data, Information |
| Phase 4 | Presentation and Reporting | Evidence, Report |
| Phase 5 | Disseminating the case | Evidence Explanation, New Policies, New Investigation Procedures, Evidence Disposed, Investigation Closed |

There are number of different process models and frameworks and it seems there are no standard procedures in digital forensics investigation area. However it was interest to compare different process models and find some relationships in the different process model proposed to achieve the same end results. It is generally acknowledged that process does not really matter whether as long as we follow the basic, inherent process to digital forensics (Sansurooah, 2006).

It is clear that much additional work will be required in order to have standard digital forensics investigative process and standardisation in investigation process will help to conduct effective investigation.

## 2.3 TOOLS

Technologies make our life easier, less complicated, and provide tools to improve our effectiveness. Technology matters in digital forensics area as well. Technology contributed hugely in investigation process by providing useful tools, which are used to assist the forensic investigation including the identification, examination to the analysis of digital evidence with rapid changing technologies. Tools enable forensic

investigators to examine evidence more effectively and in a forensically sound manner. Early digital forensic examinations were conducted investigation on the digital device itself in order to obtain data and every file on the storage media has to be examined along with the entire digital media. Although there were some basic tools like dd (the oldest imaging tool used in digital forensics), which existed in the 1980s, it was still in its infancy stage and these tools were not widely used. The existing techniques and tools used in digital forensics may result in neglect in finding evidence and process cannot be forensically sound as accessing suspect's digital device can alter the evidence. However, digital investigation without proper tool is no longer practical as systems have become more complicated and hard drive capacity on our computers and portable devices are growing geometrically (Pollitt, 2008).

Pollitt (2008) stated that digital forensic examiners are now performing targeted examinations using the tools, searching evidence by selecting specific files that they are looking for and ignore irrelevant files or types of evidence and contents in order to perform examination effectively.

According to Casey (2004), digital forensic tools have been developed since 1990s. For example, tools like SafeBack and DIBS were introduced as digital forensic tools that can extract data without altering the evidence from the source media. Since then, many companies and government departments offered a variety of tools, some even offered complete forensic tool packages. Data extraction has expanded to both hardware and software extraction tools and capability of these tools provide better performance and easy of use for the examiners. Later stage, more advanced tools such as FTK and EnCase software has been developed and assists digital forensic examiners to perform their job much effectively. These two tools are proven software tools that can be trusted by most countries court and from law enforcement agencies. Apart from these commercial tools, open source forensic tools were also being written and provided to the public users.

The user interface of the forensic investigation tools have been improved significantly. It used to be based on a command line based interface but most tools now provide graphical user interface (GUI) and provide user-friendly versions.

### 2.3.1 Selection of leading digital forensic tools

Table 2.7 provides selection of market leading digital forensic tools, which have been developed so far. The purpose of the Table 2.7 is to understand the trends in development of digital forensics tools. This table will not only help to categorise forensic tools for different use, but also gives better understanding of each tool's capability and purpose.

**Table 2.7: Selection of market leading Digital Forensic Tools**

| Product Name | Purpose / Capability | Category | |
|---|---|---|---|
| | | Platform | License |
| **Computer Forensic tools** | | | |
| DD | The oldest imaging tool. It provides basic low level copying and conversion of raw image files. | Windows, Linux, Mac OS | Open Source (GNU) |
| SafeBack | Digital media collection and create bit by bit backup | Windows (DOS) | Commercial |
| Encase ® Forensic | Encase software is one of the most trusted and widely used tool in digital forensics. Can be used data acquisition, email and internet investigation. | Windows | Commercial |
| Forensic Tool Kit (FTK®) | FTK is also well known forensic tool, which is used by government agencies and law enforcement around the world. (AccessData, 2011) | Windows | Commercial |
| DFF | Digital Forensics Framework (DFF) is open source digital forensic investigation tools and development platform | Windows/Linux, MacOS | Open Source (GPL) |
| SIFT Workstation 2 | SANS Investigation Forensic Toolkit – VMware application that allows examine raw disks and evidence format. | Windows, Linux, Mac OS | Open Source (GPL) |
| Helix3 Pro | Provides incident response and computer forensic tools. Allows to make forensic images of all internal devices and physical memory (e-fense, 2011) | Linux (Live CD) | Commercial |
| BackTrack | Linux based penetration testing tool developed for security professionals. | Linux (Live CD) | Open Source (GPL) |
| The Sleuth Kit | C library and is collection of command line digital investigation tools. | Linux, OS X, Unix | Open Source (GPL) |
| UltraBlock | UltraBlock is a hardware based write blocker that allows a disk drive to be connected to a personal computer for forensic image acquisition and analysis. (Intelligence, 2006) | N/A | Commercial |

| **Mobile Device Forensic tools** | | | |
|---|---|---|---|
| Paraben | Provides digital forensics solutions for portable devices such as mobile phone or PDAs. Also supports hard drive and network evidence acquisition. | Windows | Commercial |
| Oxygen forensic suite | Mobile forensic software that goes beyond standard logical analysis of cell phones, smartphones and PDAs. | Windows | Commercial |
| Cellebrite | Provides extraction and analysis of invaluable evidentiary data from mobile devices. | Windows | Commercial |
| XRY | XRY is a complete digital forensics system for mobile devices that can be used on any Windows PC. XRY can recover data from thousands of different mobiles including deleted information. (Micro Systemation XRY, 2011) | Windows | Commercial |
| **Internet/Network/Social networking site forensic tools** | | | |
| Internet Evidence Finder | IEF is a software application that can search a hard drive or files for Internet related artifacts. It is a data recovery tool that is geared towards digital forensics examiners (JAD Software, 2011a) | Windows | Commercial |
| CacheBack | Internet cache and history analysis + social networking sites analysis | Windows | Commercial |
| Wireshark | Wireshark is a network protocol analyser, which allows capturing and interactively browsing the traffic running on a computer network and some of its network packet capturing capability can be used for digital forensics investigation. (Wireshark, 2011) | Windows, Linux, Max OS | Open Source (GPL) |
| TcpDump | Command line based network packet analyser. Allows digital forensic investigator to intercept TCP/IP and other packet transfer information. | Windows, Linux, Max OS | Open Source (GPL) |

Digital forensic tools must be reliable and relevant in order to make evidence legally admissible in the court. With the rapid growth of technologies, crimes using these technologies have been increased significantly. This is resulting many companies producing digital forensic tools in order to respond with those computer crimes or crimes using any of digital technologies. It is great to see the number of digital tools have been developed for forensic investigators. These tools will not only help digital

forensic examiners to effectively perform their investigation, but also help law enforcement agents and court for their decision making process by providing accurate and relevant digital evidence that has been committed using digital media. In the following section, tools, which can be used for social networking site investigation will be evaluated and most effective tools for this purpose of study will be identified.

## 2.4 EVALUATION OF TOOLS FOR SOCIAL NETWORKING SITES

Digital forensics investigations require a vast knowledge of software and hardware in order to perform an effective investigation. Knowing the right tools for different investigation scenarios will not only save time but also helps to avoid unnecessary steps, and avoid inadvertent alteration of evidence. Investigators do not therefore, need to go back and re examine the evidence several times. The tools can help investigators easily identify where to look, what to look for, and how to look for the required evidence in a forensically sound manner. These aspects of forensic tools play an important role in the digital forensic environment, as the tools will immensely enhance the forensic investigation process.

This section will evaluate different tools that can be used in forensic investigations of social networking sites. Social networking site investigation can be very useful and as the sites contain valuable, time stamped data and locations which can be used for finding relationships with crime or find actual suspects. Thus, when social networking sites are involved in a crime or other incidents, it is important for forensic examiners to know which tools can be used for their investigation process in order to retrieve relevant information effectively and accurately. The following section will describe an overview of selected social network forensics software and provides information about their capabilities and limitations. In the section that follows, a brief introduction to these different digital forensic tools is provided.

### 2.4.1 EnCase Forensics

Encase Forensics software is a commercial tool developed by Guidance Software and it is one of the most popular digital forensics application used in the industry (Casey, 2002). According to the vendor's promotional literature, EnCase is "the industry-standard computer investigation solution for forensic practitioners who need to conduct efficient, forensically sound data collection and investigations using a

repeatable and defensible process. The proven, powerful, and trusted EnCase Forensic solution, lets examiners acquire data from a wide variety of devices, unearth potential evidence with disk level forensic analysis, and craft comprehensive reports on their findings, all while maintaining the integrity of their evidence"(Guidance Software, 2011).

The EnCase forensics platform is illustrated in Figure 1 below.

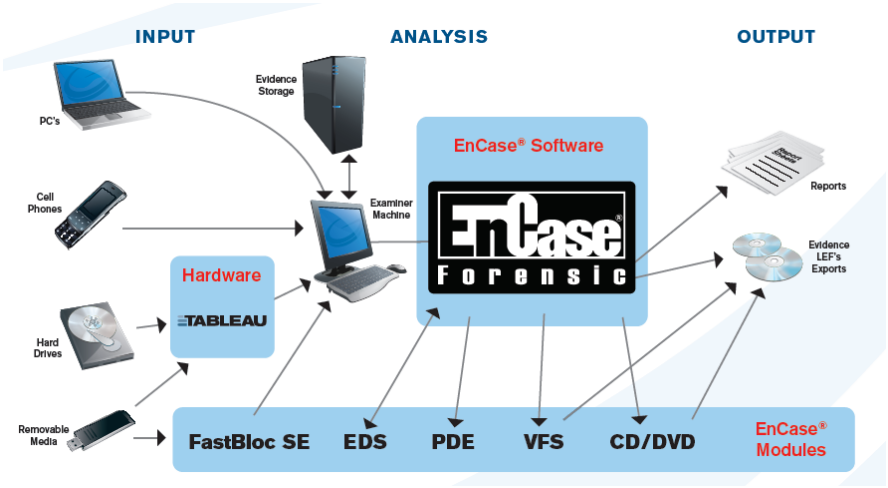



**Figure 2.3: EnCase Forensics Platform**

Source: EnCase Forensic for Law Enforcement (2011)
http://www.guidancesoftware.com/WorkArea/linkit.aspx?LinkIdentifier=ID&ItemID=674

EnCase forensic can be used to find evidence from different operation systems such as, Windows, Linux and Mac OS X (Cheng et al., 2009).

Encase Forensic's feature includes:

**Acquire from almost anywhere** – including RAM, images, email, internet artifacts, Web history and cache, HTML page reconstruction, chat sessions, compressed files, backup file.

**Acquire evidence in a forensically sound manner** – produce an exact binary duplicate of the original media.

**Advance analysis** tool.

**Provides programming capabilities** to forensic examiners, allowing users create to custom programs to help them automate time-consuming investigative tasks.

**Provides an automated reporting** tool.

(Adopted from Guidance Software, 2011)

### 2.4.2 CacheBack 3

CacheBack software will be used to rebuild cached web pages and examine Internet histories and activities from the social networking sites (such as Facebook chat).

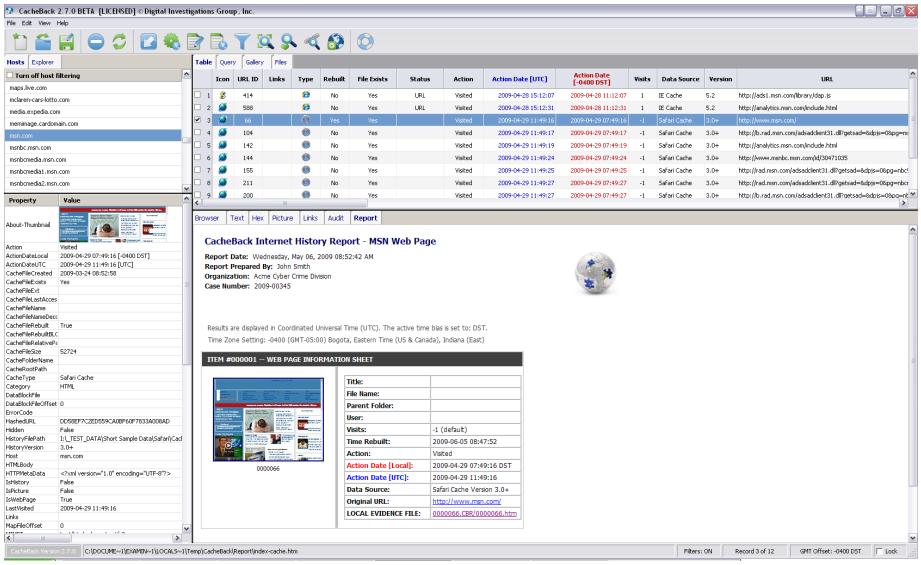



**Figure 2.4: Sample screenshot of CacheBack Internet forensic tool**

According to Cacheback, Cacheback is the only Internet forensic tool on the market today that supports all five top browsers (IE, Firefox, Google Chrome, Opera and Safari). They further claims that Cacheback is the preferred Net analysis tool for forensic investigations. It is also the leading finder of Internet evidence and related artifacts that consolidates everything into a single, comprehensive user interface (CacheBack, 2011).

### 2.4.3 Internet Evidence Finder

This application can search hard drives or files for artifacts generated in an online space and, like the Encase tool, it has been specifically designed for digital forensics examiners. However, its design is also straightforward and intuitive to use, making training requirements minimal (JAD Software, 2011a). According to the vendor's promotional literature, "IEF v4 searches the selected drive, folder (and sub-folders, optionally), or file (memory dumps, pagefile.sys, hiberfil.sys) for Internet artifacts. A case folder is created containing the recovered artifacts and the results are viewed through the IEF v4 Report Viewer where reports can be created and data exported to various formats" (JAD Software, 2011a, para. 3). A sample screenshot from JADSoftware's Internet Evidence Finder application is shown in Figure 2 below.

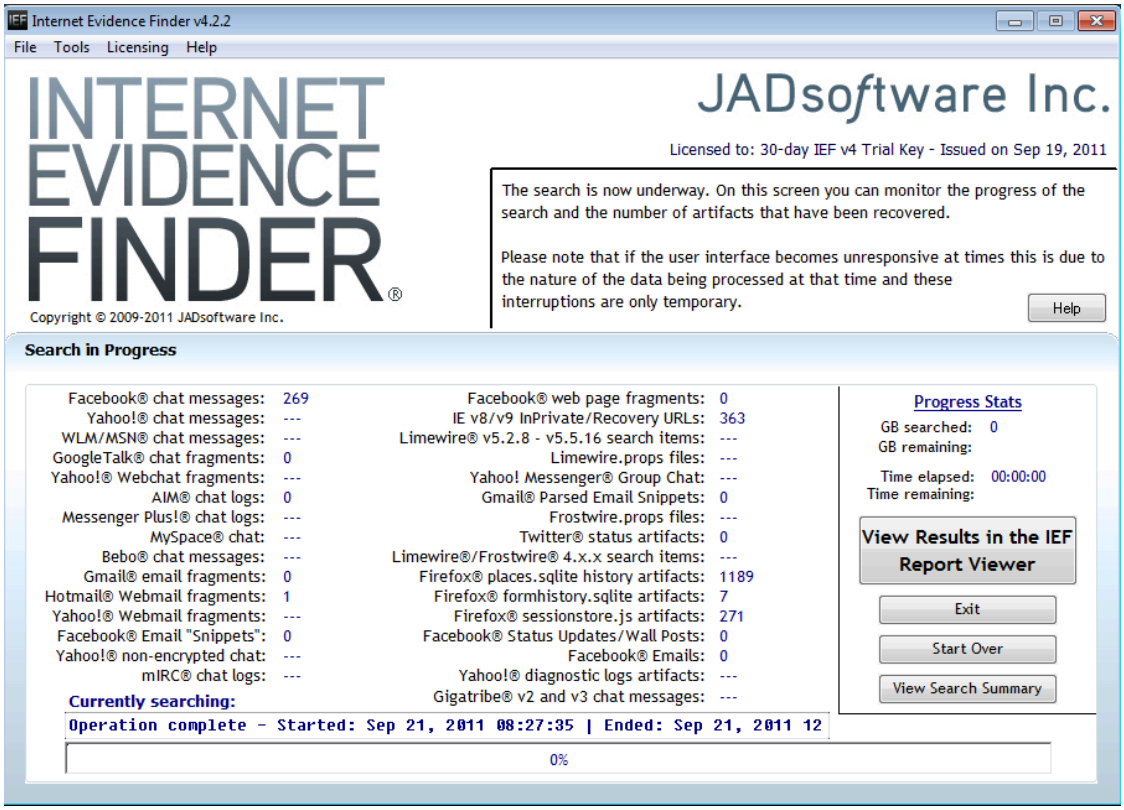



**Figure 2.5: Sample screenshot of Internet Evidence Finder Interface**

Source: JAD Software at:
http://www.jadsoftware.com/go/wp-content/themes/jadsoftv2/images/iefv4-1.png

Moreover, IEF v4 also has some useful features for social networking site applications, including:

**Facebook live chat search** to find even more chat, including damaged fragments (Messages sent and received using the Facebook live chat feature. Information found with the message can include the Facebook profile ID used to send/receive the message, the from/to names and ID's, and the date/time (in UTC) that the message was sent. However, there are a few different formats of Facebook chat and not all formats include all this data).

**Converting Facebook Unicode text.**

**Updated MSN/Windows Live Messenger search** re-written to find more chat faster.

**Facebook page fragments:** Facebook related web pages, including but not limited to the Inbox page, emails, photo galleries, groups, and so on. Most recovered items will be fragments and not the complete page, but attempts are

made to recover the entire page and filter out false positives. A header is added to the fragment to aid in viewing the page in its original format.

**New Portable Edition** that can run on live systems.

**Yahoo Messenger existing log files** are now parsed without requiring usernames.

**Yahoo! Messenger chat log validation** has been improved, with support for date ranges and message text filtering (JAD Software, 2011a, para. 2-3).

In this section, three digital forensics tools were evaluated with respect to their capabilities and effectiveness within the social network site investigation process. These three tool were chosen for illustrative purposes and because of relevance to with social network forensic investigation. This section shows information for each tool for digital forensic investigators to make informed choices about acquiring and using forensics tools for cases that are related to social networking sites. Applications like EnCase will be needed in order to find information about deleted files, restore slack space or unallocated space and files that are hidden or password protected. In addition to the EnCase application, CacheBack 3 or Internet Evidence finder will be useful to perform investigation that are specifically related social networking site, such as Facebook chatting history, web browsing history and other internet browser related digital forensic investigations. As these tools are available individually with specific features, it would be useful for the investigators to have a guideline and tools matrix, which can inform what tools to use in the each investigation process.

## 2.5 ETHICAL CONCERNS

Recently, directly or indirectly, a surge in computer-related crime and the reality of this phenomenon has become a great concern in our society. This phenomenon has impacted on normal investigation process and the new term “Digital Forensics” has gathering more weight in court cases because of this. Due to the advent of computer crime, digital forensics as a means of crime prevention has become a useful technology. In addition, digital forensics is a preferred technology as evidence in courts of law. Therefore, it is very important that in the course of investigating crimes, there is a digital forensics expert to present scientific evidence with a systematic procedure that is legally proven and scientifically sound.

However, there are at present very few ethical standards for digital forensics experts. Although the Crimes Act 1961 and Evidence Act 2006 do exist for the law, the law does not provide ethical guidelines. The principal problem is that with the existing Crimes Act or Evidence Act, they deal with only legal concerns. They do not deal with the professional ethical issues in digital forensics. This section explores ethical issues and dilemmas in digital forensics and will look at some ethical issues that are related to social network forensics in particular.

### 2.5.1 Ethical issues and dilemmas in digital forensics

What is an ethical issue? According to the Oxford paperback dictionary (1999), ethical means "morally correct, honourable" (1999, p. 264). The idea of ethical practice has been emphasised in computer industries and the discovery of ethical issues in computer science have become commonplace. While the idea of those ethical standards deals with common users who are using computer systems, the idea of ethical practice in digital forensics is targeted at people who are investigating evidence from those users, in order to make proper investigation. Due to the nature of the work, these experts have to deal with many unethical end user practices, and need to keep to the highest standards of transparency and professionalism during the forensic investigation life cycle.

An investigation report from a digital forensics expert has become crucial and the preferred information source used in legal proceedings. As it is very sensitive material, the digital forensic expert can sometimes supersede the interest of their clients in favour of committing some unethical behaviour, or even taking illegal actions such as perjury. Ethics in digital forensics is not only important for finding the true evidence in computers, networks and digital storage media, but has a responsibility to the public to provide and raise the level of digital forensic awareness in the field of information assurance.

There are many ethical dilemmas in digital forensic investigation. It is because the law is slower to change than technology, and our perception of some meanings changes with the time. For example, the meaning of objectionable in one generation may be different from what is objectionable in few years' time (Cox, 2006). Due to the nature of digital forensic investigation, there are a number of ethical dilemmas in this

field. According to Irons (2007) common ethical dilemmas in digital forensics include: integrity, completeness of an investigation, potential corruption or contamination of digital evidence, ignoring or changing evidence, not following the standard procedure, bribery, and working with emotional involvement in their cases (Irons, 2007). When it comes to a situations like truth vs loyalty, individual vs community, short term vs long term or justice vs mercy, digital forensics expert will be faced with ethical dilemmas, and yet there is no standard guidelines to resolve this ethical dilemmas (McDonald & Pak, 1996). It would be necessary to draw up a suitable international standard code of ethics for digital forensic investigation and interaction with relevant areas of law and professional code of ethics will greatly contribute to our society in clarifying the substantive truth, which can also minimise grey areas in digital forensics.

### 2.5.2 Ethical concerns in social network forensics

Since Social networking sites have gained huge popularity, SNSs have altered the way people communicate (Lewis, Kaufman, Gonzalez, Wimmer, & Christakis, 2008). The purpose of social networking sites is to volunteer information to communicate, and this voluntarily posted information can be sometimes very private and viewable to only particular groups or friends who has been allowed to see. These postings or chatting history from SNSs contain useful information in the range of legal investigation, discovery and litigation. Activities on SNSs are recorded online and this recorded information contains personal behaviour, location and some private information, which can be tracked down during digital forensics investigation. This can have serious consequences and therefore, raises a number of concerns about the ethical aspects of social network forensics. In order to have effective investigation of SNSs, there are some ethical issues that need attention.

Particular ethical issues with social network forensics will be introduced in the next section and some common dilemmas and challenges that are associated with social network forensics will be highlighted.

#### 2.5.2.1 Privacy issues

Many social networking sites allow users to list personal details such as full name, date of birth, contact numbers and home address in their profile. Even though users have control to limit their connections and make this profile visible only to certain

people, such private information can be collected and viewed by digital forensic investigators during the investigation process.

Bassett, Bass and O'Brien (2006) argue that "the most common ethical problem is managing the discovery of confidential data that is irrelevant to the case at hand" (p. 25). They continue with examples where an investigator finds incriminating evidence of adultery or some other sort of inappropriate material that is not relevant to the case. They emphasise that the forensic expert must deal with this situation and need to ignore this kind of data as they are not relevant to the investigation (Bassett et al., 2006).

In the process of social networking site investigation, it is possible that investigators will be able to see private information that is not related to the particular case they are investigating. Sometimes, this private information cannot be retained in order to be produced as evidence in a court of law to prove a crime. It is therefore digital forensic investigators who must keep in mind that such private information should be remain confidential and not to be available other people while they are performing the investigation.

#### 2.5.2.2 Fairness, honesty, data integrity issue

Admitting mistake is one of the ethical practices for a forensic investigator. However, people normally find it very hard to admitting their errors especially when they believe they are already a professional in that area (CyberSecurity-Institute, 2004). Bassett, Bass and O'Brien (2006) also expressed a similar view that "Many Computer Forensic Specialists find it hard to admit these mistakes because one major screw up could lead to immediate unemployment" (Bassett et al., 2006).

Since the increase of users in SNSs and this phenomenon resulted in an increase number of crimes, forensic investigator need to learn new tools and new investigative processes in order to conduct forensically sound investigation of SNSs. Because this is still new area in the digital forensics field, digital investigators face a with lack of standardization (Norulzahrah M. Zainudin, 2010).

Sometimes, forensic investigators need to work under huge time constraint pressures, to satisfy customers and keep their reputation in the forensic industry. This may result in them not checking evidence files thoroughly enough or sometimes submitting the investigation report without completion of proper analysis work. As

this is a new emerging field in the digital forensics, they may need some additional tools or software to collect evidence from SNSs. Forensic investigators might not have enough budget to purchase more software for this particular investigation and they might use existing tools that are designed for general computer storage forensics processes.

Currently there are not many software packages that are specifically designed for SNSs investigation and lack of standardizations in this area can create a lot of ethical issues such as dishonesty, unfairness, or an unethical investigation. Those issues can result in serious problems, as the evidence becomes the main source of judgment in the courtroom.

#### 2.5.2.3 Qualifications

A forensic expert needs to declare their qualifications and experience in the brief. There are many real cases in where fraudulently misrepresented their qualification. A case was found from a UK technology news website that a forensic expert Jim Bates who gave a false witness statement to the court has been given a six month suspended sentence for perjury (Blincoe, 2008). Further to this, the judge commented that Bate's career life as a forensic expert was finished. This case demonstrated how important it is to keep the professional ethics in digital forensics area. Due to the serious nature of digital forensics work, it is expected and required that expert witnesses should have an appropriate qualification and membership of a professional association. As digital forensics is in its beginning stage, not many people have the relevant qualifications or certifications as of yet, particularly in the SNSs forensics field.

Even though some vendors provide trainings and certification courses for SNSs investigative tools, it is quite important to maintain knowledge and skills in these areas as features and functionality of SNSs change rapidly. If they are not keep themselves up to dated with new technologies, their qualifications and skills will soon be obsolete and therefore, they will have difficulties in collecting and analysing evidence that came from the cutting edge technologies. In this regard, it is an important part of ethical issues for digital forensic investigators. Keeping themselves up-to-dated with new technologies and knowing what they are investigating and how evidence should be collected and presented in the court is an important part of professional ethics for all digital forensics experts.

#### 2.5.2.4 Other ethical issues

Above section introduced some professional ethical issues for forensic experts in particular. However, ethical issues for companies who are creating forensic software should not be overlooked. When they are developing software for SNSs investigation, they might be neglect to consider ethics, such a protection of privacy.

The role of ethics in software development has increased in importance recently. Thomson & Schomoldt (2001) stated that: "Computer software systems lie at the heart of modern decision making, including data/information storage and manipulation, data availability, and 'alternatives' formulation and selection." They further stressed that all software systems need to be critically examined as they are developed and deployed because software development can have impact on people and their cultural, corporate and other intuitions (Thomson & Schmoldt, 2001).

Mason (1986) also identified earlier with four ethical issues with software development. He categorised ethical concerns into privacy, accuracy, property, and accessibility concerns (Mason, 1986).

It is very important for software developers to create and update software that complies with ethical standards as wrong software and inaccurate analysis report from that software may cause a number of serious problems.

## 2.6 SUMMARY OF ISSUES AND PROBLEMS

Literature shows that the concept of Social Network Forensics in the digital forensic area has developed rapidly in the past few years, and there are a lot of concerns and problems that are associated with social network forensics. There is no accepted model of professional standards or standardised tools that the investigator can use in this area.

It is important to explore the implications of social network and develop standard tools and guidelines for SNS investigation. Although some software companies like Guidance Software provides EnCE certification programme for digital forensics, and provide some social network forensics investigation features, there is no central body or disciplinary board which can be used as a role model for the SNS investigation process. Having a solid guideline and tools that forensic investigators can follow will be great value for our society. Looking at the ethical implications and dilemmas in digital forensics area and the challenges, issues and opportunities that

digital forensics experts are facing, it is too important to rely ethical issues to each individual forensic expert.

Technologies change all the time, and tools, which can help forensic experts to do their job, will also have rapid development. While it is positive news that technologies will help forensic experts to do the better job, digital forensic experts also need to develop their skills and keep the professional ethics and knowledge as a parallel with rapid changing technologies in order to maintain themselves as a professional digital forensic expert.

Apart from ethical issues, there are many other challenges remaining in digital forensics investigations in social network environments. The following section will summarises some problems and issues associated with Social network forensics:

### 2.6.1 Problem 1: Admissibility of evidence

Identifying the communication post originator, and locating potential evidence from SNSs is very difficult due to the social network's distributed network. It is also hard to find everything on SNSs, as evidence may be stored on multiple SNSs. Finding completely accurate evidence can be problematic and the risk of missing data is more common in social network forensics.

### 2.6.2 Problem 2: Interpretation/Perception from investigator

Social network analysis will give investigators different viewpoints, different clues of what to look at, how to look at it, and how it is related to others within social network. It is common for people to interpret different things from a social network. Investigators may interpret evidence and present evidence from different viewpoints, and they may presume that the information they found from social networking sites is related to criminal activities.

### 2.6.3 Problem 3: Jurisdictional differences

As social networking is happening in cyberspace, the person who committed a crime through on SNSs may be located in a different country to that of the victim. The Digital Forensic Investigator will find difficulties if evidence is posted from different jurisdictional area.

### 2.6.4 Problem 4: Social Network Forensic Tools

Several digital forensics and network forensics tools have been developed to collect potential evidence from the digital medium. However, collecting evidence from SNSs remains one of the most challenging problems in social network forensics. As described in the Section 2.4, each tool is available individually and there are not many software suites that are specifically designed for social network forensics.

Adequately preserving evidence from SNSs is the most crucial part of the investigation process, which can be challenging given characteristics of social networking sites. There are no all-in-one standard tools that forensic investigators can follow. In order to properly collect and analyse evidence from SNSs, it is necessary to have tools developed for social network forensic investigation, so that forensic investigator can collect and provide relevant evidence, which is admissible to the court of law.

### 2.6.5 Problem 5: Lack of Standards

According to the Oxford dictionary, standard means something used as a measure, norm, or model in comparative evaluations (Dictionary, 1999). The idea of having a standard is to set up a protocol that everyone understands and can follow. With the explosion of digital crime, digital forensics is more and more relevant. The digital forensic discipline has developed rather rapidly, but to date, very little international standardisation with regards to procedures or management has been developed.

Moses Hadas once said "The larger and more indiscriminate the audience, the greater the need to safeguard and purify the standard." It is necessary to draw up a suitable international standard code of ethics with proper tools for social network forensics investigation. It is also necessary to standardise interaction with relevant areas of law, and professional code of ethics will greatly contribute to our society in clarifying the substantive truth, which can also minimise problems and issues in social network forensics.

## 2.7 CONCLUSION

A careful analysis of obtainable literature that is related to Social Network Forensics has been made in the literature review chapter. The literature review conducted in Chapter 2 provides an overview of the current state of knowledge and trend of Social Networks. It is noted that social network is represented in a variety of forms, and the most popular way is via social networking sites, mobile phones, and content sharing sites such as blogs. It is clear that social network provides opportunities for proving or disproving alibis. It also can be an instrument of crime or a target of crime.

As shown in the section 2.1 of the literature review, statistics indicates a massive uptake of social network usage, and this has resulted in changing the digital landscape immensely. Differences between digital forensics, network forensics and most importantly social network forensics have been discussed. Section 2.2.1 and 2.2.2 introduced the key elements of the digital forensics process, so that Social Network Forensic investigators can learn disciplines from digital forensics. While the Social Network investigation process has many similarities with the digital forensics investigation process, there are some aspects of social networking that make Social Network Forensics much difficult than other aspects of digital forensics. Literature indicates that Social networks will form a major part of the future digital landscape.

Investigation of social network data can be extremely complex, and provides online evidence that is different from the conventionally accepted evidence. Digital forensic investigators and law enforcement professionals can start to look into a disciplined approach for effective ways to bring data from SNSs into investigations. Even though social network investigators can apply and learn much from digital forensics disciplines, investigation requires different tools and techniques for social network forensics to ensure the investigation process is effective and forensically sound. It is clear that digital landscape is changing dramatically and forensic investigators need new tools and techniques to accommodate these changes. Section 2.3 and 2.4 introduced digital forensic tools and tools that are designed specifically for social networking sites investigation. Three of the sample applications were chosen for detailed study, which simulated each tool's capability. There was an expectation that standard tools for Social Network Forensic investigation will be found from

literature review. However, there was insufficient information that indicates standard tools or guidelines for Social Network Forensics.

As Social Networking sites are growing in popularity and functionality, continuous work will be required in order to provide standard tools that can be used in Social Network Forensics. It is proposed that this research will focus on comparison of tools and techniques that can be used in Social Network Forensics. Chapter 3 will firstly undertake a review of similar approaches relevant to Social Network Forensics in order to gain methodology knowledge and to identify available tools at the time of this study. The limitations of the derived methodology are also to be discussed.

# Chapter Three

# RESEARCH METHODOLOGY

## 3.0 INTRODUCTION

The literature review conducted in Chapter 2 provides information about Social Network Forensics and identified the importance of applications that can collect evidence from Social Networking Sites (SNSs) in a forensically sound manner. While data from SNSs provide compelling source of evidence, the literature also highlighted characteristics of SNS evidence and a number of issues that surround the topic of performing digital forensic investigation from SNSs. There is a lack of standard tools for acquisition and preservation of SNS evidence and selecting the most suitable tools for capturing SNS evidence trial a valuable contribution to knowledge.

In Chapter 3, the objectives are to formulate research questions and to develop an appropriate research method for the proposed research. The approach to be used by the proposed study in identifying the most effective tool for SNS forensics will be tested and analysed by using three chosen forensic tools from the literature review. Namely - EnCase, Internet Evidence Finder and Cacheback software.

A number of similar approaches in the chosen research field will be reviewed and evaluated in Section 3.1 in order to develop research methodology and to learn from other researchers in the same domain of study. Section 3.1 will provide information about how people approached the Social Network Forensics investigation process. The research question for this study and hypothesis derived from Section 2.6 will be discussed in section 3.2. In section 3.3 the proposed research design is discussed in detail to show how the research question and sub-questions will be answered. The data requirements in Section 3.4 will highlight the preparation, collection, analysis, presentation and incident closure methods required to conduct the research. Expected outcomes from this research will be discussed in Section 3.5 and any limitations of the research will be identified and discussed in Section 3.6 followed by a conclusion.

## 3.1 REVIEW OF SIMILAR APPROACHES

Chapter 2 introduced a selected literature about digital forensics and the importance of social network forensics. The main focus in Chapter 3 is to discuss how to conduct research on the topic. A number of similar approaches in testing and evaluating tools for digital forensic investigation will be critically reviewed in order to develop a methodology for this research topic. Five independent research approaches to evaluate forensic investigation tools have been sourced and reviewed in order to develop the method for this research. The following research studies have been selected for relevance and similarity to the chosen research area, and the method or selection of tools for Social Network Forensics investigation.

The first approach, by the National Institute of Standards (NIST) (2001) examines the general approach for testing computer forensic tools and required procedures for the test method. The second approach, by Bryson and Stevens (2002) outlines the tool testing and analytical method for digital forensic investigation, and provides examiners with a handful of concepts that will assist in making a sound decision. The third approach by Wilsdon & Slay (2006) discusses the need for evaluation of forensic computing software and proposed an evaluation framework, while addressing the shortcomings of other similar frameworks and extending their capabilities. The six phases of the evaluation process are identified and described, to assist vendors and digital forensics investigators in undertaking the same testing process with their environment. The fourth approach by Guo & Slay (2010) proposes a detailed functionality orientated validation and verification framework of computer forensic tools. The final study by Jadhav & Sonar (2011) examines software evaluation criteria, evaluating, and comparing evaluation approaches with the widely used existing previous software evaluation techniques such as Analytical Hierarchy Process (AHP) and Weighted Scoring Method (WSM).

### 3.1.1 General approach for testing computer forensic tools from NIST

Due to the critical need in the law enforcement community to ensure reliability of digital forensic tools, the National Institute of Standards and Technology, an agency of the United States Department of Commerce, has proposed approaches to measure viability of computer forensic tools. This approach is based on International

Organization for Standardization/International Electro technical Commission (ISO/IEC 17025), 'General Requirements for the Competence of Testing and Calibration Laboratories', which is a well-recognised method for conformance testing and quality testing.

NIST has summarised the approach to testing computer forensic tools. Figure 3.1 illustrate the approach used as presented by NIST for testing computer forensic tools.

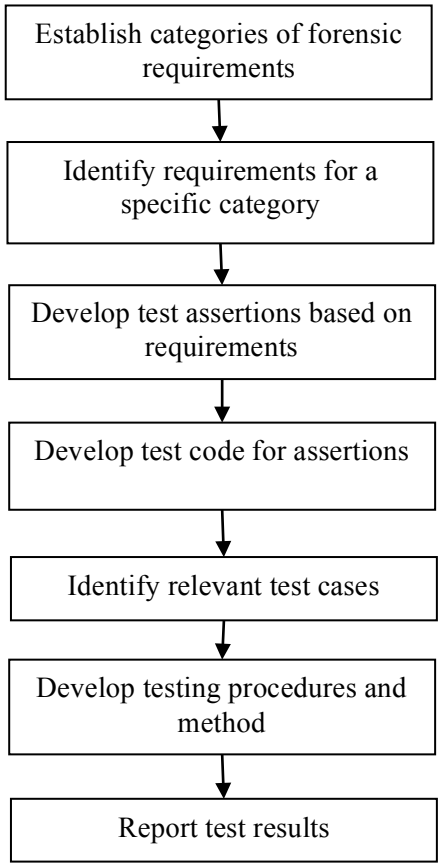



**Figure 3.1: General approach for testing computer forensic tools (NIST, 2001)**

The above approach provides law enforcement personnel with a means of deciding whether the tools in consideration for use should be applied for the purposes required. This approach from NIST has a direct link to the proposed research as this approach considers not only the accuracy and reliability of the software functionality but also considers existing international standards.

### 3.1.2 Tool testing and analytical methodology

Bryson & Stevens (2002) aim to provide examiners with a number of concepts that assist in making a sound, rational decision to select forensic tools, as opposed to emotional, reactive, or externally motivated factors. The concepts proposed in this study help examiners to identify the strengths and weaknesses of the tools. Although this research argues that forensic examiner's knowledge and the methods used are more important than the technical efficacy of the tools, the principles of the study can also be applied to Social Network Forensics.

"Computers may be running completely different operating systems and file systems in the future. Therefore, examiners should not become overly reliant on tools and must develop a solid understanding of the underlying technology and related forensic examination techniques" (Bryson & Stevens, 2002, p. 115). Bryson & Stevens statement is particularly significant, as tools will be updated in conjunction with the development of technologies. It is therefore crucial to check functionality and abilities of the tools in multiple operating systems, and with different case scenarios. The tool testing method adopted by Bryson & Stevens (2002) is shown in Figure 3.2.

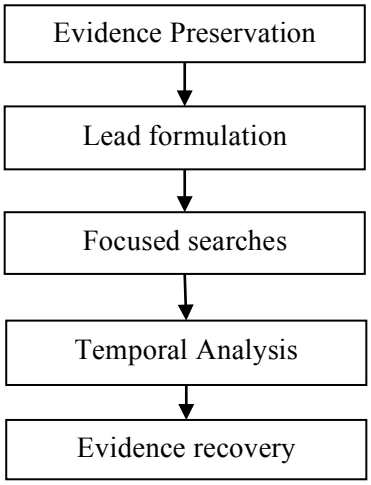



**Figure 3.2: Tool Testing and Analytical Methodology (Bryson & Stevens, 2002)**

Bryson & Stevens stated that above 5 steps are the basic set of requirements the examiner must meet. The examiner can meet these core requirements through a myriad of tools or techniques. The first step involves capturing a forensically sound binary image using MD5 checksum or other hash functions to ensure the integrity of evidence. The next step checks the acceptable search hits generated by tools in

different cases, as each tools has strengths and weaknesses. The third step involves specific information search, which evaluates the scalability of the tools. Bryson & Stevens argue that tools must have effective search facilities. Advanced search functionality is a crucial component of the forensic investigation process, as investigators now perform targeted examination by searching specific areas such as email conversation, Internet histories and online chatting logs (Pollitt, 2008). This is due to the complexity of operating systems, and increased storage capacities. So the 'focused search' capability must be evaluated to ensure the efficiency of the forensic tool. In the temporal analysis step, any tool must enable examiners to gather date and time information regarding the file, as well as deletion time of a given file or directory. After locating evidence from the above steps, the efficacy of recovering deleted files, as well as the collection of active files will be tested with multiple system types. According to the author's experience, file/data recovery tools were capable of working against multiple computer file system architecture such as FAT, VFAT, NTFS, EXT2, and UFS.

Bryson & Stevens (2006) stressed that software tools are a part of forensic process only, and the examiner need to be knowledgeable enough to go to a level far beyond that of a simple user with the same tools. Evaluating the tools capability with core forensics processes, this method can assist investigators in avoiding risk of loss of their credibility by using inappropriate tools.

### 3.1.3 Validation of Forensic Computing Software Utilizing Black Box Testing Techniques

Wildson & Slay (2006) developed a set of tests to validate forensic software and proposed an alternative testing framework, which is similar to both the NIST Computer Forensic Tool Testing (CFTT) programme and The Scientific Working Group on Digital Evidence (SWGDE)'s software evaluation framework. Wildson & Slay (2006) addressed the shortcomings of the current tool models testing framework from NIST and CFTT, and proposed a framework that is built based on the software testing standards of ISO 17025-2005 and IEEE 610.12-1990.

Wildson & Slay (2006) argue that the framework proposed in their research paper is more efficient with respect to time, output and financial requirements. They also discussed the important point at the outset: That there is no standard definition of

what a forensic computing tool is (p. 2), and stressed the need to examine tools in regular basis (p. 2). The importance of setting up goals prior to testing software is also discussed, and introduces four categories of starting point prior for conducting tests.

This research conducted by Wildson & Slay (2006) is concentrated on the accuracy and reliability of forensic computing tools and the authors proposed six stages of evaluating software applications. These help to determine whether to the tool performs correctly and accurately in the investigation process. The six stages of evaluation process in the research are illustrated in Figure 3.3.

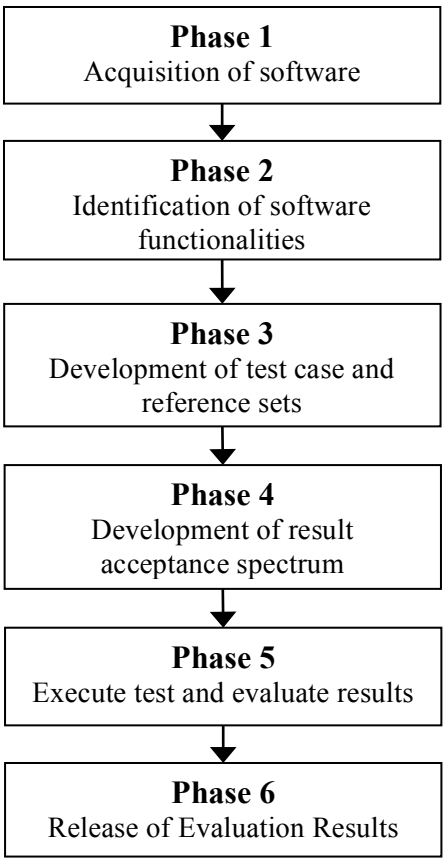



**Figure 3.3: The 6 process for evaluating software applications (Wilsdon & Slay, 2006)**

This evaluation approach begins with acquiring the relevant software applications to be evaluated. Using MD5 checksum or hash function generates a unique signature of the software and this process ensures software versions, firmware updates or modifications are not misinterpreted. Functions of software are identified from a variety of source of documentation provided by software vendors or online forums.

All functions must be clearly documented as an item to be tested. Documenting functionality is a crucial part of this phase, as it is an implicit requirement of the next phase of evaluation. When all requisite functions are identified and documented, test cases must be developed to ensure correct operation. Test cases are developed based on Black Box testing techniques. According to Wilsdon & Slay (2006), Black box testing techniques are well known, and determined to be an example of real world scenarios, which will put organised data into an image referred to as a reference set. The next phase relates to assessing the test results. In the development of the result acceptance spectrum, a method from ISO 14598.1-2000 is used to divide potential results into 4 groups; (1) Exceeds requirements, (2) Target range, (3) Minimally acceptable and (4) Unacceptable. Tests will be executed and documented according to ISO 17025-2005 and AS 4006-1992 requirements, and finally once the evaluation process is complete, making the test result available to the community. Releasing the evaluation result allows examiners or organizations to undertake the same testing process within their environments, and helps to gather input from numerous domains.

This testing approach developed by Wilsdon & Slay (2006) utilises Black Box testing techniques. This approach addresses shortcomings of existing framework proposed by NIST or SWDGE and extends the capabilities. The 6 phases of evaluating software applications validates the software utilised, as forensic computing tools. It's a streamlined process, with community input, and multiple environment testing makes the proposed approach more efficient.

### 3.1.4 Data recovery function testing for digital forensic tools

Guo & Slay (2010) propose a detailed functionality oriented validation and verification framework for computer forensic tools, which describes the background of the validation and verification of software within the field of digital forensics. Two existing approaches of validation and verification of tools are introduced. The first approach is the 'Tool Oriented' approach. This work has been conducted by vendors, with such a tool as 'Encase' from Guidance Software, and 'FTK' from Access Data. The second approach is a 'Functionality Oriented' approach conducted by NIST and CFTT. Guo et al pointed out that there are two potential issues with the existing work. Firstly, the existing work has a lack of operational focus, as it does not look at the

process of analysis as a whole. The second issue is that method proposed by NIST/CIFF and DFTT are broad and offer no conclusive detailed identification of what needs to be tested (Guo, Slay, & Beckett, 2009). Figure 3.4 presents the proposed validation and verification methodology.

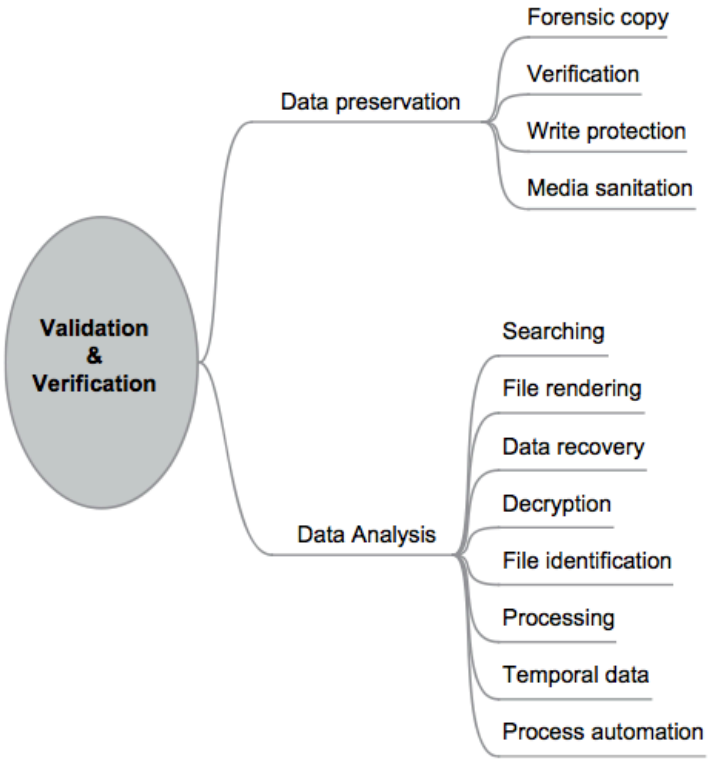



**Figure 3.4: Validation and verification top level mapping (Guo et al., 2009).**

Starting from a formal model and function mapping, digital forensics components and processes are defined in the model. Validation and verification of digital forensics tools is accomplished by specifying requirements for each mapped function. Once the discipline is mapped for each specification, the expected result is identified and mapped as a reference set, and tools are validated based on these reference sets.

This study attempts to complete the mapping of the functional categories of digital forensics that can be used as guidance for tool developer and educators as well as for tool validation or the verification process. Guo & Slay (2010) claim that this Function Oriented validation framework has several advantages such as detachability, extensibility, tool version neutrality, and transparency (p. 299).

### 3.1.5 Framework for evaluation and selection of the software packages

Jadhav & Sonar (2011) describes a generic method for software selection, software evaluation criteria, and a proposed hybrid knowledge based system (HKBS) approach, to assist decision makers in selecting appropriate software for their needs. Even though this evaluation framework is not specifically designed for evaluation of digital forensics tools, the concept of evaluating and selection of the software package can be applied for digital forensics tools. Jadhav & Sonar (2011) also compares the HKBS approach with the widely used software evaluation frameworks such as analytic hierarchy process (AHP) and weighted scoring method (WSM).

The Authors describe decision software selection decision making framework comprises with following 3 main categories: (1) Methodology for selection of the software packages, (2) Common criteria for evaluating software packages, and (3) the HKBS approach for evaluation software packages. The first category involves procedures and steps that can be followed in selecting software and there are 6 stages:

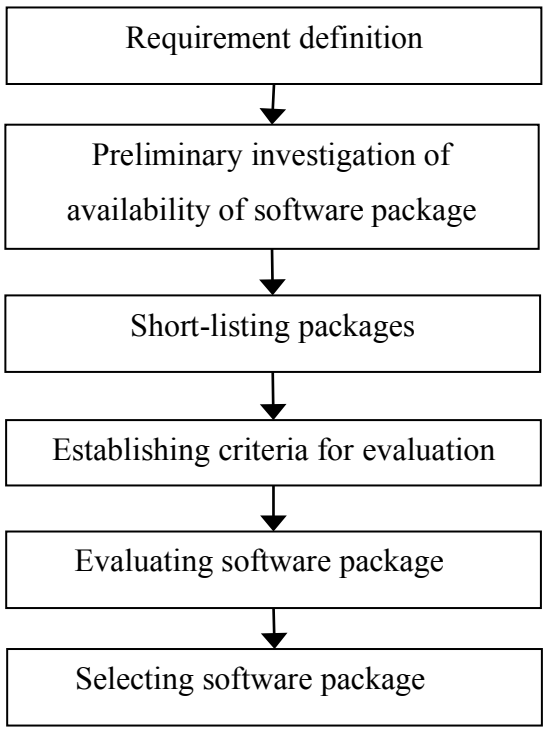



**Figure 3.5: A generic stage based methodology for selection of the software packages (Jadhav & Sonar, 2011)**

Second category provides general list of soft evaluation criteria that can be used for evaluation of any software package.

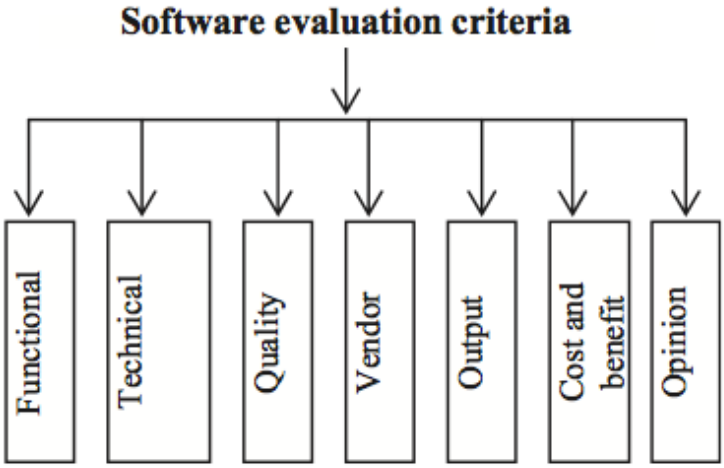



**Figure 3.6: Software evaluation criteria (Jadhav & Sonar, 2011)**

Finally, the HKBS approach for the software evaluation is introduced. The HKBS approach is based on case based reasoning techniques for selection of a software package. A detailed architecture of the evaluation and selection criteria is shown in Figure 3.7. It first divided by rule based and case based approaches for the evaluation process. The rule based expert component stores information about the software evaluation criteria and captures user needs for the software package. Once user needs of the software package are identified, these requirements are submitted to the Case Based Reasoning part of the HKBS approach. Case based reasoning techniques are then used for comparing user needs for the software, with the description of the packages, and ranks them based on how well each software package meets the user needs. A higher rank will be given to the software package that has greatest affinity to the user's requirement.

The HKBS approach presented in this paper can also be used as guidance for a digital forensics tools selection approach, as it helps to choose criteria for evaluation of the software package and to determine the effectiveness of forensic tools for examiners needs in any particular investigation.

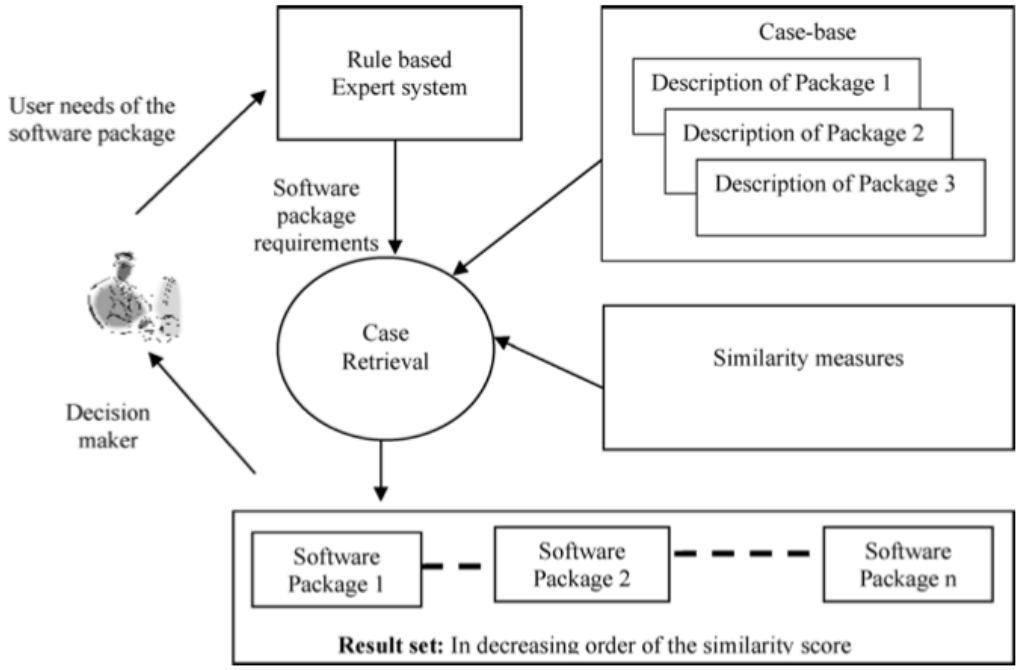



**Figure 3.7: HKBS approach for evaluation and selection of the software packages (Jadhav & Sonar, 2011)**

## 3.2 THE RESEARCH QUESTION AND HYPOTHESIS

The literature review in Chapter 2 provides a background of theoretical knowledge regarding the chosen research area of evidence collection and the method for acquiring evidence from both digital forensic investigation and social network environments. A diverse body of literature has been cited, ranging from social network forensics in general, usage trends, ethical issues and problems associated with Social Network Forensics. The literature about investigative processes and standardisations of digital forensic evidence was reviewed with the 'seven-sample' model for investigative process. Review of the investigative approach acknowledged that there are common elements in digital forensics investigations. Additionally, the preceding review of similar approaches (Section 3.1) has given various methods that can be used for selection of Social Network Forensic Tools evaluation.

The development of a research question was conducted based on the literature reviewed in Chapter 2, and the review of similar approaches in Section 3.1 has discovered a number of techniques to evaluate digital forensic tools. Conductive and

proactive frameworks for evaluating and testing tools were identified and existing digital forensic tools like EnCase, Internet Evidence Finder and CacheBack will be compared in order to determine an effective investigation process.

The mode of tool use in digital forensics investigation has involved many vendors for sometime. There were a lot of concerns about using tools. For example, tools might cause problems such as a blow out in running costs, investigators becoming dependent on particular tools, and the actual validity of the tools used in the gaining of forensic evidence. However, forensic examiners existed prior to the development of current technologies and often struggle to maintain currency with existing tools. Commercial vendors are racing to sell their products and keep producing new tools causing investigator confusion.

Combining all these concerns, this research will examine a number of computer forensic tools and relate their attributes and performance to a framework that has been discussed in Section 3.1. The research question underpinning this research asks if the existing digital forensic tools have enable forensic investigators to enhance investigative process, and what features there are each tools that can collect evidence from SNSs.

This research will explore evidence extraction tool capabilities by posing the following main research question:

> ***What are the capabilities of the 3 chosen tools to collect and analyse evidence from Social Networking Sites in a digital forensic investigation?***

As discussed in Section 3.1.2, poorly used or improperly functioning tools can cause a loss of credibility for forensic investigators. The main focus of this study is to examine (1) the accuracy and completeness of evidence collection from social networking sites (2) the generation of analysis reports, and (3) to check the ability to find probative artifacts from social networking sites by using the three chosen forensic tools.

In order to answer the main research question, associated sub-questions are formulated:

**Sub-Question 1:** What are the current tools' capabilities? (for both examiners and court of law)

**Sub-Question 2:** What are the hardware and software requirements for the successful acquisition of SNS data as digital evidence?

**Sub-Question 3:** What functionality is necessary for collecting evidence from SNSs?

**Sub-Question 4:** How can the selected tools be ranked in terms of accuracy and completeness of collected evidence?

**Sub-Question 5:** Which tool is the best for SNS investigation?

**Sub-Question 6:** What new function of tools might be useful in addressing the current concerns for examiners of Social Network Forensics?

The key findings from this research will be used to evaluate questions. With the analysed data, this paper will explore possibilities combine all the strengths of existing tools to maximise effectiveness of the Social Network Forensic investigation process. The result of the capability comparison of the chosen tools would then enable the investigator to evaluate whether the tool chosen meets the requirements demanded for their scenario, and to improve the efficiency of the investigation process. Answering above sub questions will indicate ways which those combined strengths from existing tools can be structured with right methodology and can satisfy both forensic examiners and thus the court of law.

A number of hypotheses have also been developed for each of the sub questions. The hypotheses have been devised in order to link with each sub question to inform the main research question.

**Hypothesis 1:** Given the fact the data exchange in question creates largely volatile data, survivability of data created during normal user interaction with SNSs is unknown. The chosen tools face difficulties in recovering the entire evidence from SNSs. Nevertheless, sufficient data can still be acquired to determine the likelihood of criminal activities, and the timelines and artifacts for legal proceedings. An inductively strong case for prosecution may result, even though hard evidence may be incomplete.

**Hypothesis 2:** That the hardware and software requirement for each chosen tool will vary and also varies on the data digital investigators have to analyse. Different requirement for hardware and software will impact on the investigation process and collection result. It is expected that tools will support a particular operating system, and will not be able to find evidence when collecting evidence from different testing platforms.

**Hypothesis 3:** EnCase will have much more functionality than other two selected forensic tools. However, it is expected that each tool have several core functionalities in common but distinct from the others. For example, Encase will have better acquisition functionality, and CacheBack will have better functionally in searching Internet Cache and Online Chatting histories.

**Hypothesis 4:** Tool evaluation approaches reviewed in Section 3.1 will inform clearly defined testing metrics for ranking each forensic tools in terms of it's functionality, accuracy and completeness.

**Hypothesis 5:** EnCase Forensics software will perform better than other two selected tools in the data acquisition process. CacheBack 3 and Internet Evidence Finder will perform better than EnCase in finding evidence from SNSs and presentation process.

**Hypothesis 6:** The fairness and lack of bias in the evidence collection process will be useful in addressing the current concerns of acquiring evidence from SNSs. A function that enables the examiner to check the investigation process with the 5 common steps of digital forensics investigation identified in Section 2.2.6 would be useful. Furthermore, the functionality of recording the processes themselves while conducting the investigation would be a plus as this can help investigator to make whole process repeatable.

In order to answer the above research questions, and validate the proposed hypotheses that are related to each sub question, a research flow chart was developed for guiding the main phases of evaluation for the three chosen forensic tools. Figure 3.8 presents the flow chart of the pre-evaluation phases. Figure 3.9 presents the flow chart outlining the main research question, sub-questions and the links to associated tool evaluation phases. The findings gathered from the research-testing phase will be checked against to the asserted hypotheses.

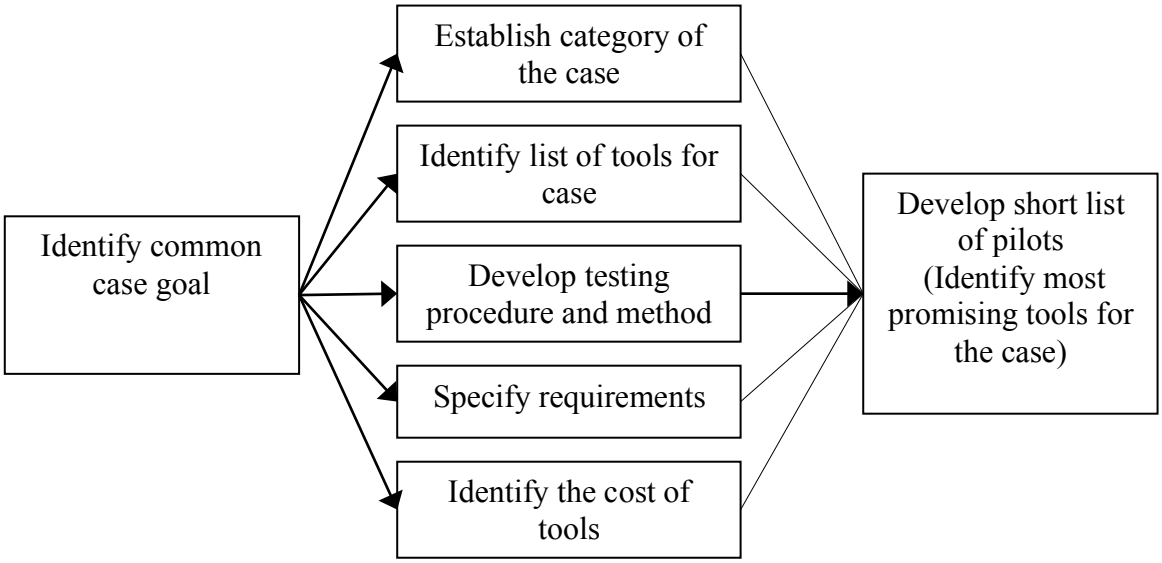



**Figure 3.8: Pre-Research Flow Chart**

| | **Description of Tasks** | |
|---|---|---|
| Main Research Question | What are the capabilities of the 3 chosen tools to collect and analyse evidence from Social Networking Sites in a digital forensic investigation? | |
| Establish Sub-Questions | SQ1 SQ2 SQ3 SQ4 SQ5 SQ6 | |
| Hypothesis | H1 H2 H3 H4 H5 H6 | |
| Evaluation Methodology | • Establish evaluation requirements<br>• Establish rating levels for metrics<br>• Establish criteria for assessment | • Functional requirements<br>• Cost evaluation<br>• Prioritise evaluation criteria |
| Test Scenarios & Findings | • Select metrics and test tools against criteria<br>• Functionality Test | • Evaluate Trailer<br>• Review Performance<br>• Acceptance Testing |
| Analysis | • Requirement Analysis<br>• Access Test results | • Risk Analysis<br>• Compare with Criteria |

**Figure 3.9: Research Flow Chart**

## 3.3 THE RESEARCH DESIGN

The purpose of the proposed study is to conduct research concerning social media forensic tools that can be used to develop crucial evidence from Social Networking Sites (SNSs) such as Facebook, Twitter, LinkedIn and Google Plus. Besides social networking sites, such venues include 'blogs' (a contraction of "weblogs") and 'wikis' (a website that allows the creation and modification of any number of interlinked web pages). This research will demonstrate how to approach the evidence-collection process in these venues by using forensic software applications such as EnCase Forensic, CacheBack and Internet Evidence Finder. These forensic tools are evaluated and compared through an analysis of the sample testing data that results from their use in a laboratory simulation. Other purposes of the proposed study include developing relevant recommendations for the use of these forensic tools (capabilities defined by noted limitations and performances), as well as the professional ethical responsibilities that are involved in their professional use. Guidance Software stated that:

> *"The computer is an infallible witness; it cannot lie. Digital evidence contains an unfiltered account of a suspect's activities, recorded in his or her direct words and actions. This type of evidence can provide the pivotal data investigators need to turn an open investigation into an open and shut case"* (EnCase Forensic for Law Enforcement, 2011, p. 2).

As a result, the identification of the most effective forensics software applications that can capture evidence from social networking sites represents an important initiative for law enforcement agencies seeking to maximize their return on software investments (these applications are costly, at around $10,000). The research design will consist of a comparison of the effectiveness of three mainstream forensic applications - Guidance Software's EnCase digital forensic, JADSoftware's Internet Evidence Finder (IEF) and Cacheback forensic tools.

Since there is a need to collect, analyse, and interpret quantitative and qualitative data in one study, a mixed methodology consisting of both qualitative as well as quantitative elements will be used to conduct the analytical comparison of the EnCase, IEF and Cacheback products. The quantitative elements will consist of how many instances of specified key word searches and other functions of each product results in the desired outcomes (i.e., the identification of desired evidentiary information) using three hard drives containing SNS related artifacts that will be created specifically for this purpose. The qualitative elements will produce a more comprehensive understanding required to inform decision-making, and helps the author to address

research questions appropriately. Using mixed methodology will not only enable the author to address a wide and a more defined range of research question but also enable the author to generate theory through qualitative designs and then evaluate it quantitatively.

From the author's previous technical experience, these three applications are expected to perform within reasonably comparable timeframes, the time required to perform each function will not be included in the data analysis. The weighted numerical totals of each outcome will be collected for each product. Quantitative data only will not provide the robust feedback that is required for such an analytical comparison. A weight will be assigned to each product's data analysis results to indicate their quality, scope and reliability.

This approach is congruent with Lawrence & Neuman's (2003) guidance concerning conducting analytical comparisons. According to Lawrence & Neuman (2003), an analytic comparison "identifies many characteristics and a key outcome, then checks the agreement and difference among the characteristics, to learn which ones are associated with the outcome" (p. 458). This aspect of Neuman's analytical comparison framework makes it an appropriate method for a social network based comparison work, such as one proposed in this research. The results of this weighted comparison of the EnCase, IEF and Cacheback products will be presented in tabular and graphic formats, and interpreted in a narrative fashion.

It is proposed that similar approaches in testing and evaluating tools reviewed in the Section 3.1 will be implemented to determine the capabilities of the chosen tools and its ability to provide digital evidence of an acceptable standard from SNSs. The proposed theoretical research model described is illustrated in Figure 3.10.

Finally, to improve the trustworthiness of the findings, the case management recommendations provided by EnCase for conducting the analytical comparison of three vendors' application products will be followed:

Separate folders for each case; use unique directory names.

Use large capacity, high Revolutions Per Minute (RPM) hard drives with single partition for evidence files.

Forensically sterile the target media to eliminate any claims or arguments of cross-contamination.

Create default Evidence, Export, and Temp folders for each case (EnCase study guide, 2011).

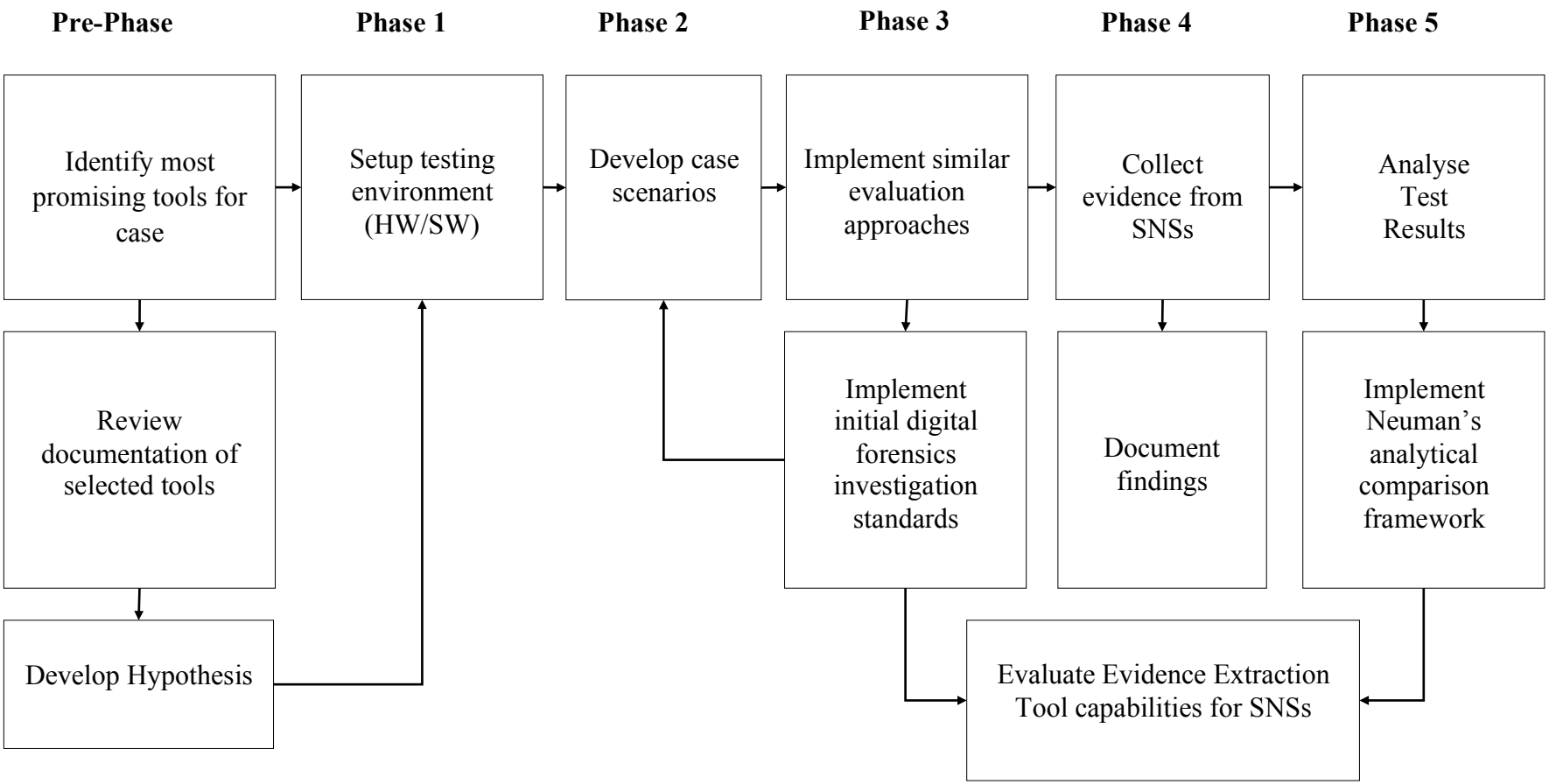



**Figure 3.10: Theoretical Research Design Phases.**

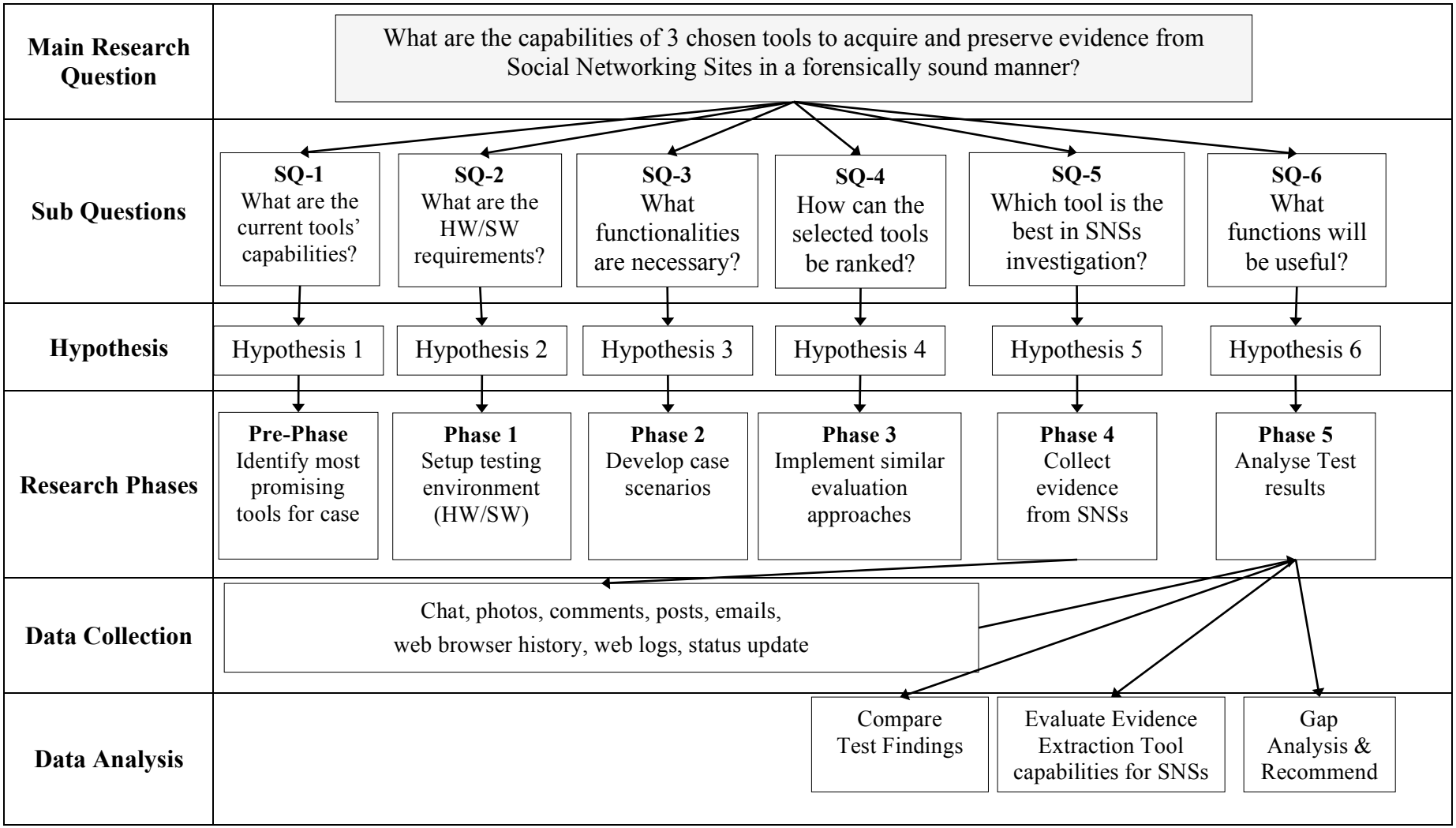



**Table 3.1: Data Map**

## 3.4 DATA REQUIREMENTS

There are a number of requirements for data collection process during the proposed research phases. Information collected from Phase 1 contains a review of related literature, a review of similar approaches in evaluating tools, and technical documentation from the software vendors. In the Phase 2, the testing environment will be configured based on the short list of the 3 chosen tools for this research, the literature review, and the given assertions. A Social Network Forensics case scenario will be developed in phase 3. A number of similar approaches in evaluating tools will be adapted in this research in order to enhance existing approaches. Data requirements that need to be addressed in the research will be checked against digital forensic investigation standards. A series of tests are to be performed and documented in phase 4 according to the adopted testing evaluation approach. By implementing Neuman's analytical comparison framework, data collected in the phase 4 will be analysed accordingly in Phase 5. Finally, the data that is collected will then be analysed and the findings reported in Chapter 4.

### 3.4.1 Preparation

As described in Section 2.2.4, digital evidence is easily distorted, is invisible, and concealed, in nature. The preparation of sample evidence data is an important step. In order to evaluate the chosen tools, it is crucial to prepare what is required prior to collecting evidence from SNSs. Initial preparation includes preservation of source of evidence. It is essential to (1) Have a clear picture of the desired information and intended analyses, (2) include necessary analyses of reliability and validity of evidence. (3) Generating expected evidence data in SNSs (4) Define amount and type of data preparation required before evidence collection phase, and (5) Make sure the computer contains collectable data for each of the 4 main SNSs for the purpose of this study. (6) Precautions are to be taken to prevent alteration of digital information of digital information.

Imaging of computers and associated media must be considered in all cases where further investigation or disclosure may be required. Capturing data using forensically sound methods is mandatory for the integrity of any subsequent investigation to be maintained. It is necessary to prepare tools like Write Blockers for physically imaging entire storage media. Write Blocker is usually used to insure that

evidence is not compromised during the imaging process as it allows information to be read from suspect drive but does not allow the accessing computer to write data to the drive. In addition to preparing tools for collecting data from digital media, software and hardware for the testing process must be prepared. The following software and hardware is prepared for the acquisition, analysis and reporting of the evidence.

**Table 3.2: Prepared list of Software and Hardware**

| Type | Name | Description |
|---|---|---|
| **Software** | EnCase Forensic ver. 6.19 | Encase Forensic is the premier computer forensic application with the ability to image a drive, preserving it in a forensic manner using the EnCase evidence file format (LEF or E01). |
| | CacheBack ver.3.7.5 | As of version 3 (August 2011), a single USB key (dongle), which is required for the software to function, is prepared. A fully functional copy of the software for a period of 5 months has been arranged with the vendor for the purpose of this research project. |
| | Internet Evidence Finder ver.4.3 | A trial version of Internet Evidence Finder is used for searching hard drives or collected files for Internet related artifacts. |
| | AccessData FTK Imager ver.3.0.1 | AccessData's free forensic imaging application is used in many cases. In this study, FTK is used to mount evidence image as a virtual drive. |
| **Hardware** | iMac | An iMac with Mac OS X (version 10.6.8) is configured as an investigation machine. The iMac has configured with Parallel desktop, so that test can be performed on different windows environments. |
| | Desktop PC | A Dell Desktop PC with Windows 7 Professional operation system on a 40GB hard drive is used as a target machine. |
| | Seagate FreeAgent GoFlex (USB) External Hard Drive | A 1 TB external hard disk drive with NTFS file system, which will contain a bit-by-bit copy of the evidence image from the Windows 7 Target computer. |
| | Tableau T35e - Forensic SATA/IDE Bridge - Write Blocker | The Tableau T35e Forensic SATA/IED Bridge write blocker is connected between the target machine's hard drive and the forensic computer in order to acquire evidence image file. |
| | USB 3.0 cable, PC | USB 3.0 cable is used to connect between forensic computer and evidence storage external hard drive. |
| | Anti static Wrist Strap | An Anti static wrist strap is used to prevent electrostatic discharge (ESD) by safely grounding a person working on electronic equipment. |
| | Anti Static Bag | An Anti Static Bag is used for bagging the evidence and during the transfer of evidence to a different location. |

All of the above prepared hardware and software has been calibrated in accordance with the documentation and recommendation of the manufacturer and forensic best practices/standards/procedures.

### 3.4.2 Acquisition

Acquiring forensically sound data is crucial to the data requirements. Data generated in SNSs will be acquired with prepared software/hardware described previously (Section 3.4.1). Data will be collected from the 4 most popular (at the time of writing) social networking websites – Facebook, Twitter, Linked In and Google plus. Each site will store different types of information. The following section describes the artifacts that need to be collected from each SNS. Possible locations, including files or disk areas are also provided.

**Table 3.3: Types of collectible data from each SNS**

| Social Media | File Type | Description | Possible location |
|---|---|---|---|
| Facebook, Twitter, LinkedIn & Google Plus | Web history | Examine and collect Internet histories for Internet Explorer, Firefox, Safari, and Google Chrome. | Users folder, local settings, temporary internet files |
| | Web Cache | Examine and collect Internet cache for Internet Explorer, Firefox, Safari, and Google Chrome. | Users folder, local settings, temporary internet files, unallocated space |
| | Cookies and Session | Cookie, session information can be collected from 4 major browsers. | Firefox profile folders, Temporary internet files, pagefile.sys / hiberfil.sys files, file slack space, and unallocated clusters, places.sqlite files if user used Firefox |
| | Images | Collect all images from 4 different browsers from temporary internet files and internet cache. | Users folder, local settings, temporary internet files, unallocated space |
| | Video | Collect all videos from 4 different browsers from temporary internet files and internet cache. | Users folder, local settings, temporary internet files, unallocated space |
| | Comments and Reply | Corresponding comments and reply | Browser cache file, user folder, unallocated space, pagefile.sys/ hiberfil.sys files. |

| | | | |
|---|---|---|---|
| | Wall Post and Status update | Collect status updates and wall posts. Collectible items include the User ID and Name of the person making the status update or wall post, and the contents of the update/post itself. Possible to collect location information from the status update – collect where the status was updated from, geo-tags, and the text of the status update. | Temporary Internet files, live memory dumps, the pagefile.sys/hiberfil.sys files, file slack space, and unallocated clusters. |
| | Location | Users location stored on Facebook and Google plus can collected from number of different places. | Browser cache file, user folder, unallocated space, pagefile.sys/ hiberfil.sys files. |
| | Chat | Messages sent and received using the Facebook chat feature. Information found with the message can include the Facebook profile ID used to send/receive the message, the from/to names and ID's, and the date/time that the message was sent. | Temporary Internet files, file slack space, and unallocated clusters, pagefile.sys/hiberfil.sys files. |
| | Emails | Collect emails sent or received on SNSs, including but not limited to email notification, friend request notification. Collectible items can include the subject of the email, the recipients of the email, the Last Updated Time, the local time, the User ID and Name, whether or not it was sent from a mobile device, any attachments, and the message. | Temporary Internet files, live memory dumps, the pagefile.sys/hiberfil.sys files, file slack space, and unallocated clusters, outlook profile data. |

It is expected that collectible data from each SNSs will be different, however the steps to be followed for collecting evidence are same for each SNS. The source accuracy must be determined, and then the data must be preserved in a forensically sound manner, documented, and deemed relevant to the investigation purpose. Data from SNSs, like all data on the World Wide Web, can be found from numerous locations. Data can be mainly stored on the web server of the SNS itself, where the data was posted. Therefore, one place to obtain data posted on SNSs is from the site itself. Another main source of the SNS data is the computer utilised to access SNSs. This research will be focus on collecting evidence from the computer of the user who accessed the website.

Because the data from the SNSs is dynamic, data from websites can altered or deleted altogether. To check the integrity of the collected data, MD5 hash value of the data will be calculated and documented during the collection process. In order to properly preserve evidence, collection must be done completely to ensure that all SNS information is captured from the user's computer. Collecting a complete image of user's computer provides evidence of users web usage, IP address, activity log, time stamps of relevant post or attached documents, and even deleted files may be found from the SNSs. As finding data from user's computer is dependent on how often user uses computer, what programmes were installed and used, a forensic copy of the computer can indicate how the user interacted with the computer, and what software has been installed and used.

To ensure the research process is repeatable and auditable like other digital forensic procedures, a journal of every action performed during the collection will be documented in a chain of custody form. The chain of custody will also contain the exact date and time the collection task was performed, the user's computer system information, and procedural information. The chain of custody will provide detailed information for the court of law and other forensic examiners, about what has happened after the seizure of the user's computer. An additional technical note with much detailed information will be kept to remind forensic examiners what has been done to collect data from the user's computer and therefore, other forensic examiners can perform the same collection procedure and get the same result. Notes will include information about system type, software configuration settings, collection procedure, size of data, and time spent for data collection.

### 3.4.3 Analysis

The first level of data analysis will be an examination of the accuracy of the collected data from SNSs. Once the data is accumulated, analytical study is to be performed to explore the meanings of collected data from the SNSs. Collected data from each of the three applications will be analysed. Once the data is accumulated, in depth analysis work will be performed to capture the meanings of the recovered data from a logical and physical space, the professional space, and the capability space. This analysis work from the collected data will answer questions including:

**Who** posted content in question?

**When** was the content(s) posted?

**Place** from which the contents was posted (Geo tag information)

**Who** will be the person to contact for more information (User ID or SNS provider)

**What** other evidence can be collected from the SNSs?

In the second level of analysis will be a comparison of three chosen tools. Data analysis is planned to scope the capability and then to compare each tool to the others by performance and by function. Table 3.4 shows the data analysis procedures to examine functionality of each tool.

**Table 3.4: Data Analysis Procedure**

| Procedures | Task description |
|---|---|
| SNS data examination | Forensic examination of SNS data from suspect's external hard drive and splitting and merging of collected information based on evaluation requirements. |
| SNS data analysis | Forensic analysis of examined data to determine tools performance and function. |
| Rating Tools | Based on against assessment criteria, weighted numerical totals of each outcome will be collected and calculated for each tool. |

As data collected from the suspect's hard drive is the main source of evidence, the analysis will categorise the testing results based on evaluation requirements. Ability to collect chat logs, photos, comments, posts and emails from SNSs will be examined to determine tools performance. In order to rating the performance and function of each tool, HKBS approach will be used.

The final stage of data analysis is a weighted analysis of data requirements. As discussed in section 3.3 the weighted numerical totals of each outcome will be collected for each product based on the HKBS method previously outlined. For example, the test result will be ranked with the scale of measurement for criterion is level of satisfaction on the level 0 (very poor) to 5 (very good). Average score will be calculate for each tool and this will be used as a metrics for evaluating tool.

The testing result will be empirically based to Neuman's (2003) guidance and will inform the research questions. In addition to the analytic comparison method developed by Neuman (2003), this research will also apply the Event-Based Digital

Forensic Investigation framework developed by Carrier and Spafford at the Purdue University (Carrier & Spafford, 2004). It is expected that the amount of data collected from the 3 applications will be large and considerable processing effort derive information from the yielded data (McKemmish, 2008). Targeted examinations will be performed by selecting specific files and data types for review while ignoring file of irrelevant type and content (Pollitt, 2008). This analysis work will be based an assumptions of the importance of relationships in the criminal case, and (1) working backwards by asking what information is desired, (2) selecting query that searches in specific locations in order to analyse the link between the collected data and the characteristics of case. This allows the collected information to produce information that may sufficient in courts of law. As the process continues, it may be necessary to refer back the literature and find the relationships between the collected data and observations already reflected upon.

The event based digital forensic investigation framework has been selected as an additional research design and method for this research as a stated aim of this method is to find evidence from the events and take to the stage that makes a significant findings from chosen forensic software. Using mixed tool evaluation approaches that has been studies in Section 3.1 and adding Newman's comparison method will assure a higher level of reliability and validity to the research findings. In this way the results can be established for each tool, a comparison between tools, and benchmarking against user expectations.

### 3.4.4 Presentation & Incident closure

Once the analysis is complete, presenting an understandable, defendable and complete report is required. Data analysis will enable the digital forensics examiner to reconstruct some of the user's activities on SNSs. Deleted access logs or files recovered from the user's computer can show not only traces of the user's activities, but also can show when and how user interacted with SNSs. The result from all three tested applications will be collected in order to create a timeline of events.

Subsequent to data collection and analysis, reconstruction of the evidence will be performed. A weighting will be assigned to each product's data analysis results to indicate their quality, scope and reliability. The weighted numerical totals will be reported, analysed and presented in order to clearly convey the findings achieved from

the 3 applications in the collection phase. Data needs to be presented to show the capabilities of each tool in the collection of evidence from SNSs. The various point outlined by the data collection requirements will be evaluated and the aggregated data produced will be reported in a table and graphical chart format. A number of important points of interest need to be presented. For example, characteristics of URLs from SNS, location of evidence found, and a physical memory analytical report will also be important aspect of this research. In addition, a 'percentage of collected data' will be calculated to display the evidence extraction capabilities for each tested tools.

The extraction tool capability result based on the analysis phase will be clearly displayed to present the strengths and weaknesses of each tool. The presentation will be easily understandable by non-technical people and explained in precise detail. The addition of relationship charts, of entities, timelines, and SNS activity analysis will be produced in order to give readers a clear understanding of each tool's capabilities as well as to convey method of acquiring evidence from SNSs.

The final stage of investigation process is the incident closure phase. As the phase name implies, collected data and analysis work will be finalised and focus will be given to closure of the investigation. A critical review of the entire investigation process as well as tool evaluation process will be conducted, and items of significance from this research will be highlighted. Based on the research findings and analysis work, relevant recommendations will be developed. Recommendations will be made for three distinct areas of Social Network Forensics. Firstly, recommendations will be made for the use of forensic tools for Social Network investigation. Secondly, recommendations for choosing tools in terms of capabilities, limitations and performance in each tool based on the case, and finally recommendation for professional ethical standards in Social Network investigation, as well as responsibilities that are involved in their use of evidence extraction tools.

## 3.5 EXPECTED OUTCOMES

The expected outcomes of the proposed research design will be outlined and discussed in regard to the capabilities of each tool from the data collection and analysis phases.

As discovered from the literature review, Social Network Forensics is a new field in digital forensics. Therefore it is expected that capability to extract evidence from SNSs will be limited. Obtaining evidence from SNSs will be complex due to the

characteristics of SNSs (posting from a number of different location with different devices by any given user). Obtaining complete evidence from SNSs is not possible, however collected data from one of the tools will be able to give clues for where to look in order to get more information. Thus, the expected outcome of the extraction tool capability evaluation is that no tool will find all of the evidence from SNSs. Some tools may extract more data in one social networking site and less from the others.

Collected data from all three tools will be weighted in each category of collection requirements and it is expected that this weighted number indicate strengths and weaknesses in each tool. It is also expected that no one particular tool will be ranked significantly higher than other tools, and indicating the need for multiple tools for best investigative results. Understanding what capabilities each tool have and what functionalities can be used for investigation will assist forensic investigators in utilising the most suitable tools, or, in utilising the multiple tools together to enhance the investigation process.

## 3.6 LIMITATIONS OF RESEARCH

The research evaluates an evidence extraction tool's capability in the case of Social Network investigation with capability tests being applied across the three different tools. When SNSs are involved in a crime, the digital forensic investigator needs to choose tools to collect and analyse the evidence from technical devices. Because each tool has its own functionalities and limitations, the research method that has been proposed poses a number of limitations. It is crucial to identify such limitations in order to correctly perform a forensically sound investigation and to understand the capability of the tools.

Evaluation of extraction tools also has some limitations that must be taken into account to set realistic expectations of each tools capability. The first limitation of the proposed research is that none of the three selected tools are specifically designed for Social Network investigation. There are limitations in the selection of tools in this research. The three tools have been selected due to availability and reputation in the market place. A number of other available tools (both open source and commercial software) are available on the market and they can be used for SNS forensics, but the focus of evaluation is on three selected well-known and available tools.

The second limitation is that the tool evaluation process cannot establish the entire functionality of each tool as the testing result is based on the research design model proposed in this research. The objective of this research is to identify and test any many evidence extraction capabilities and functionalities as possible, not necessarily to identify all of them. There is limitation in identifying every possible capability on different case scenarios.

Another limitation of the proposed research is that evaluation process cannot be used to measure capabilities in all SNS investigation process as it may different case-by-case bases. Additionally, the testing environment within which the testing machine is configured is itself fabricated for the purpose. Testing environments have been set up in AUT's digital forensic laboratory, that has been created for this specific purpose. Hence, it may or may not be completely representative of the actual digital forensic investigation environments, which examiners will encounter in digital forensic investigation.

Although this research seeks to ensure the highest probability of accuracy in testing, the above limitations must be considered. The identified limitations of this research method and limitation of tools' capability will provide directions for future research in the area of SNS evidence extraction tool development and implementation.

## 3.7 CONCLUSION

Literature review conducted in Chapter 2 indicated that need for looking into a disciplined approach for effective ways to extract evidence from SNSs. Digital forensic investigators require different tools and techniques to collect evidence and researching into the capability of extraction tools will help the investigation process in a more effective way.

In Section 3.1, five similar approaches in evaluating tools have been reviewed. It is of interest to compare digital forensic tools evaluation approaches and general software evaluations approaches. All similar approaches obtained from the review in section 3.1 are used to determine the most objective approach for this research. Review of similar approaches undertaken in this chapter shows that there are a number of different approaches in evaluating tools capabilities. Each evaluation method has its

strengths and weaknesses. In this study of attitudes toward Social Networking investigation tools evaluation, a combination of approaches in addition to the analytic comparison method developed by Neuman (2003) with the Event-based Digital Forensic Investigation framework is indicated as the most appropriate method. The choses extraction tools will be evaluated and rated accordingly. Data will be collected, documented and analysed based on the research design proposed in this chapter and findings will be presented, and an attempt will be made to reconstruct some of the key evidence found from SNSs.

A main research question and its sub questions have been set in Section 3.2. The research questions and hypothesis set in the section 3.2 is the key variable in this research. Section 3.3 discussed the research model to answer those questions. The research design has been set by addressing (1) author's interests, (2) author's abilities and the (3) available resources. The proposed research will look at the capability of evidence extraction tools for the collection and analysis of data stored on a user's computer. An attempt will be made to find relevant logs and histories that are related to SNSs. The collection will be made based on the data requirements discussed in Section 3.4. Limitations of this research are outlined in Section 3.6, providing the possible errors in this research were detailed and discussed.

Chapter four will conduct the evidence collection and analysis work based on the research design and methodology developed in Chapter 3. Research findings will provide comparison results of the extraction capability provided by each tool in terms of functionality and accuracy. A more detailed illustration of such evaluation result will be presented in a table and graphical chart format. The research result will inform both forensic investigators and vendors in a realisation of the shortcomings of existing tools, and for future improvement to address the identified weaknesses.

# Chapter Four

# RESEARCH FINDINGS

## 4.0 INTRODUCTION

The availability of digital forensic tools that provide evidence extraction capabilities from SNS environments continues to grow. However, the literature review indicates that there is no single tool that has the ability to examine every possible type of data or artifact from SNSs. Each tool is available with specific capabilities making it vital for forensic examiners to understand the use of each tool they use for investigation process in order to critically analyse digital evidence. The literature review in Chapter 2 helps us define SNS forensics, the necessity of using tools for the SNS investigation process, and raises a number of issues with SNS forensics. Chapter 3 formulated the main research question and sub-questions based on the problems identified in Chapter 2. The research model has been designed based on the main research question and hypotheses. A number of similar approaches in evaluating tools have been explored to establish the research method for the purpose of this study. The methodology was then established for this study to answer the research questions.

The purpose of Chapter 4 is to report on the research findings from the research design model and data collection phases outlined in Chapter 3. Chapter 4 falls into four major sections. Section 4.1 sets up the variations in the research specification and how each of the three evidence extraction tools performs in collecting data from the test environment. The summarised data collection result from each phase is presented with in tabular form in Section 4.2, from the laboratory testing work. Collected data is analysed in Section 4.3 and the mixed evaluation approaches reviewed in the Chapter 3 are used to evaluate tools with the forensic procedure discussed in Chapter 2. In the final section 4.4, the research findings and analysis report are presented in tabular and graphic formats, and interpreted in a narrative fashion.

The three selected tool's extraction capabilities have been tested with common SNS activities such as comments, events, or chatting logs extractability. Research findings in this chapter will assist forensic examiners to identify the strength and weaknesses of extracting evidence from SNSs using a tool tested in this study, and may contribute to the digital forensic community as a valuable reference.

## 4.1 VARIATIONS IN DATA REQUIREMENTS AND METHODOLOGY

The testing data went through four phases as discussed in chapter 3: 1) data preparation, 2) data collection, 3) data analysis, and 4) data presentation and closure. Most of the evaluations were conducted according to the test plan specified in Chapter 3. However, a few minor changes were necessary in order to continue progressing with the data preparation and collection phases. Minor changes made to the preparation and collection phases are explained in the following sections.

### 4.1.1 Data preparation

Unforeseen issues discovered during initial testing resulted in a couple of changes needed to be made to the data preparation procedure. For example, some of the planned tests were not successful due to data artifacts remaining in the testing target hard drive. This resulted in finding more evidence than expected in the data. Therefore, test data had to be re-entered after "zeroing" the target machine's hard drive. In order to eliminate the issue, Partition Magic and Eraser 6.0.8 tool was used to zero out the hard drives prior to putting the second testing data into the hard drive, so that author could control the testing environments from a known baseline. Eraser tool is selected to zero out the hard drives as it allows completely remove the data from the hard drive by overwriting it several times with carefully selected patterns.

A zeroed hard drive was setup with the Windows 7 professional operating system. After installing the Windows 7 operating system on a target machine, the latest version (at the time of writing) of four web browsers (Firefox 7.0.1, Chrome 14, Safari 9, IE 9) were installed on the target machine. A simple test was performed against all 4 installed browsers to make sure website access information is stored on each browser. Testing data has been posted and uploaded into 4 different browsers on each social networking site (See Appendix – Testing data section).

### 4.1.2 Data collection

A couple of additional software packages had to be used in the data collection phase. The hard drive was collected and imaged using Tableau Imager (TIM) in order to optimise for imaging with Tableau write-blockers described in chapter 3.

Internet Evidence Finder (IEF) v4 cannot run directly on forensic image acquired in .E01 format, these image files must be mounted as a virtual drive first. To mound the evidence image as a virtual drive, additional software - FTK imager 3.0.1 has been used to mount the image as a virtual drive and run IEF.

CacheBack has released a beta version of standalone disk-level Facebook chat recovery software as an add-on tool called Recover My Chat (RMC). Instead of relying on an Encase script provided by Cacheback, Facebook chatting could be recovered by this standalone chat forensic recovery and reporting tool. This add-on service provides disk level access as well as logical file access to NTFS and FAT32 partitioned hard disks, which makes a good tool for this testing scenario. Like IEF v4, CacheBack cannot run directly on a forensic image acquired in .E01 format. However it has the ability to scan the logical and physical disk space from mounted volumes. Unfortunately CacheBack's RMC is incompatible with a FTK image that has been used for IEF investigation, as FTK imager mounts NTFS volumes as Raw FAT32 volumes instead of their original NTFS format. It is therefore, requires additional mounting software – Mount Image Pro (MIP). Version 4 has been used for Facebook chatting history collection process with CacheBack's RMC.

### 4.1.3 Data Analysis

In order to get the number of expected web history, cache and cookies on a target computer, the following open source utilities have been used to count the expected number of Internet access records.

**Table 4.1: Open source utilities used to count browser access records**

| Software | Version | Purpose |
|---|---|---|
| IE History View | v1.65 | To count the number of histories made using Internet Explorer 9. |
| IE Cache View | v1.46 | To count the number of files currently stored in the Internet Explorer cache. |
| IE Cookies View | v1.74 | To count the number of cookies that Internet Explorer stores on target computer. |
| Mozilla History View | v1.42 | To count history data file (history.dat) of Firefox Web browsers. |
| Mozilla Cache View | v1.50 | To count the number of cached items from cache folder of Firefox Web browser. |
| Mozilla Cookies View | v1.36 | To count the number of cookies stored inside the cookies file. |
| Chrome History View | v1.05 | To count the list of all visited Web pages in Chrome web browser. |
| Chrome Cache View | v1.30 | To count the list of all files currently stored in the cache in Chrome browser. |
| Chrome Cookie View | v1.02 | To count the list of all cookies stored by Google Chrome Web browser. |
| Firefox Add-on SQLite manager | v0.7.6 | To count the number of cookies, caches stored on safari browser. |

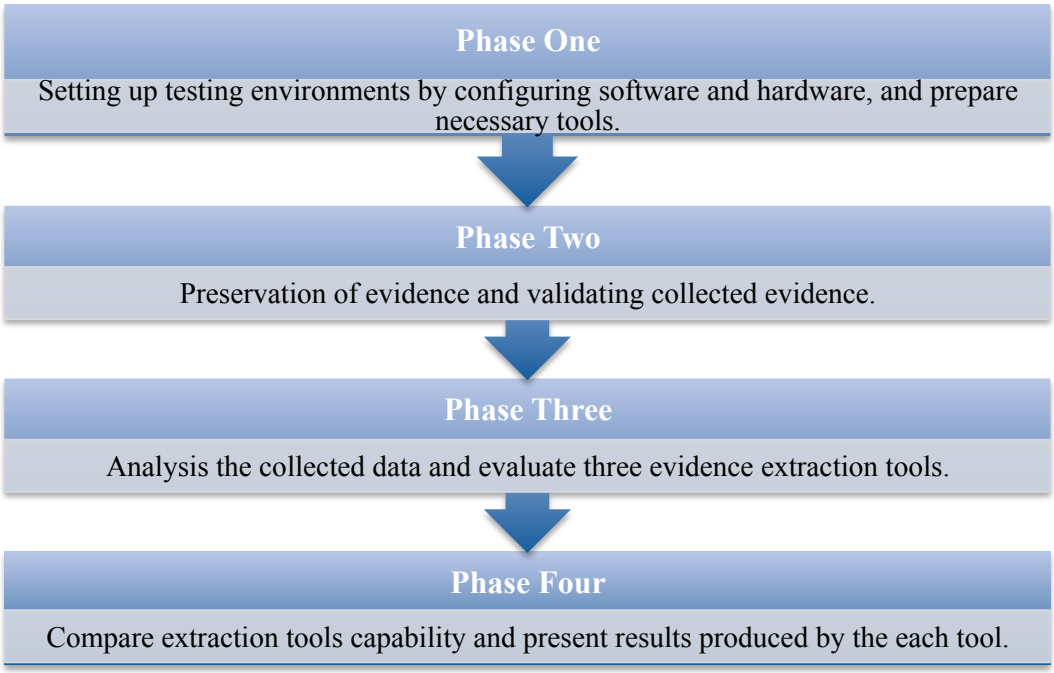
To test if the tool can produce the same result with different investigator's computer, test cases were performed with 2 different investigation computers instead of 1. Test is performed 3 times on each forensic machine, one with parallel Windows 7 on a Mac OSX (Virtual Windows environment), one with Windows 7 on Dell laptop computer.

### 4.1.4 Presentation & Incident closure

Testing data is presented exactly as from what has been defined in section 3.4.4 and a critical review of the entire investigation process as well as tool evaluation process has been conducted.

## 4.2 FIELD FINDINGS

The fieldwork was carried out in four phases:




Each phase is carried out sequentially and logically connected. Phase one involved setting up an accurate testing environment for this research both at AUT's digital forensics laboratory and at personal research space. All required hardware and software have been organised and installed on the forensic laboratory. Phase two involved acquiring evidence from the target computer (Windows 7 PC laptop) in a forensically sound manner. A number of tools, such as Access Data's FTK Imager, and USB Tableau T8 Write Blocker have been used to make sure the collection

process is forensically sound. Phase three involved analysing the collected data from the target computer and listing the identified evidence for each tools tested. The final phase was a comparison of extraction tools capability with corresponding case requirements. Based on assessment criteria and the analysis result from the previous phase, weighted numerical totals of each outcome are collected and calculated for each tool.

### 4.2.1 Testing Environments

In order to collect and analyse evidence acquired from the target desktop computer, the testing environment has been set up accordingly to accommodate the needs of forensic analysis of the target machine. Required hardware and software identified in table 3.2 have been prepared to make the collection process forensically sound. Complete hardware specifications are shown in Table 4.1. A list of software that was used during the testing is also summarised in Table 4.2. The software and hardware has been selected in consideration of PC and MAC compatibility issue.

Test machine was created on two Windows 7 operating systems. One is installed on iMac with the Parallel Windows operating system, the same operating system with Windows 7 Enterprise version was installed on the second testing system to be used as an investigation machine. Both testing system had 2GB of RAM. A desktop PC with Intel 4 CPU, 2.00GB of RAM is used as the target machine. Windows 7 Professional version was installed. Prior to installing Windows 7, the target machine's hard disk was overwritten with zeros to ensure that previous artifacts remained on the media were completely removed. A new user account is created on the target machine with administrator's privilege, so that testing can predict that user has access for all activities on the system.

Target computer and investigation computer has been selected in accordance with the existing resources that were available. A combination of tools was required to create appropriate testing environments for the data collection, analysis work and evaluation of the three selected tools. The full hardware and software specifications for the testing environment are displayed in Table 4.2 and 4.3.

**Table 4.2: Detailed Evidence Hardware & Operating systems Specifications**

| Purpose | Kind | Manufacturer | Format/Details |
|---|---|---|---|
| Target computer | Desktop PC with Windows 7 Professional | Dell | Intel 4 CPU 3.20 GHz 2.00GB of RAM |
| For secure, hardware-based write blocking | Forensic SATA/IED Bridge | Tableau | Model: T35e |
| Evidence image storage disk | External USB Hard Drive (1TB) | Seagate<br>(Model: Seagate FreeAgent GoFlex) | FAT32<br>Firmware Revision: 210 |
| Investigation computer | Mac OS X Version 10.6.8 with Parallel Windows 7 | iMac/Apple | 3.06 GHz Intel Core 2 Duo with 4GB DDR3 memory |
| Investigation computer | PC Laptop with Windows 7 | Dell (Model: Latitude E6500 Laptop) | Intel® 45 Express Chipset (160GB)<br>2.00GB of RAM |

**Table 4.3: Detailed software specifications**

| Software | Version | Purpose |
|---|---|---|
| Tableau Imager | 1.11 | To image target hard drive with Tableau write-blockers. |
| FTK Imager | 3.0.1 | To mount the image as a virtual drive and run IEF and Cache Back on that drive. |
| CacheBack | 3.7.5 | Used to analyse SNS evidence from target computer. |
| CacheGrab | 1.9.0 | To collect cache and history from the logically mounted volume. |
| GrabMedia | 1.0.3 | To collect media files from the logically mounted volume. |
| Recover My Chat ™ Add-on (RMC) | Beta | To collect internet chatting messages (including facebook)- standalone disk-level Facebook chat recovery tool. |
| Mount Image Pro | 4.5.9.853 | Used to mount EnCase .E01 file (used with RMC) |
| Internet Evidence Finder | 4.3 | Used to analyse SNS evidence from target computer. |
| EnCase Forensic | 6.19 | Used to run EnScript provided from Cacheback. |

**Table 4.4: Detailed Web browser used in testing environment**

| Browser | Version | Details |
|---|---|---|
| Mozilla Firefox | 7.0.1 | Most up to dated firefox browser at the time of writing |
| Google Chrome | 14.0 | Most up to dated Chrome browser at the time of writing |
| Microsoft Internet Explorer | 9 | Most up to dated Internet Explorer at the time of writing |
| Apple Safari | 5.1 | Most up to dated Safari browser at the time of writing |

### 4.2.2 Field Findings: Evaluation of SNS evidence extraction tool's capability

This section discusses the testing procedures taken in this study and shows the testing result for each testing scenarios. A data collection process is performed to collect the entire physical disk image from the target computer. The disk imaging tools were utilised to acquire evidence from a target machine (PC laptop) and the acquisition result was verified using FTK Imager and EnCase image verification tools. Figure 4.1 shows the collection setting on testing environments.

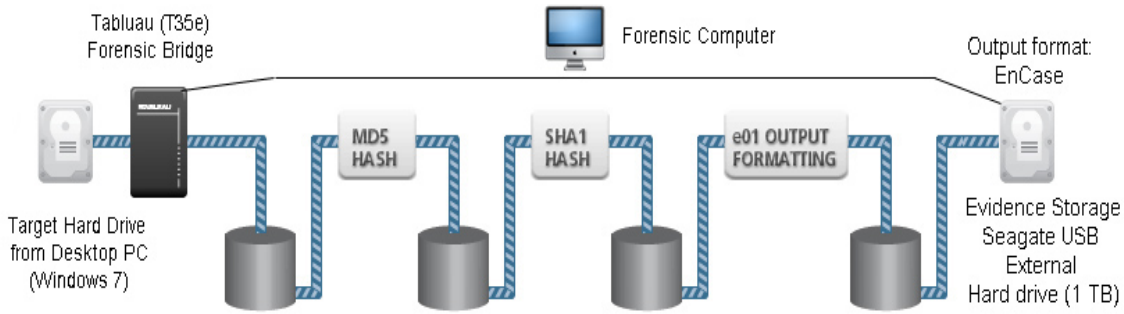



**Figure 4.1: Data collection setting**

The image SHA1 values and MD5 checksum have been checked after acquisition. The verification result is shown in Appendix A-4. After the verification, the acquisition results were further analysed for each tool. Evidence extraction tools are tested against the types of collectible social SNS data described in Table 3.3.

To determine the accuracy of a forensic tool, each extraction result is assigned a quantitative value between 0 and 3 for each of the 11 scenarios outlined below. If a tool failed to recover any data in a particular area, it was rated a 0 for that category.

A rating of 1 indicates some information was found however it did not meet the expected result and therefore cannot be presented as digital evidence. A rating of 2 indicates the tool met the expected results. A rating of 3 indicates the tool exceeded the expected result including recovering deleted data and/or more information than other tools were able to recover. Following table 4.5 summarises the test rating scale:

**Table 4.5: Test rating scale**

| Rating | Rating description | Rating standard | Found |
|---|---|---|---|
| **0** | Miss | Unable to find any evidence | 0% |
| **1** | Below | Sometimes to find evidence but not accurate | 1 - 30% |
| **2** | Meet | Can meet the search requirement | 31-60% |
| **3** | Above | Can meet the requirement and provide excellent result | 61 - 100% |

Before testing can be performed, it is necessary to know the expected data from the target hard drive so that each tool can be compared against that expected data. The target disk has been completely cleared by "zeroing" the disk and removed all unused disk space to control the testing environments from a known baseline.

In order to have some determine accuracy of the test result, prepared post and media have been posted on each 4 social networking sites using 4 most popular web browsers. Each post contains unique number and browser identifier. Appendix B-1 – Appendix B-8 shows the identifier for each posting made on each SNSs. The findings from the tests of three evidence extraction tools for each test case are summarised and discussed below.

#### 4.2.2.1 Web history analysis

Web history analysis is important for Social Network investigation as critical evidence can be found from web browser history. In cases that involve crimes predominately carried out using web browsers, a tool's ability to extract web history in a visual format is crucial part for digital investigators. After inserting test information on SNSs, the number of web history, cache entries, and cookies been counted on each browser (See Appendix B-1). NirSoft's s utilities are used to confirm number of history items on each browser. Reading the history.dat, index.dat file from each

browser, each visited web page entry has been exported into an excel file to calculate the total expected numbers.

**Table 4.6: Internet history extraction test result summary**

| | | CacheBack v.3.7.5 | IEF v.4.3 | EnCase v.6.19 | Expected |
|---|---|---|---|---|---|
| Facebook | Firefox | 11 (55%) | 4 (20%) | 0 (0%) | 20 |
| | Chrome | 12 (23%) | 0 (0%) | 0 (0%) | 52 |
| | Safari | 8 (72%) | 0 (0%) | 0 (0%) | 11 |
| | IE | 0 (0%) | 4 (66%) | 6 (100%) | 6 |
| **Rating** | | **2** (37.5%) | **1** (21.5%) | **1** (25%) | - |
| Twitter | Firefox | 29 (88%) | 19 (58%) | 0 (0%) | 33 |
| | Chrome | 26 (74%) | 0 (0%) | 0 (0%) | 35 |
| | Safari | 12 (100%) | 0 (0%) | 0 (0%) | 12 |
| | IE | 0 (0%) | 1 (6%) | 15 (100%) | 15 |
| **Rating** | | **3** (65.5%) | **1** (16%) | **1** (25%) | - |
| LinkedIn | Firefox | 17 (100%) | 7 (40%) | 0 (0%) | 17 |
| | Chrome | 13 (86%) | 0 (0%) | 0 (0%) | 15 |
| | Safari | 11 (100%) | 0 (0%) | 0 (0%) | 11 |
| | IE | 0 (0%) | 4 (67%) | 6 (100%) | 6 |
| **Rating** | | **3** (71.5%) | **1** (27%) | **1** (25%) | - |
| Google Plus | Firefox | 10 (52%) | 8 (42%) | 0 (0%) | 19 |
| | Chrome | 8 (53%) | 0 (0%) | 0 (0%) | 15 |
| | Safari | 2 (100%) | 0 (0%) | 0 (0%) | 2 |
| | IE | 0 (0%) | 0 (0%) | 3 (100%) | 3 |
| **Rating** | | **2** (51.25%) | **1** (11%) | **1** (25%) | - |
| **Total Rating** | | **2** (56%) | **1** (19%) | **1** (25%) | |

The entire device is examined, including file 'slack space' and unallocated space, in the collection of Internet history. The testing procedure and some sample results can be found from Appendix C-1, Q and U. Table 4.5 provides summary of the result of internet history collection result. It is noted that Cacheback collected the highest number of Internet histories from all 4 browsers.

#### 4.2.2.2 Internet Cache analysis

The Internet cache is very useful in digital forensics investigation as it stores copies of web pages the user has visited.

**Table 4.7: Internet cache extraction test result summary**

| | | CacheBack v.3.7.5 | IEF v.4.3 | EnCase v.6.19 | Expected |
|---|---|---|---|---|---|
| Facebook | Firefox | 334 (90%) | 0 (0%) | 115 (31%) | 369 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 335 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 264 |
| | IE | 184 (58%) | 2 (1%) | 316 (100%) | 316 |
| **Rating** | | **2** (37%) | **1** (0.25%) | **2** (33%) | - |
| Twitter | Firefox | 34 (69%) | 0 (0%) | 28 (57%) | 49 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 46 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 53 |
| | IE | 17 (53%) | 1 (3.2%) | 32 (100%) | 32 |
| **Rating** | | **1** (30%) | **1** (0.8%) | **2** (39%) | - |
| LinkedIn | Firefox | 263 (96%) | 0 (0%) | 98 (36%) | 273 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 257 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 300 |
| | IE | 26 (15%) | 5 (2.8%) | 172 (99%) | 173 |
| **Rating** | | **1** (27.75%) | **1** (0.7%) | **2** (34%) | - |
| Google Plus | Firefox | 70 (55%) | 0 (0%) | 2 (1.5%) | 127 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 62 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 6 |
| | IE | 12 (13%) | 3 (3.4%) | 86 (100%) | 86 |
| **Rating** | | **1** (17%) | **1** (0.85%) | **1** (25%) | - |
| **Total Rating** | | **1** (28%) | **1 (0.65%)** | **2** (33%) | |

A number of techniques have been applied to count the total number of found cache items on each browser. For example, a customised sql query has been written and applied to CacheBack's custom query option (See Appendix C-1). Internet Evidence Finder was able to find some cache data from Firefox's place.sqlite history file (See Appendix C-5), A comprehensive Internet history search function has been used in EnCase (See Appendix C-9).

#### 4.2.2.3 Internet cookies and session analysis

A website cookie is a small file containing information about the web site visited by users and is saved as information on the user's computer so it can be used at a later date.

**Table 4.8: Internet cookies and session extraction test result summary**

| | | CacheBack v.3.7.5 | IEF v.4.3 | EnCase v.6.19 | Expected |
|---|---|---|---|---|---|
| Facebook | Firefox | 7 (100%) | 0 (0%) | 0 (0%) | 7 |
| | Chrome | 6 (100%) | 0 (0%) | 0 (0%) | 6 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 0 |
| | IE | 1 (100%) | 0 (0%) | 1 (100%) | 1 |
| **Rating** | | **3** (75%) | **0** (0%) | **1** (25%) | - |
| Twitter | Firefox | 10 (100%) | 0 (0%) | 0 (0%) | 10 |
| | Chrome | 9 (100%) | 0 (0%) | 0 (0%) | 9 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 1 |
| | IE | 1 (33%) | 0 (0%) | 3 (100%) | 3 |
| **Rating** | | **2** (58.25%) | **0** (0%) | **1** (25%) | - |
| LinkedIn | Firefox | 17 (100%) | 0 (0%) | 0 (0%) | 17 |
| | Chrome | 12 (100%) | 0 (0%) | 0 (0%) | 12 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 0 |
| | IE | 3 (100%) | 0 (0%) | 3 (100%) | 3 |
| **Rating** | | **3** (75%) | **0** (0%) | **1** (25%) | - |
| Google Plus | Firefox | 5 (100%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 4 (100%) | 0 (0%) | 0 (0%) | 4 |
| | Safari | 0 (0%) | 1 (100%) | 0 (0%) | 1 |
| | IE | 1 (100%) | 0 (0%) | 1 (100%) | 1 |
| **Rating** | | **3** (75%) | **1** (25%) | **1** (25%) | - |
| **Total Rating** | | **3** (70%) | **1** (6%) | **1** (25%) | |

While IEF and EnCase were able to collect a few cookies from Internet Explorer, CacheBack was able to collect most cookies from all browsers, except Apple Safari web browser.

#### 4.2.2.4 Photo analysis

Cachback produced a gallery view of photo file found from the evidence image and quickly categorised and reported on the evidence. Cacheback's user-friendly graphical interface dramatically reduced the amount of time to collect the number of expected photos from the forensic image of the target machine. Encase image and videos have been checked with Hashing analysis function from EnCase. Hash value (digital fingerprint) for the originally uploaded pictures and videos has been generated. The MD5 hash is then compared to fingerprints of files found from the EnCase (See Appendix C-10). Finding notable images from EnCase was very fast and effective as well. In order to see all the notable pictures from the evidence disc image, hash values have been created for the original images, and hash analysis performed to see the any matched evidence against to the expected testing data. Internet Evidence Finder does not support any image collection.

**Table 4.9: Photo extraction test result summary**

| | | **CacheBack v.3.7.5** | **IEF v.4.3** | **EnCase v.6.19** | **Expected** |
|---|---|---|---|---|---|
| Facebook | Firefox | 5 (100%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 3 (60%) | 0 (0%) | 0 (0%) | 5 |
| **Rating** | | **2** (40%) | **0** (0%) | **0** (0%) | - |
| Twitter | Firefox | 5 (100%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 2 (40%) | 0 (0%) | 0 (0%) | 5 |
| **Rating** | | **2** (35%) | **0** (0%) | **0** (0%) | - |
| LinkedIn | Firefox | 5 (100%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 5 (100%) | 5 |
| **Rating** | | **1** (25%) | **0** (0%) | **1** (25%) | - |
| Google Plus | Firefox | 5 (100%) | 0 (0%) | 5 (100%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 5 (100%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 5 (100%) | 5 |
| **Rating** | | **1** (25%) | **0** (0%) | **3** (75%) | - |
| **Total Rating** | | **2** (31%) | **0** (0%) | **1** (25%) | |

The author found the CacheBack tool intuitive, and no unexpected events in the operation of the tool were indicated during testing. Identifying and cataloguing graphical image based evidence with minimal effort, resulted in the highest rank among the three tested tools in collecting images from SNSs. CacheBack also has the Photograph Aspect Ratio Differential (PARD) system, which uses photograph aspect ratio theory. Using CacheBack's photo analysing functionalities (PARD) with the bookmark query feature, significantly reduced investigation time and author was able to isolate pictures that are of photographic and forensic interest to the particular research.

#### 4.2.2.5 Video component analysis

Only CacheBack was able to extract a few video clips from the Google plus website. Collected videos include: 5 videos uploaded into Google Plus via Firefox and 1 video clip from Internet Explorer. While CacheBack identified these video clips, a video player provided by Cacheback was not able to play the video clips.

**Table 4.10: Video extraction test result summary**

| | | **CacheBack v.3.7.5** | **IEF v.4.3** | **EnCase v.6.19** | **Expected** |
|---|---|---|---|---|---|
| Facebook | Firefox | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| **Rating** | | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) |
| Google Plus | Firefox | 5 (100%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 1 (20%) | 0 (0%) | 0 (0%) | 5 |
| **Rating** | | **1** (30%) | **0** (0%) | **0** (0%) | **0** (0%) |
| **Total Rating** | | **1** (15%) | **0** (0%) | **0** (0%) | |

#### 4.2.2.6 Wall post and Status Update analysis

Ability to recover status update and wall post from the 4 SNSs have been tested. Recovered items include the User ID and name of the person who made the status update or wall post on Facebook as well as the text of the status update. While CacheBack and IEF failed to extract any information from the 4 SNSs, EnCase was able to find some wall posts and status updates from each SNS (See Appendix C-13).

**Table 4.11: Wall post and Status update extraction test result summary**

| | | CacheBack v.3.7.5 | IEF v.4.3 | EnCase v.6.19 | Expected |
|---|---|---|---|---|---|
| Facebook | Firefox | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| **Rating** | | **0** (0%) | **0** (0%) | **0** (0%) | - |
| Twitter | Firefox | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 4 (80%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 4 (80%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| **Rating** | | **0** (0%) | **0** (0%) | **2** (40%) | - |
| LinkedIn | Firefox | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 4 (80%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 5 (100%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| **Rating** | | **0** (0%) | **0** (0%) | **2** (45%) | - |
| Google Plus | Firefox | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| **Rating** | | **0** (0%) | **0** (0%) | **0** (0%) | - |
| **Total Rating** | | **0** (0%) | **0** (0%) | **1** (20%) | |

Many wall post and status updates posted on SNSs were not identified in both the browser cache and pagefile.sys file. However, Encase found 4 LinkedIn status updates, 4 Twitter status updates, 3 Facebook status updates from the Systems volume information, and found 79 more status update from Unallocated space (See Appendix C-13).

#### 4.2.2.7 Comments and Reply analysis

Wall post comments, replies and their corresponding footprints can be found from browser cache file, pagefile.sys, the hibernation file, and unallocated space. This test case involved testing whether each tool could find comments and replies made on the 4 SNSs. Am extraction test was performed, and only EnCase was able to extract comments or replies made on SNSs.

**Table 4.12: Comments and Reply extraction test result summary**

| | | CacheBack v.3.7.5 | IEF v.4.3 | EnCase v.6.19 | Expected |
|---|---|---|---|---|---|
| Facebook | Firefox | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| **Rating** | | **0** (0%) | **0** (0%) | **0** (0%) | **-** |
| Twitter | Firefox | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| **Rating** | | **0** (0%) | **0** (0%) | **0** (0%) | **-** |
| LinkedIn | Firefox | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| **Rating** | | **0** (0%) | **0** (0%) | **0** (0%) | **-** |
| Google Plus | Firefox | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 5 (100%) | 5 |
| **Rating** | | **0** (0%) | **0** (0%) | **1** (25%) | - |
| **Total Rating** | | **0** (0%) | **0** (0%) | **1** (6.25%) | |

The author posted a status update “Jung Son Forensic investigation test post 01 (firefox)” on a SNS wall, pressed the “Like” button on Facebook, and then made a comment “Facebook comment – Firefox – 01” on the wall. The comment and reply

was not clearly identified on both Internet browser history or cache file. However, some part of the comment message "You like this Jung Son Linkedin Comment - Firefox - 01 3 minutes ago" from the user could be identified from unallocated space. EnCase extracted (overall 6.25%) comments and replies. Additionally, Encase found 20 Facebook comments, 20 Twitter comments, 19 LinkedIn comments and 20 Google plus comments on unallocated space as shown in Appendix C-14.

#### 4.2.2.8 Location information analysis

This test scenario involved testing the capability of extracting users' location information. This test case only applied to Facebook and the Google Plus site, as these two sites allow users to add their location information from a desktop computer. Only EnCase was able to find location information posted on SNSs (See Appendix C-12). Table 4.13 shows the test results:

**Table 4.13: Location information extraction test result summary.**

| | | CacheBack v.3.7.5 | IEF v.4.3 | EnCase v.6.19 | Expected |
|---|---|---|---|---|---|
| Facebook | Firefox | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 3 (60%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 5 (100%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 4 (80%) | 5 |
| **Rating** | | **0** (0%) | **0** (0%) | **2** (60%) | - |
| Google Plus | Firefox | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Chrome | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | Safari | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| | IE | 0 (0%) | 0 (0%) | 0 (0%) | 5 |
| **Rating** | | **0** (0%) | **0** (0%) | **0** (0%) | - |
| **Total Rating** | | **0** (0%) | **0** (0%) | **1** (30%) | |

#### 4.2.2.9 Facebook Chat Message analysis

Facebook chatting message extraction capabilities were tested with 3 extraction tools. Even though all 3 selected tools support Facebook chat extraction, only CacheBack and IEF were able to find chatting histories from the target machine (See Appendix C-3 and R).

**Table 4.14: Facebook chat extraction test result summary.**

| Evidence Location | CacheBack v.3.7.5 | IEF v.4.3 | EnCase v.6.19 | Expected |
|---|---|---|---|---|
| Temporary file | 0 | 0 | 0 | 20 |
| Unallocated clusters | 0 | 0 | 0 | |
| Pagefile.sys | 0 | 0 | 0 | |
| hiberfil.sys | 0 | 0 | 0 | |
| System volume information | 20 (100%) | 20 (100%) | 0 | |
| **Total Rating** | **3** (0%) | **3** (100%) | **0** (0%) | - |

#### 4.2.2.9.1 Facebook Chat details analysis

CacheBack's Recover My Chat (RMC) successfully identified detailed Facebook chatting artifacts. Information found with the chatting message include the Facebook profile ID, send and received message, from and to names and ID, and the chatting conducted time (See Appendix C-3).

**Table 4.15: Detailed Facebook chatting information extraction test result.**

| Functionality | CacheBack v.3.7.5 | IEF v.4.3 | EnCase v.6.19 | Expected |
|---|---|---|---|---|
| Sender's Details | 20 | 0 | 0 | 20 |
| Receiver's Detail | 20 | 0 | 0 | |
| Message Sent Time | 20 | 0 | 0 | |
| **Total Rating** | **3** (100%) | **0** (0%) | **0** (0%) | - |

Even though IEF was able to find 20 of 20 chatting messages from the target evidence image, IEF failed to show detailed information such as the sender or receiver's information or the message send and receive times.

Guidance software provides a free EnScript (Facebook Chat Parser) to help investigators to recover and report Facebook Chat artifacts. Two versions of Facebook Chat Parser (V1.4 and V2.1) have been used with EnCase to extract Facebook Chat artifacts from the target hard drive, however EnCase failed to extract any Facebook Chat artifacts from the target drive.

#### 4.2.2.10 Email analysis (Webmail and Outlook)

This test case involved testing whether the tool can extract SNS related email messages from either Google Webmail (Gmail) or Microsoft Outlook. Table 4.26 shows a summary of the performed testing result from the three tested tools. CacheBack failed to acquire any email messages, Internet Evidence Finder was able to acquire 10 of 10 Google Plus email messages sent from pagefile.sys file (see Appendix C-7), EnCase was able to successfully find all email messages (See Appendix C-11).

**Table 4.16: Email extraction test result summary**

| | **CacheBack v.3.7.5** | **IEF v.4.3** | **EnCase v.6.19** | **Expected** |
|---|---|---|---|---|
| Facebook | 0 (0%) | 0 (0%) | 10 (100%) | 10 |
| Twitter | 0 (0%) | 0 (0%) | 10 (100%) | 10 |
| LinkedIn | 0 (0%) | 1 (10%) | 10 (100%) | 10 |
| Google Plus | 0 (0%) | 10 (100%) | 10 (100%) | 10 |
| **Total Rating** | **0** (0%) | **1** (27.5%) | **3 (100%)** | |

#### 4.2.2.11 Repeatability and Reproducibility testing

International Organisation for Standardisation (ISO) defined repeatability as the closeness of agreement between independent test results under repeatability conditions that are as constant as possible (International Organization for Standardization, 1994). It is important to check whether tools tested in this research produced repeatable extraction results under same condition, where same condition means that nothing changed in testing environment except the time of the testing.

ISO also defined reproducibility as the closeness of agreement between independent test results under reproducibility conditions under which results are obtained with the same procedures on same testing scenarios, but in different testing equipment (ISO1994).

According to the National Institute of Standards and Technology, test results must be repeatable and reproducible as it is not possible to estimate experimental errors without them (NIST, 2001). Tools tested in this research must always acquire the same results, thus making a case result reproducible and reliable. To ensure this, all above 10 testing case scenarios were performed 3 times, with each selected tool in

order to observe the accuracy and consistency of the results. The same examiner took the testing with the same procedure in a same testing location. Table 4.17 shows how consistent the extraction result produced by three tested tools.

**Table 4.17: Repeatability and reproducibility test result summary**

| | **CacheBack v.3.7.5** | **IEF v.4.3** | **EnCase v.6.19** |
|---|---|---|---|
| 1. Web History | **3** (100% Match) | **3** (100% Match) | **3** (100% Match) |
| 2. Cache | **3** (100% Match) | **3** (100% Match) | **3** (100% Match) |
| 3. Cookies/Session | **3** (100% Match) | **3** (100% Match) | **3** (100% Match) |
| 4. Images | **3** (100% Match) | **3** (100% Match) | **3** (100% Match) |
| 5. Multimedia/Video | **3** (100% Match) | **3** (100% Match) | **3** (100% Match) |
| 6. Wall Post/Status update | **3** (100% Match) | **3** (100% Match) | **3** (100% Match) |
| 7. Comments/Reply | **3** (100% Match) | **3** (100% Match) | **3** (100% Match) |
| 8. Location | **3** (100% Match) | **3** (100% Match) | **3** (100% Match) |
| 9. Facebook Chat | **3** (100% Match) | **3** (100% Match) | **3** (100% Match) |
| 10. Emails | **3** (100% Match) | **3** (100% Match) | **3** (100% Match) |
| **Total Rating** | **3** (100%) | **3** (100%) | **3 (100%)** |

All three evidence extraction tools obtained the same results for the same testing environment and produced exactly same results on a 2 different investigation computers (tested with parallel Windows 7 on Mac OSX, Windows 7 on Dell laptop as an investigation computer).

## 4.3 RESEARCH ANALYSIS

This section summarises the result and explains the field findings performed in section 4.2. The field findings are reported with 11 different and relevant testing scenarios for extracting evidence from SNSs. Each test result is presented in a table summarising the extraction capabilities of the three selected evidence extraction tools. Each scenario is compared against the predefined expectations and rated based on the testing rating scale defined earlier in Table 4.16. The rating result “Below” indicates that the tool fell short of extracting enough evidence, Similarly, “Meet” indicates that the tool met the expectations, “Above” indicates that the tool exceeded expectations and “Miss” indicates that the tool did not find any evidence and therefore could not meet any expectations.

### 4.3.1 Analysis of the Testing Results

The testing results for each scenario presented in section 4.2 are analysed in this section. After a careful analysis of data obtained from the 4 main web browsers, the result shows that each browser saves the web browsing history, cache and cookies in their own native format and location. Browsing data may be found in different locations, according to the user's operating system, and version of the web browser used by the operator. Various techniques are used to identify the location of each browser's browsing footprint. Internet history, cache and cookies were found in C:\Users\<user profile> folder in the Windows 7 Operating system. Table 4.18 shows detailed location information where history, cache and cookies are located on 4 different browsers tested in this research.

**Table 4.18: Internet access history, cache, and cookie information stored on different Web Browsers**

| **Browser** | **Artifact** | **Folder Path** (from the User profile folder) | **Files** |
|---|---|---|---|
| Firefox 7.0.1 | History | \AppData\Roaming\Mozilla\Firefox\Profiles\<name>.default\ | places.sqlite |
| | Cache | \AppData\Local\Mozilla\Firefox\Profiles\<name>.default\Cache | All files |
| | Cookies | \AppData\Roaming\Mozilla\Firefox\Profiles\<name>.default\ | cookies.sqlite |
| Google Chrome 14.0 | History | \AppData\Local\Google\Chrome\User Data\Default\ | History |
| | Cache | \AppData\Local\Google\Chrome\User Data\Default\Cache | All files |
| | Cookies | \AppData\Local\Google\Chrome\User Data\Default\ | Cookies |
| Microsoft Internet Explorer 9 | History | \AppData\Local\Microsoft\Windows\History | All files |
| | Cache | \AppData\Local\Microsoft\Windows\Temporary Internet Files | All files |
| | Cookies | \AppData\Local\Microsoft\Windows\Temporary Internet Files | All files |
| Safari 5.1 | History | \AppData\Roaming\Apple Computer\Safari | History.plist |
| | Cache | \ AppData\Local\Apple Computer\Safari | Cache.db |
| | Cookies | \AppData\Roaming\Apple Computer\Safari\Cookies\ | Cookies.binary cookies |

The Internet access URL history of each browser used by the target computer has been analysed. The browser history contains the information for the date of last access, and number of visits, which can be useful for digital forensic investigation. Figure 4.2 - 4.5 shows history information saved on each browser.

| URL | First Visit Date | Last Visit Date | Visit Count |
|---|---|---|---|
| http://facebook.com/ | N / A | 4/10/2011 3:47:35 ... | 1 |
| http://gmail.com/ | N / A | 4/10/2011 8:33:11 ... | 1 |
| http://linkedin.com/ | N / A | 4/10/2011 5:57:42 ... | 1 |
| http://mail.google.com/mail/ | N / A | 4/10/2011 8:33:11 ... | 1 |

**Figure 4.2: Firefox Internet history**

| URL | Title | Visited On |
|---|---|---|
| http://facebook.com/ | Facebook | 4/10/2011 3:59:37 |
| http://facebook.com/ | Facebook | 4/10/2011 5:41:34 |
| http://facebook.com/ | Facebook | 4/10/2011 6:20:49 |

**Figure 4.3: Chrome Internet history**

*URL History Explorer*

| Last Visited | Title | URL | Last Updated | Expires |
|---|---|---|---|---|
| 4/10/2011 9:00:46 p.m. | | file:///E:/Browser%20Testing%20Records/IE/iecookie... | 4/10/2011 9:00:46 p.... | 30/10/2011 8:53:36 |
| 4/10/2011 8:58:04 p.m. | | file:///E:/Browser%20Testing%20Records/IE/iecache... | 4/10/2011 8:58:04 p.... | 30/10/2011 8:58:04 |
| 4/10/2011 8:57:28 p.m. | | file:///E:/Browser%20Testing%20Records/IE/iecache... | 4/10/2011 8:57:28 p.... | 30/10/2011 8:57:28 |

**Figure 4.4: Internet Explorer Internet history**

| | | |
|---|---|---|
| Edit Profile \| LinkedIn | Last Visited Today | http://www.linkedin.com/profile/edit?trk=hb_tab_pro_top |
| Twitter / Home | Last Visited Today | https://twitter.com/sessions?phx=1 |
| Twitter | Last Visited Today | http://twitter.com/ |
| Welcome to Faceboo... Up or Learn More | Last Visited Today | http://www.facebook.com/ |
| Twitter | Last Visited Today | http://twitter.com/jung921/status/121068310531018752/photo/1/large |
| (no title) | Last Visited Today | http://upload.twitter.com/1/statuses/update_with_media.iframe |
| Twitter | Last Visited Today | http://twitter.com/jung921/status/121068041848102912/photo/1/large |
| Twitter | Last Visited Today | http://twitter.com/jung921/status/121067778559062016/photo/1/large |
| Twitter | Last Visited Today | http://twitter.com/jung921/status/121067598640189440/photo/1/large |
| Twitter | Last Visited Today | http://twitter.com/jung921/status/121067399079395328/photo/1/large |

**Figure 4.5: Safari Internet history**

Analysis of Internet history from each browser shows that searching by relevant and specific keywords can trace the user activities taken online.

The cache file is a component of the browser that stores visited website files, so that the next time the user visits the same website, user will not have to download the same graphics and web pages again (Jones, 2003). Locations of where each browser stores history, cache and cookies have also been identified. It is clear that all

four browsers are using the cache to improve the speed of user's web site browsing experience. Analysis of cache information shows that single keyword string may miss the information from SNSs. For example, Facebook access information is saved from either facebook.com or fbcdn.net. Table 4.19 describes the relevant keywords used to search cache files from the SNSs.

**Table 4.19: Keywords in SNSs**

| SNSs | Keywords | Sample cached URL |
|---|---|---|
| Facebook | Facebook | http://www.facebook.com/images/fb_icon_50x50.png |
| | fbcdn.net | http://static.ak.fbcdn.net/rsrc.php/v1/yb/r/GsNJNwuI-UM.gif |
| Twitter | Twitter | http://twitter.com/images/spinner.gif |
| | twimg | http://p.twimg.com/Aa4chKtCAAADSEk.jpg |
| | http://t.co | http://t.co/JbufLIkB → equivalent to http://twitter.com/#!/jung921/status/121065216971776000/photo/1 |
| LinkedIn | LinkedIn | http://www.linkedin.com/share?viewLink=&sid=s620543287&url=http%3A%2F%2Fwww%2Ewebconcept%2Eco%2Enz%2Flinkedin%2Flinkedin-firefox-04%2Ejpg&urlhash=qeH-&pk=nhome-chron-split-realtime-updates&pp=1&poster=22549911&uid=5526837165637513216&trk=NUS_UNIU_SHARE-pic |
| Google Chrome | Plus.google | https://plus.google.com/_/photos/lightbox/?uname=106412413750736394738&returnmeta=true&view=PPQ&photoid=5659485694729068674&returnexif=true&aname=2011100305&returnshapes=true&returncomments=true&filter=true&returnalbum=true |

Website cookie information has been analysed accordingly with keywords identified in the Table 4.19. A summary of the testing results for each case is divided for each tool and shows the test ratings for each case scenario.

#### 4.3.1.1 CacheBack Matrix of Results

**Table 4.20: Summary of CacheBack capability results**

| Scenario | Cacheback v3.7.5 Results | | | | Rating | Result |
|---|---|---|---|---|---|---|
| | Facebook | Twitter | LinkedIn | Google Plus | | |
| 1. Web History | **2** (37.5%) | **3** (65.5%) | **3** (71.5%) | **2** (51.25%) | **2** (56%) | **Meet** |
| 2. Cache | **2** (37%) | **1** (30.75%) | **1** (27.75%) | **1** (17%) | **1** (28%) | **Below** |
| 3. Cookies/Session | **3** (75%) | **2** (58.25%) | **3** (75%) | **3** (75%) | **3** (70%) | **Above** |
| 4. Images | **2** (40%) | **2** (35%) | **1** (25%) | **1** (25%) | **2** (31%) | **Meet** |
| 5. Multimedia/Video | **0** (0%) | - | - | **1** (30%) | **1** (15%) | **Below** |
| 6. Wall Post/Status update | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) | **Miss** |
| 7. Comments/Reply | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) | **Miss** |
| 8. Location | **0** (0%) | - | - | **0** (0%) | **0** (0%) | **Miss** |
| 9. Facebook Chat | **3** (100%) | - | - | - | **3** (100%) | **Above** |
| 10. Emails | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) | **Miss** |
| 11. Repeatability | **3** (100%) | **3** (100%) | **3** (100%) | **3** (100%) | **3** (100%) | **Above** |

#### 4.3.1.2 Internet Evidence Finder Matrix of Results

**Table 4.21: Summary of Internet Evidence Finder capability results**

| Scenario | Internet Evidence Finder v4.3 Results | | | | Rating | Result |
|---|---|---|---|---|---|---|
| | Facebook | Twitter | LinkedIn | Google Plus | | |
| 1. Web History | **1** (21.5%) | **1** (16%) | **1** (27%) | **1** (11%) | **1** (19%) | **Below** |
| 2. Cache | **1** (0.25%) | **1** (0.8%) | **1** (0.7%) | **1** (0.85%) | **1** (0.65%) | **Below** |
| 3. Cookies/Session | **0** (0%) | **0** (0%) | **0** (0%) | **1** (25%) | **1** (6%) | **Below** |
| 4. Images | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) | **Miss** |
| 5. Multimedia/Video | **0** (0%) | - | - | **0** (0%) | **0** (0%) | **Miss** |
| 6. Wall Post/Status update | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) | **Miss** |
| 7. Comments/Reply | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) | **0** (0%) | **Miss** |
| 8. Location | **0** (0%) | - | - | **0** (0%) | **0** (0%) | **Miss** |
| 9. Facebook Chat | **3** (100%) | - | - | - | **3** (100%) | **Above** |
| 10. Emails | **0** (0%) | **0** (0%) | **1** (10%) | **3** (100%) | **1** (27.5%) | **Below** |
| 11. Repeatability | **3** (100%) | **3** (100%) | **3** (100%) | **3** (100%) | **3** (100%) | **Above** |

#### 4.3.1.3 EnCase Matrix of Results

**Table 4.22: Summary of EnCase capability results**

| Scenario | EnCase v 6.19 Results | | | | Rating | Result |
|---|---|---|---|---|---|---|
| | Facebook | Twitter | LinkedIn | Google Plus | | |
| 1. Web History | **1** (25%) | **1** (25%) | **1** (25%) | **1** (25%) | **1** (25%) | **Below** |
| 2. Cache | **2** (33%) | **2** (39%) | **2** (34%) | **1** (25%) | **2** (33%) | **Meet** |
| 3. Cookies/Session | **1** (25%) | **1** (25%) | **1** (25%) | **1** (25%) | **1** (25%) | **Below** |
| 4. Images | **0** (0%) | **0** (0%) | **1** (25%) | **3** (75%) | **1** (25%) | **Below** |
| 5. Multimedia/Video | **0** (0%) | - | - | **0** (0%) | **0** (0%) | **Miss** |
| 6. Wall Post/Status update | **0** (0%) | **2** (40%) | **2** (45%) | **0** (0%) | **1** (21%) | **Below** |
| 7. Comments/Reply | **0** (0%) | **0** (0%) | **0** (0%) | **1** (25%) | **1** (6.2%) | **Below** |
| 8. Location | **2** (60%) | - | - | **0** (0%) | **1** (30%) | **Below** |
| 9. Facebook Chat | **0** (0%) | - | - | - | **0** (0%) | **Miss** |
| 10. Emails | **3** (100%) | **3** (100%) | **3** (100%) | **3** (100%) | **3** (100%) | **Above** |
| 11. Repeatability | **3** (100%) | **3** (100%) | **3** (100%) | **3** (100%) | **3** (100%) | **Above** |

According to the results presented in Table 4.20 – 4.22, CacheBack rated 5 misses, 2 belows, 2 meets, and 2 aboves, IEF rated 5 misses, 4 belows, 0 meets, and 2 aboves, EnCase rated 2 misses, 6 belows, 1 meet, and 2 aboves. Even though there were not significant differences between each tool, CacheBack achieved the highest expected test result in most the cases, and IEF rated lowest rating in most of cases event though IEF was able to find all Facebook chatting records.

## 4.4 PRESENTATION OF FINDINGS

A summary of the field-test findings from section 4.2, and analysis results from section 4.3 are presented in the following section. The purpose of this section is to interpret the field-testing results from each of the 11-testing scenarios and to convey the results in a visual manner. The evaluation results of the three tools are presented in table 4.23. Section 4.4.2 represents the individual field-testing results in two bar charts, one of which allows for a more granular examination of the underlying data. The final section, section 4.4.4, presents the comparison results from the test scenario analysis. The three selected tools are compared and graphed to display the level of capability in 11 scenarios.

### 4.4.1 Test scenario extraction result summary

This section presents a detailed summary of analysis of results in a table, and visual summaries in graphical charts. A summary of the field analysis of test results in section 4.3 is outlined and reported in Table 4.23. Table 4.35 shows the best result in each test scenario, and each case represented in a different colour. Following section 4.4.2.1 – 4.4.2.11 will explain this table with visual summaries. In the final section, 4.4.3, the scenario analysis result is compared and presented in four different chart formats (Figure 4.25 – 4.26) to display and compare the level of capability. Table 4.23 represents the test results in each tool by each testing scenario.

**Table 4.23: Summary of the field findings**

| Scenario | CacheBack | | IEF | | EnCase | |
|---|---|---|---|---|---|---|
| | Score | Rating | Score | Rating | Score | Rating |
| Web History | 56% | 2 | 19% | 1 | 25% | 1 |
| Cache | 28% | 1 | 0.65% | 1 | 33% | 2 |
| Cookies and Session | 70% | 3 | 6% | 1 | 25% | 1 |
| Images | 31% | 2 | 0% | 0 | 25% | 1 |
| Videos | 15% | 1 | 0% | 0 | 0% | 0 |
| Wall Post and Status update | 0% | 0 | 0% | 0 | 21% | 1 |
| Comments and Reply | 0% | 0 | 0% | 0 | 6.2% | 1 |
| Location | 0% | 0 | 0% | 0 | 30% | 1 |
| Facebook Chat | 100% | 3 | 100% | 3 | 0% | 0 |
| Emails | 0% | 0 | 27.5% | 1 | 100% | 3 |
| Repeatability | 100% | 3 | 100% | 3 | 100% | 3 |
| **Total - Weighted** | **36%** | **1.36** | **23%** | **0.91** | **33%** | **1.27** |
| **Total best results** | **6** | | **2** | | **6** | |
| **Ranking** | **1st** | | **3rd** | | **2nd** | |

### 4.4.2 Test Scenario Results

Section 4.4.2.1 to 4.4.2.11 represent the individual testing results of the tools CacheBack, IEF, and EnCase Forensics, in the test scenarios that were applied to them. Each section shows two bar charts. One representing extraction hit-rate by tool, and one representing hit-rate by web browser type.

#### 4.4.2.1 Test Scenario One: Web History Extraction Capability

Figure 4.6 shows the web history extraction capability for the three extraction tools. CacheBack found 37.5% of web histories from Facebook, 65.5% from Twitter, 71.5% from LinkedIn, and 51.25% from the Google Plus website. Average 56% of web history lists have been extracted from 4 SNSs that have been tested with.

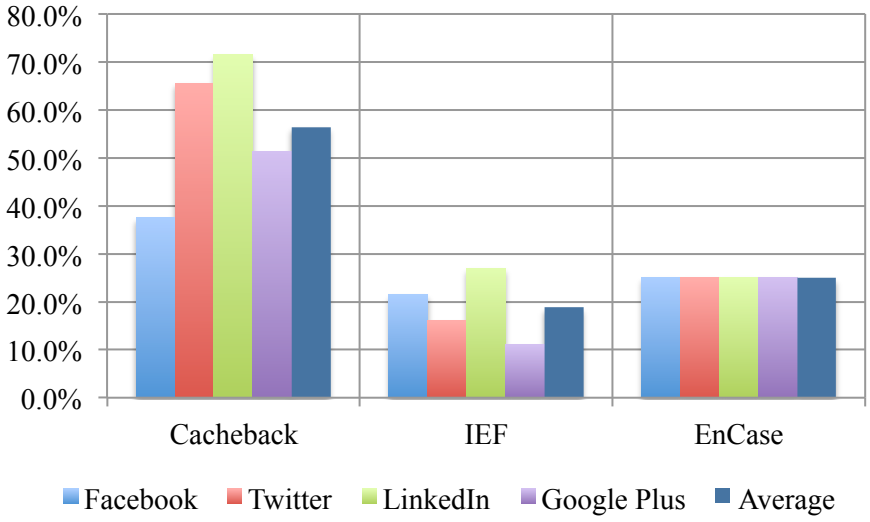



**Figure 4.6: Web history analysis hit-rate by tool**

Although figure 4.6 shows extraction hit-rate by tool, more detail can be gleaned from figure 4.7 below, which shows actual extraction results by browser type.

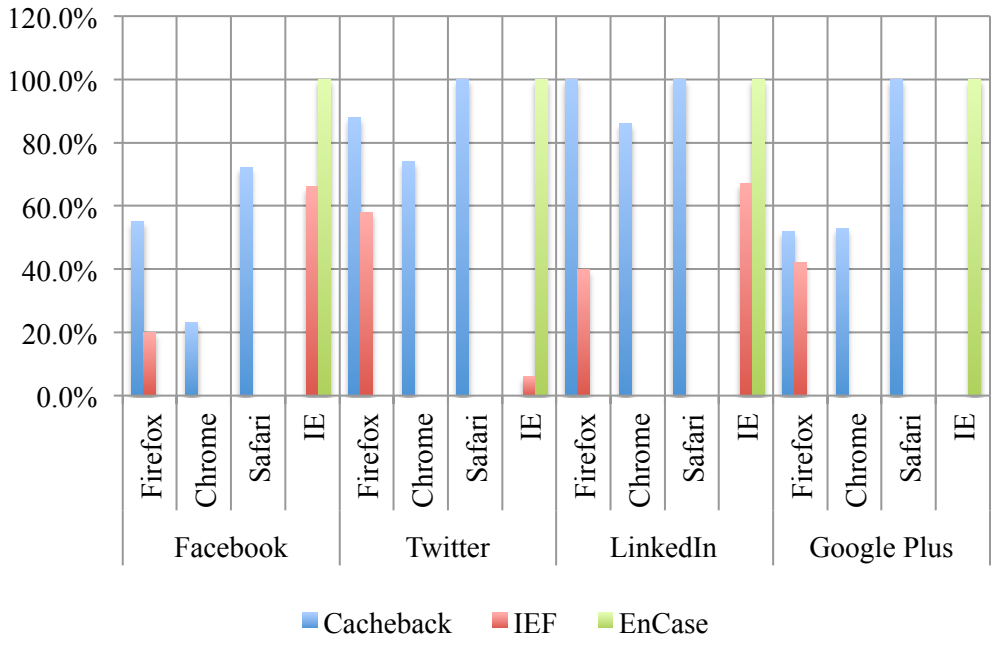



**Figure 4.7: Web history analysis results by browser type**

**CacheBack**

CacheBack consistently found web histories from 4 different SNSs. Cacheback was lacking in extraction capability from Internet Explorer.

**IEF**

IEF was able to find Internet histories from all 4 SNSs. However, IEF was not able to identify any Internet history from Google Chrome or Safari web browsers.

**EnCase**

EnCase Forensics was able to find Internet history records only from Internet Explorer.

#### 4.4.2.2 Test Scenario Two: Internet Cache Extraction Capability

Figure 4.8 is a comparison chart of Internet cache analysis results obtained from the three evaluated tools. EnCase achieved the highest rate at 33%. The summary of test results is as follows:

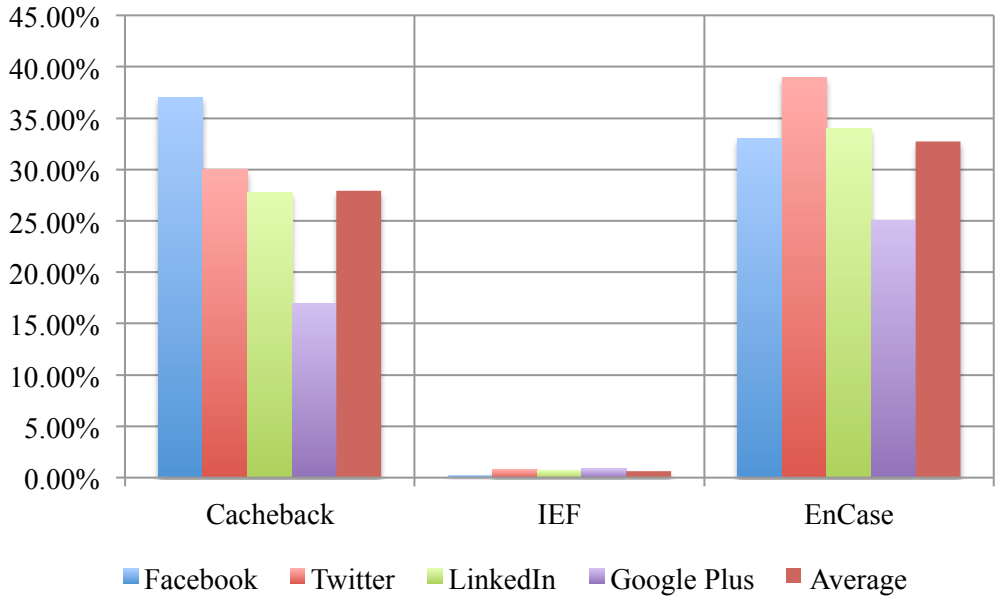



**Figure 4.8: Internet cache analysis hit-rate by tool**

Both CacheBack and EnCase extracted Internet Cache from all 4 SNSs. CacheBack extracted 28% of *targeted* cache data values, IEF extracted 0.65% and EnCase extracted 33% of *targeted* Internet Cache values. Figure 4.9 below shows which web browser yielded Cache data for each tool.

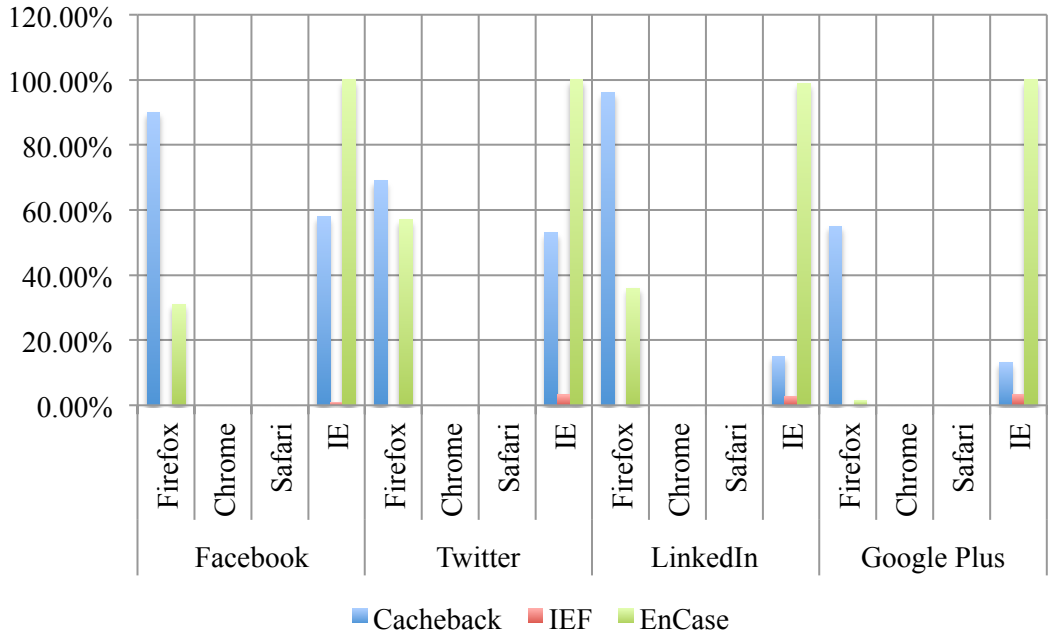



**Figure 4.9: Internet cache analysis results by browser type**

**CacheBack**

CacheBack consistently found evidence of the Internet Cache from 4 SNSs. CacheBack displays strength in extracting cache items from Firefox and Internet Explorer but lacks in extracting cache items from either Chrome or Safari web browsers.

**IEF**

While IEF does not provide extracted cache items from SNSs, IEF found a few Cache items from Internet Explorer. IEF was not able to extract any cache items from other web browsers.

**EnCase**

Like CacheBack extraction results, EnCase also consistently found a number of cache items across all SNSs. EnCase results indicated that EnCase has strength in extracting Cache items from Internet Explorer, but lacks strength in other web browsers like Firefox, and is not capable of extracting cache from Chrome or Safari browsers.

#### 4.4.2.3 Test Scenario Three: Cookies and Session Extraction Capability

CacheBack successfully acquired Cookies and Session information from 4 different browsers. IEF was not able to find any Cookie information and EnCase found 25% of cookie information that are related to 4 SNSs that were tested. The summary of test results is as follows:

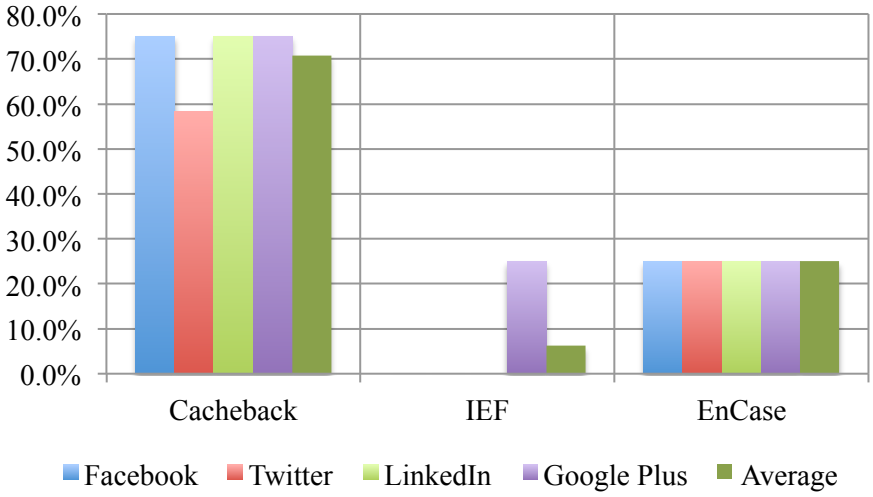



**Figure 4.10: Cookies and session analysis hit-rate by tool**

CacheBack extracted 70% of targeted cookie data from 4 SNSs. EnCase extracted 25% of targeted cookie data followed by IEF 6%. Figure 4.11 shows that both CacheBack and EnCase consistently extracted cookies from Mozilla Firefox, Google Chrome, and Microsoft Internet Explorer. Only EnCase was able to extract Google plus cookie artifacts from Apple Safari web browser.

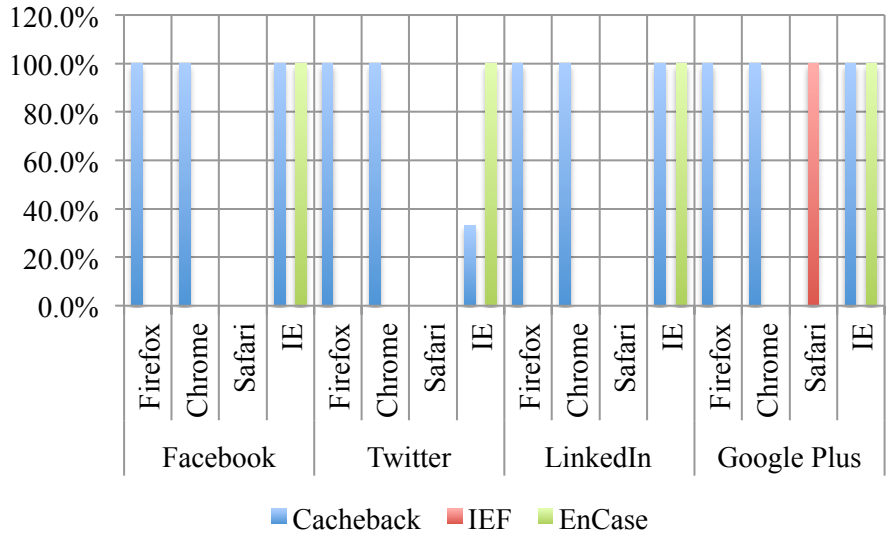



**Figure 4.11: Cookies and session analysis result by browser type**

**CacheBack**

CacheBack rated highest in extracting cookies. CacheBack again, showed consistency in finding cookie items from all 4 SNSs. CacheBack was not able to find any cookie information from the Safari web browser.

**IEF**

While IEF found some cookie information from the Google Plus website, it was unsuccessful in extracting any cookie items for the other 3 SNSs. IEF identified 100% of the Google plus cookie items from the Safari web browser.

**EnCase**

Even though EnCase consistently found some cookie items from all 4 SNSs, EnCase was not able to extract as many cookie items as CacheBack. Figure 4.11 shows that EnCase has strength in extracting cookie items from Internet Explorer but not the other 3 web browsers.

#### 4.4.2.4 Test Scenario Four: Photo Extraction Capability

Both CacheBack and EnCase were able to extract some photos, they are rated as 1 - "Below". IEF does not support extracting images from SNSs and therefore, it is rated as 0 – "Missed". The summary of test results is as follows:

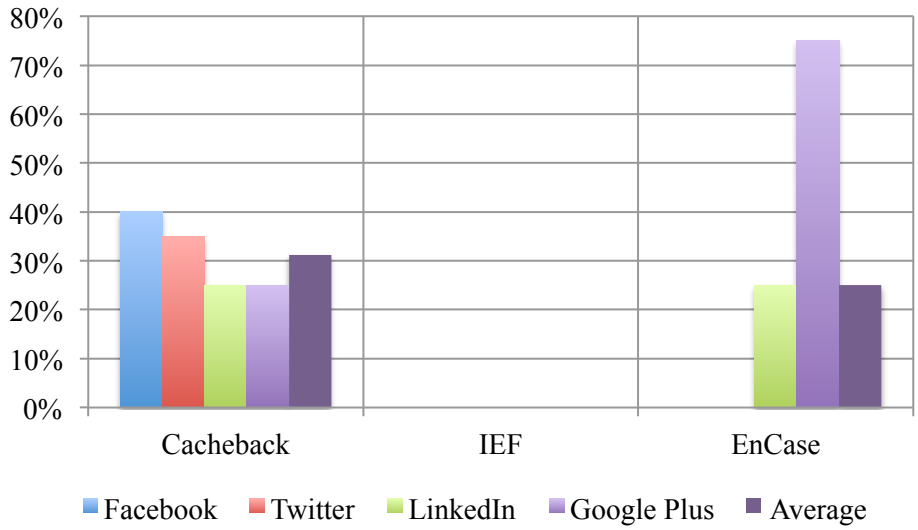



**Figure 4.12: Image analysis hit-rate by tool**

Figure 4.13 below, shows that both CacheBack and EnCase extracted image artifacts successfully from Mozilla Firefox and Microsoft Internet Explorer.

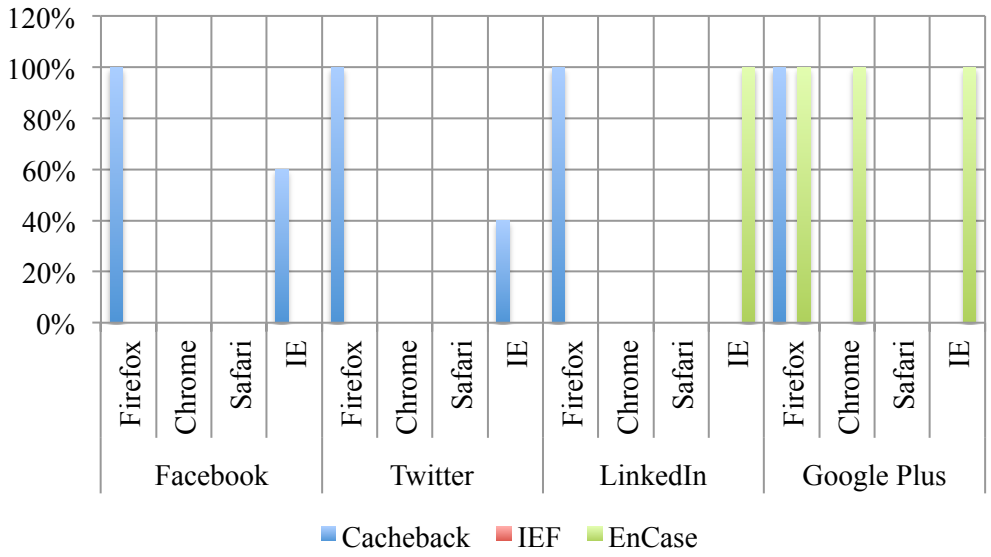



**Figure 4.13: Image analysis result by browser type**

**CacheBack**

CacheBack found images from all 4 SNSs, mostly images extracted from Firefox and Internet Explorer. CacheBack was not able to extract any images from Chrome or Safari web browsers in this test.

**IEF**

IEF does not support extraction of images and therefore IEF rated as 0 (No images extracted)

**EnCase**

EnCase found a few images mainly from the Google Plus website, EnCase found 100% of generated images posted in the LinkedIn website from Internet Explorer and found 100% of generated images posted in Google Plus from Firefox, Chrome and Internet Explorer.

#### 4.4.2.5 Test Scenario Five: Video Extraction Capability

Only CacheBack was able to extract video items posted on the Google Plus website (15%). Neither IEF nor EnCase were able to find any video items from Facebook or Google Plus website.

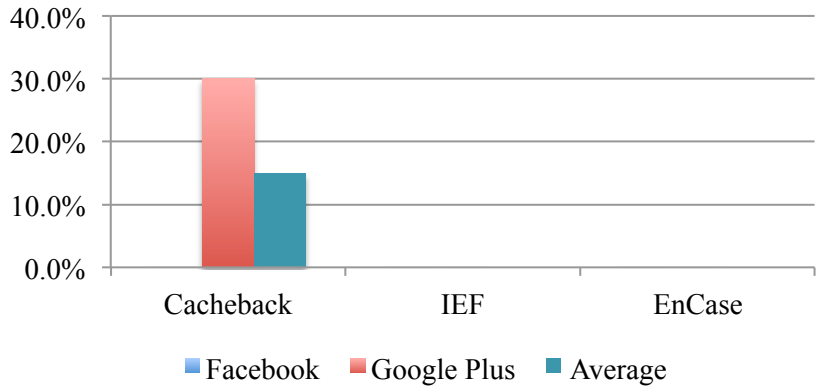



**Figure 4.14: Video analysis hit-rate by tool**

Although figure 4.14 shows that CacheBack was able to extract video posted on Facebook and Google Plus websites, the extraction result is only obtained from Mozilla Firefox and Microsoft Internet Explorer. CacheBack was not able to extract video items posted on SNSs from Google Chrome or Safari in this particular test scenario.

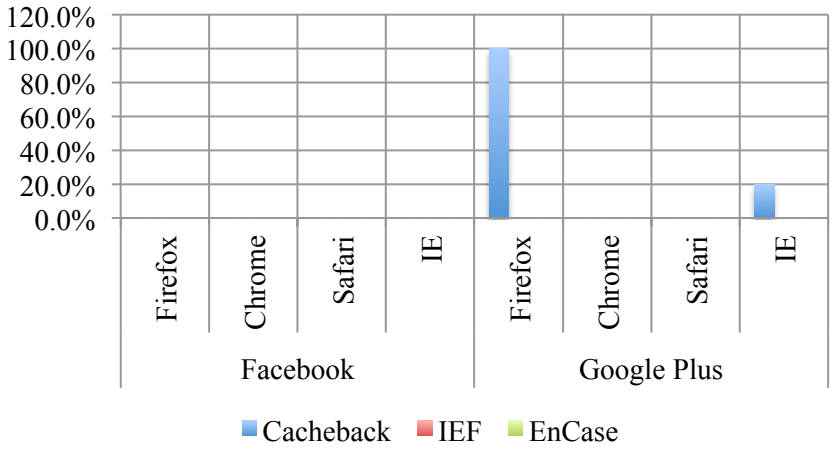



**Figure 4.15: Video analysis result by browser type**

**CacheBack**

CacheBack identified 100% of video items posted on the Google plus website user posted via Firefox web browser. CacheBack provides a list of thumbnails in the gallery tab. CacheBack was unable to extract any video posted on Facebook.

**IEF**

IEF does not support extraction of videos posted on SNSs.

**EnCase**

EnCase was not able to extract any videos posted on SNSs.

#### 4.4.2.6 Test Scenario Six: Wall post and Status update Extraction Capability

EnCase rated highest on extracting wall post and status updates posted on SNSs with 20%. A summary of test results is as follows:

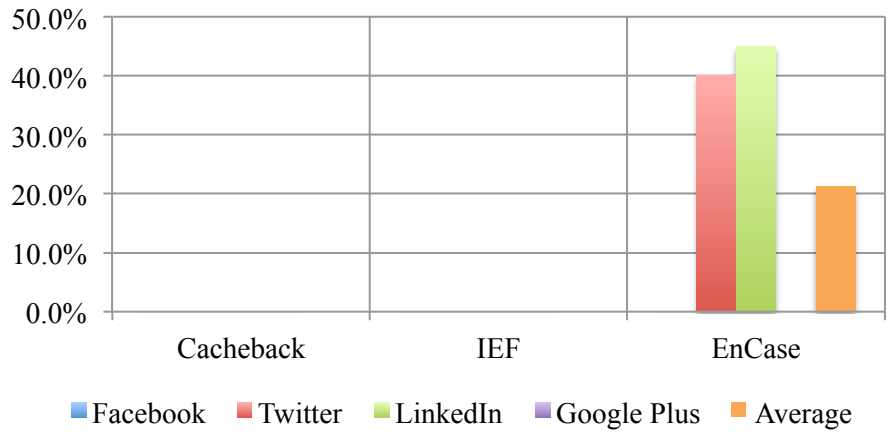



**Figure 4.16: Wall post and status update analysis hit-rate by tool**

Figure 4.17 shows test results for each tool, with more detail showing which browser the artifacts have been extracted from. EnCase extracted wall post and status update information from both Google Chrome and Apple Safari web browsers, but was unable to extract wall post or status update posts from Firefox and Microsoft IE.

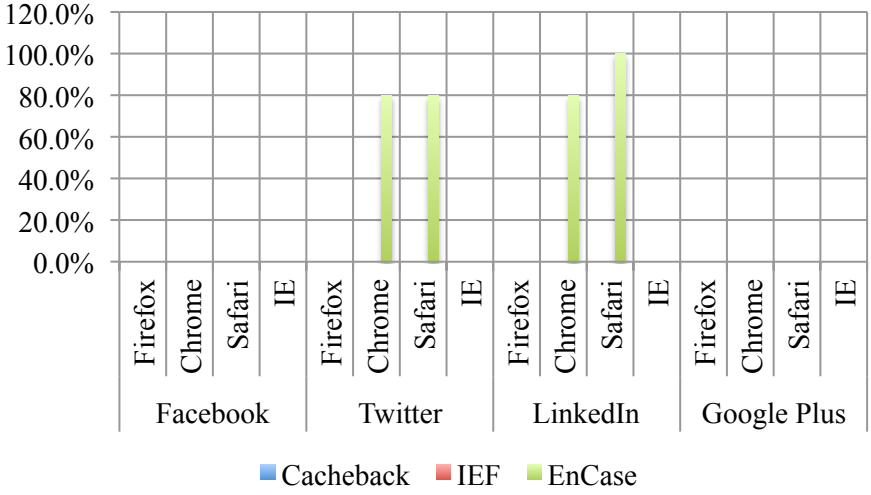



**Figure 4.17: Wall post and status update analysis result by browser type**

**CacheBack**

Even though CacheBack claims to be able to extract 'status update' and 'wall post' extraction, CacheBack was unsuccessful in extracting any status update information.

**IEF**

IEF's official website states that it can extract Status updates from Facebook and Twitter (JAD Software, 2011b), but was unable to extract any status update posted on SNSs.

**EnCase**

Only EnCase was able to extract a few status updates posted on the Twitter and LinkedIn sites. EnCase identified status update text strings from Chrome and Safari web browsers.

#### 4.4.2.7 Test Scenario Seven: Comments and Reply Extraction Capability

None of the extraction tools are able to extract any comments and replies posted on SNSs. Only EnCase found a few matching data points from the keyword search, and classifies as rating '1'. A summary of test results is as follows:

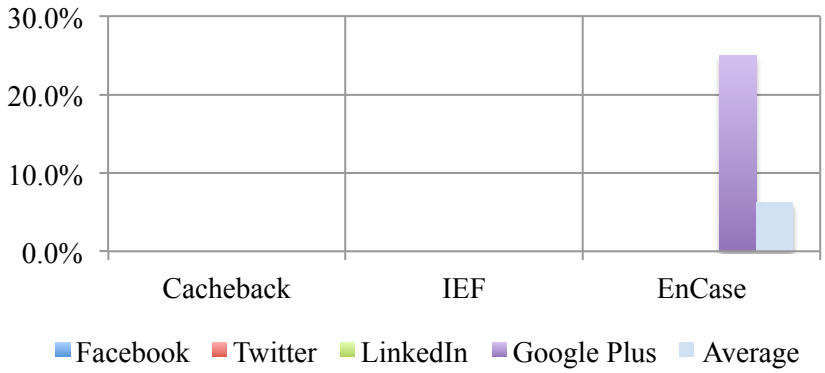



**Figure 4.18: Comments and reply analysis hit-rate by tool**

All comments and replies extracted from EnCase were extracted from Microsoft Internet Explorer.

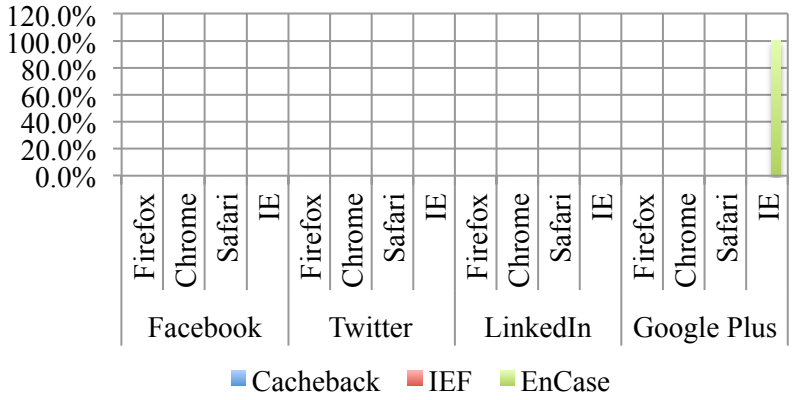



**Figure 4.19: Comments and reply analysis result by browser type**

**CacheBack**

CacheBack was unsuccessful in extracting any comment and reply items posted on SNSs.

**IEF**

IEF was unsuccessful in extracting any comment and reply items posted on SNSs.

**EnCase**

EnCase was able to find 5 of 5 comment items posted on the Google Plus website. Identified comment items were found from Internet Explorer. EnCase was unsuccessful in extracting comment and reply items from other SNSs.

#### 4.4.2.8 Test Scenario Eight: Location Information Extraction Capability

This test case only represents the extraction analysis result from Facebook and the Google Plus site, as only Facebook and Google Plus allows user to add their location information from a desktop computer. The results from Figure 4.20 indicate that both CacheBack and IEF were not able to extract any location information posted on SNSs. Keyword search from EnCase Forensic identified 30% location match. A summary of testing results is as follows:

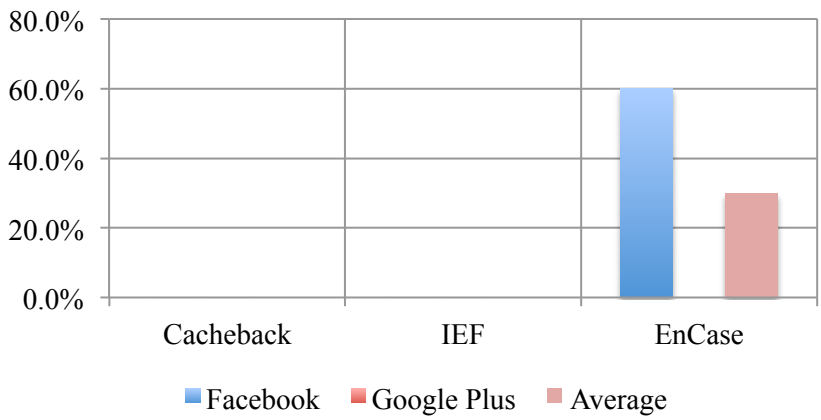



**Figure 4.20: Location analysis hit-rate by tool**

EnCase keyword string search acquired 30% of the known to exist targeted location information posted on Facebook. As the author knows the baseline of data, it was possible to perform keyword searches within EnCase. However, it would be unrealistic to perform keyword searches to extract location information without having an automated process within the tool. Location information was extracted from Google Chrome, Apple Safari, and Microsoft IE.

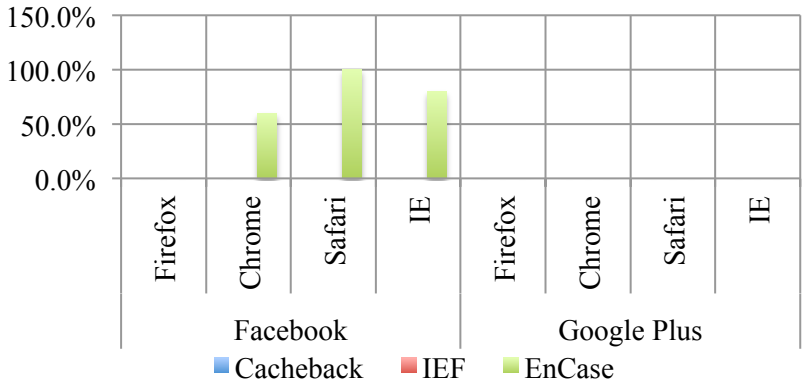



**Figure 4.21: Location analysis result by browser type**

**CacheBack**

CacheBack failed to acquire location information from any of the 4 SNSs.

**IEF**

IEF also failed to acquire location information from any of the 4 SNSs.

**EnCase**

All location information found from EnCase is shown in Figure 4.21. Location information posted on Facebook was found from Chrome, Safari and Internet Explorer. EnCase was not able to extract any location information posted on Facebook via the Firefox browser, and was not able to extract any location information from Google Plus.

#### 4.4.2.9 Test Scenario Nine: Facebook Chat Extraction Capability

The three evidence extraction tools were used to examine the artifacts left by the web browser during Facebook chat sessions. Both CacheBack and IEF successfully extracted Facebook chat messages from the 'evidence' target hard drive, EnCase failed to extract any of the Facebook chat messages. A summary of testing results is as follows:

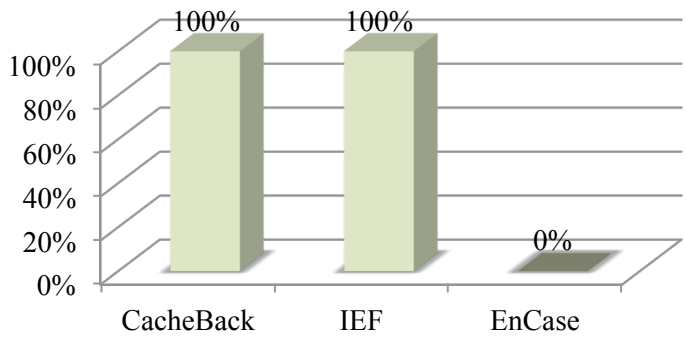



**Figure 4.22: Facebook chat history result**

**CacheBack**

CacheBack not only successfully extracted 20 of 20 Facebook chat messages from systems volume information, but also found information such as sender and receivers details as well as time of the chat.

**IEF**

IEF found 20 of 20 chat messages from system volume information. However IEF failed to extract detailed chatting records such as sender and receiver's details or message sent and received time.

**EnCase**

In order to examine the Facebook artifacts left behind from the chatting session, EnScript calls the Facebook Chat Parser (version 1.4 and 2.1 provided by EnCase). However, EnCase failed to extract any chat message from Facebook using the two versions of EnScript.

#### 4.4.2.10 Test Scenario Ten: Email Extraction Capability

Encase achieved the highest extraction result in email extraction. A summary of test results is as follows:

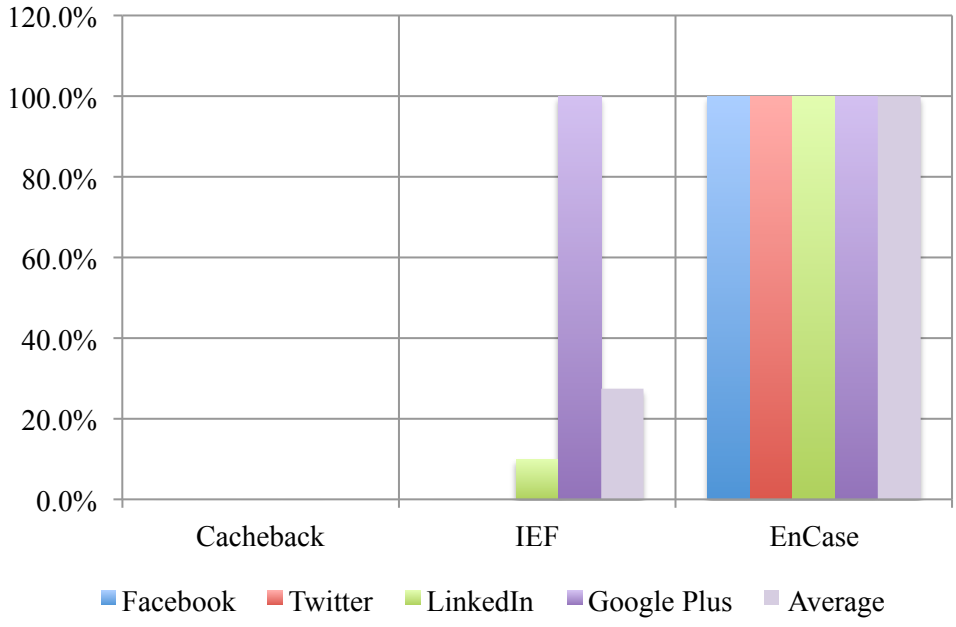



**Figure 4.23: Email analysis results**

**CacheBack**

CacheBack failed to extract any email messages from SNSs.

**IEF**

IEF found 10 of 10 email messages received from Google Plus and 1 of 10 email message received from the LinkedIn website. IEF recovered Gmail email fragments left behind in pagefile.sys file. Extracted record includes, sender name, address, subject, and first segment of the body of the email message. Appendix C-8 shows sample email message extracted from IEF.

**EnCase**

EnCase successfully extracted all emails messages from all 4 SNSs. The email search function from EnCase located email files and shows the findings in the records tab within EnCase. Appendix C-11 shows sample email message extracted from EnCase.

#### 4.4.2.11 Test Scenario Eleven: Repeatability and Reproducibility

Each of the three tools has been tested 3 times to verify that each tool can obtain a consistent result using the same evidence disk scan method provided. These tests have been performed with 2 different investigation machines described in the Section 4.2.1 to confirm the same test result can be obtained from different testing environments.

Testing results shows that the three evidence extraction tools produced test result in a forensically sound manner and therefore can be admissible as electronic evidence.

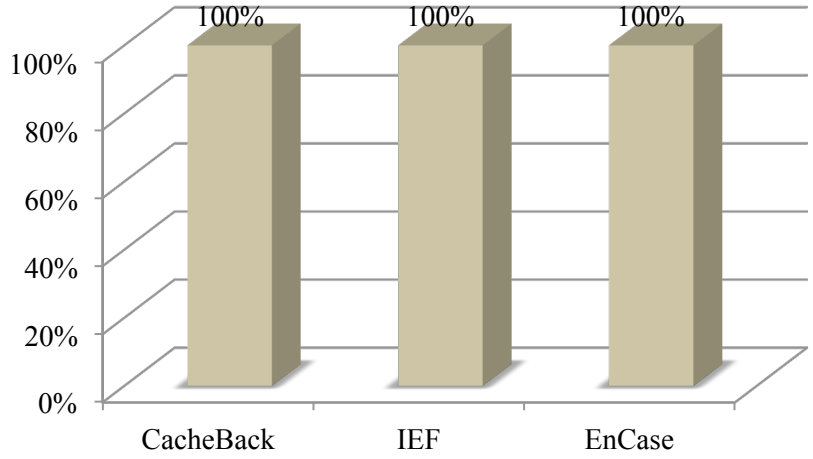



**Figure 4.24: Repeatability and reproducibility test result**

### 4.4.3 Test Scenario extraction result summary

Figure 4.25 compares the number of files extracted by each extraction tool in one table, which summarises the result presented in section 4.4.1 to 4.4.11.

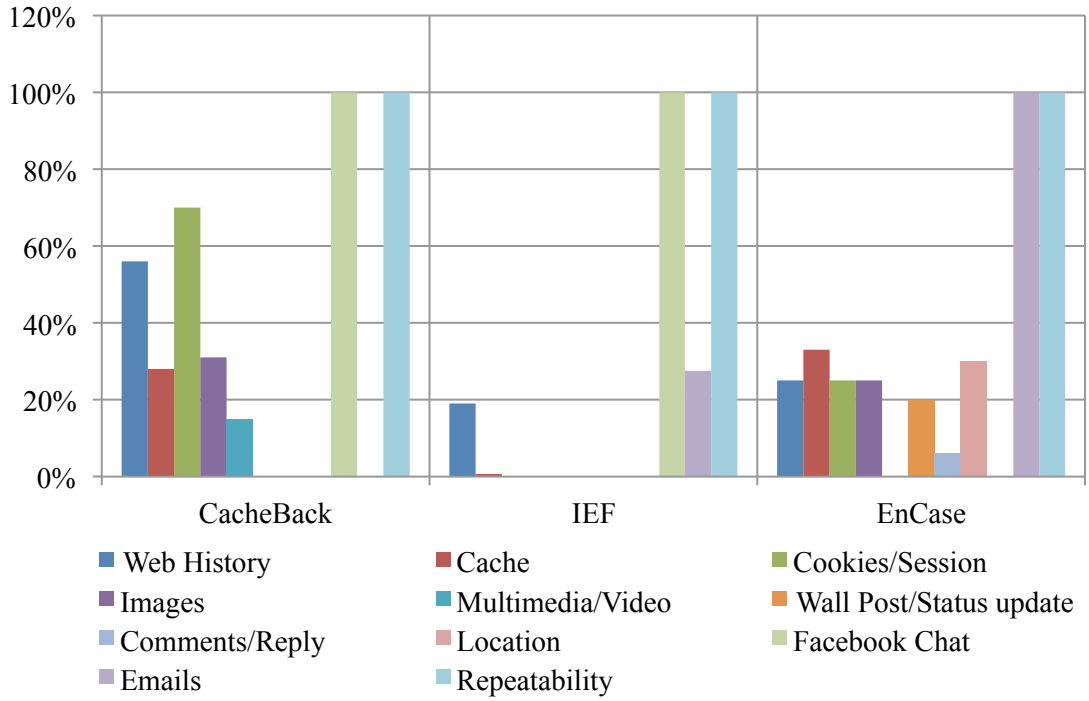



**Figure 4.25: Evidence extraction tool capabilities comparison**

### 4.4.4 Comparison of extraction tools

Eleven test scenarios were selected to compare the three extraction tools evaluated in this research. The ratings for all three tools have been plotted on Radar-chart graph (Figure 4.26) to help the reader interpret the test result easily. The range from 0 (Miss) to 3 (Above) ratings is shown and compared in the two charts. Several trends have been identified based on the comparison results. For example, CacheBack consistently achieved high ratings on web history, cookies, images, multimedia, and Facebook chatting extraction, EnCase achieved high ratings on extracting cache, wall post, comments, location, and emails. Internet Evidence Finder only achieved high ratings on Facebook chatting extraction. The final testing scenario indicates that all of three tested extraction tools are forensically sound in extracting evidence from SNSs as they all achieved 100% in repeatability and reproducibility testing.

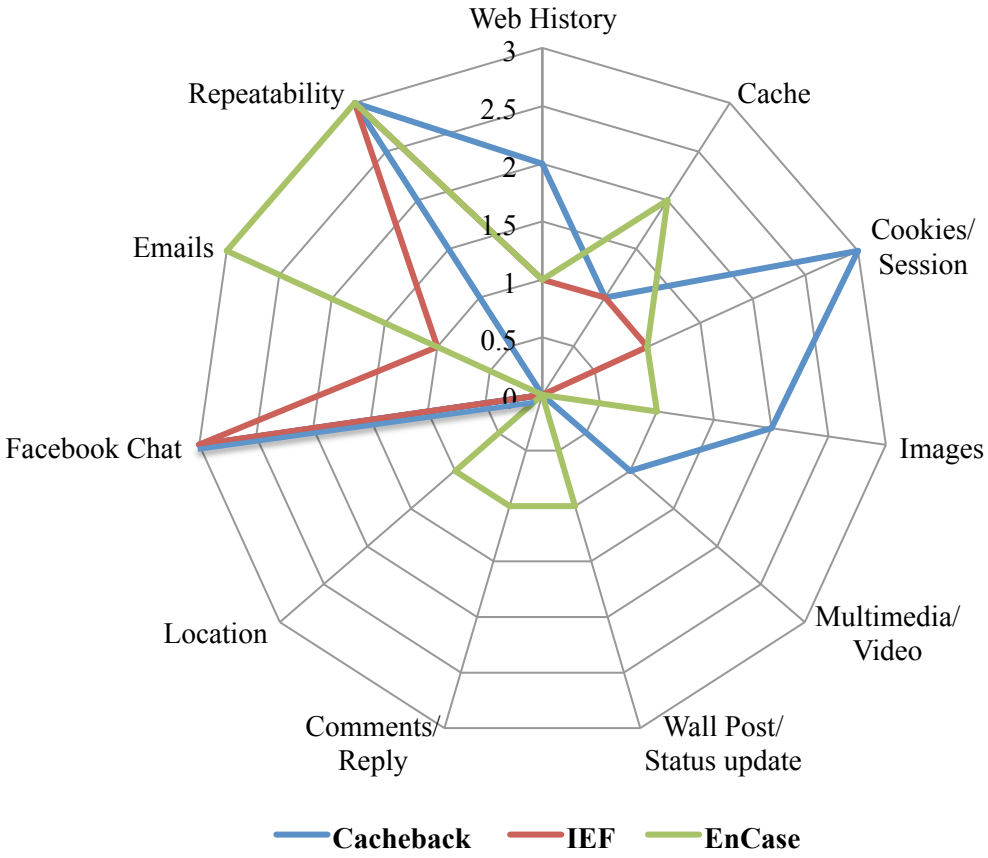



**Figure 4.26: Analysis of field finding result summary (Radar Chart)**

## 4.5 CONCLUSION

Chapter 4 has reported the field findings, analysis of research findings and finally, visually presents research findings discovered during the research testing phases. The main focus of Chapter 4 is on reporting the field-testing results and presenting the tool evaluation results in visual format, which helps readers to interpret each evaluated tool's capability and limitations. Chapter 4 also provides the digital forensics examiner the opportunity to identify and then use multiple tools effectively, to reduce the investigation time and to maximise the accuracy of the results.

Variations of what is originally proposed in Chapter 3 were outlined and described in Section 4.1 in order to clarify changes made to the proposed evaluation methodology. Field-testing was then conducted with a total of 11 test scenarios for evaluating the existing evidence tool capabilities. Each test scenario is presented with a table that summarises the testing analysis results. In Section 4.4, the analysis testing

results are illustrated with 2 different charts to explain the highest ranked tool for each case scenario, extraction result by tools, and detailed extraction results from each web browser. Figures from 4.6 to 4.26 are visual representations of the summary table presented in Section 4.2.2.1 to 4.2.2.11. A separate chart and data table summarises all 11 test scenarios are illustrated in Section 4.4.3 and the Section 4.4.4 compares the each evaluation tools tested in Chapter 4.

Understanding the capability of the evidence extraction tools that support the SNSs helps the forensic examiner determine the accuracy and effectiveness they can expect when they need to use a particular tool. The tools evaluated in this research, when identifying their strengths and weakness, can dramatically improve the efficiency of a knowledgeable examiner. While tools evaluated in this research performed not particularly well and show lack of extraction results in some areas, new versions of each tool can be expected to improve and therefore meet investigative requirements for SNS forensics. The next chapter, Chapter 5, will discuss the findings presented in chapter four. Chapter 5 will provide a detailed discussion and analysis of findings with a comparison of tool capabilities. Chapter 5 will answer the research questions and hypotheses based on the findings reported on chapter four.

# Chapter Five

# DISCUSSION

## 5.0 INTRODUCTION

Field-testing has been conducted according to the tool testing methodology defined in Chapter 3. Test results for each test scenario are reported and presented in a descriptive and a visual manner in Chapter 4. Chapter five forms a discussion of the key findings from the field-testing scenarios presented in Chapter 4, so that the significance of the results can be evaluated in association with the discipline area. Research findings provide the most value when combined with a comprehensive discussion on the strength, weakness, and limitations of each tool as well as providing possible future development opportunities.

The main research question is concerned with the functionality of the evidence extraction tools in terms of their accuracy, completeness and forensic soundness. Fielding findings and the analysis result in chapter 4 are discussed in detail in Chapter 5. The research questions and sub-questions discussed in section 3.2 are addressed, based on the research findings and the proposed hypotheses discussed in section 3.2, and validated where appropriate.

Chapter 5 consist of 3 main sections. Section 5.1 answers the research question and sub-questions outlined in section 3.2. The 6 Hypotheses proposed in section 3.2 are discussed with the weighting result reported in Chapter 4 to check the validity of the proposed hypotheses. Section 5.2 provides discussion of the findings from the evidence extraction tools testing and evaluation results of each tool. The final section 5.3 explains the overall capabilities of each tool suggests scope for improvement of each tool, and seeks possible areas for future research.

## 5.1 RESEARCH QUESTION AND HYPOTHESES

This section reflects on aspects of the main research question proposed in section 3.2. In section 3.2 the research question, sub-questions and hypotheses were derived based on the literature review conducted in chapter two. The main research question and sub-questions proposed in chapter 3 will be reviewed here to decide whether the research question has been answered successfully by the work carried out during the Field-testing conducted in Chapter 4. The research question, and sub-questions will be answered in section 5.1.1, 5.1.2. Hypotheses developed for each of the sub-questions in section 3.2 are tested in section 5.1.3 followed by a recommended path for future research.

### 5.1.1 Research Question

The main question for this research is derived in section 3.2. What are the capabilities of the 3 chosen tools to collect and analyse evidence from Social Networking Sites in a digital forensic investigation? The aim of this research was to compare evidence extraction tools capabilities based on field testings conducted in chapter 4.

Through the background literature review studies in Chapter 2 an understanding was gained of how Social Networking Sites (SNSs) work, and how to extract data in a forensically sound manner. Chapter 3 provides a number of similar approaches in testing and evaluating tools for digital forensic investigation and develops a methodology for this research. In order to answer the proposed research question, 11 testing scenarios have been set and tested each of the three tools against a test scenario. Test data has been extracted from the 3 tools and analysis is performed on each test scenario.

Using the 11 test scenarios from section 4.2.2 evaluates each tool's functionality and extraction capability. The viability of the research question is supported by examining the test scenario results, which were gathered during the field-testing of the extraction capability in Section 4.2 – 4.4. The weighted numerical totals of each outcome are collected for each case scenario. Results were measured by calculating percentage of successful found rate on each scenario.

$$Found\ Rate\ (\%) = \frac{Total\ Number\ of\ extracted\ artifacts}{Total\ number\ of\ expected\ data} \times 100$$

The ‘Find Rate’ from each scenario is then added and an average ‘Find Rate’ is calculated for each extraction tool. The percentage for ‘Find Rate’ is then assigned to each product and a ranking is given based on Table 4.16.

Test results presented in Table 4.23 indicate that the highest percentage of extraction capability is achieved by CacheBack with a rate of 1.36 (36% extraction rate on average), EnCase scored 2nd highest rank with a rate of 1.27 (33% extraction rate on average), and IEF scored the lowest rank with a rate of 0.91 (23% extraction rate on average). However, this is an average ranking, thus achieved highest score does not mean the tool with the highest rank can extract all evidence from SNSs. No tool was successful in all 11 testing scenarios, and each tool demonstrated its strength and weaknesses in extracting evidence from SNSs.

### 5.1.2 Sub-Questions

A total of associated 6 sub research questions were developed in order to assist answering the main research question. Section 3.2 outlined the sub-questions. Each sub-question is checked during the field-testing phase and supported in answering the main research question. The first sub-question is: What are the current tools’ capabilities? The question is based on the vendor’s promotional literature and an ‘identifying list’ of tools that have the capability to extract evidence from SNSs. Section 2.4 provides evaluation of tools for SNSs, and illustrates that there are three tools (CacheBack, IEF, and EnCase) capable of extracting evidence from SNSs. Based on the evaluation of existing tools conducted in section 2.4, three sample tools were chosen for detailed study and prepared for the field testing phase.

The second sub-question is: What are the hardware and software requirements for the successful acquisition of SNS data as digital evidence? A list of required hardware and software is identified in section 3.9. However, additional software was necessary for the field-testing phase. Additional software used in this research is discussed in the Section 4.1, in variations. Except for the EnCase forensics tool, test procedures revealed that the extraction tools CacheBack and IEF require additional tools for acquiring evidence from the target machine, in order to get all collected evidence validated for integrity. Since both CacheBack and IEF cannot directly scan forensic images (such as .E01 used in this research), mounting software such as FTK or MIP must be used in conjunction with the tools in order to evidence image files mounted as virtual drives.

The third sub-question is: What functionality is necessary for collecting evidence from SNSs? It is difficult to the check number of features for each tool, and evaluate them. However, four common and crucial functions are identified in the collection of evidence using the three selected tools. These four functions are forensic acquisition, examination, reporting, and an intuitive interface. EnCase provides forensically sound acquisition, examination and reporting functionality but user interface was not easier than the other two evidence extraction tools. CacheBack and IEF provide easier and more intuitive interfaces for analysing evidence, however both tools lack in acquisition functionality hence, rely on other write blocking technology such as Tableau Imager (TIM). From the findings in this research, it is acknowledged that a single tool cannot handle collecting evidence in a forensically sound manner by fulfilling all four crucial functions. Collecting evidence in a forensically sound manner, and the easy of use, and intuitive analysis functionality, are just two examples of unforeseen situations where evidence extraction tools had to be used with one or another tool.

The fourth sub-question is: How can the selected tools be ranked in terms of accuracy and completeness of collected evidence? As discussed in section 4.2.2, a test rating scale has been developed to determine the accuracy of a forensic tool. Each of the 11 test scenarios results is assigned a quantitative value between 0 and 3.

The fifth sub-question is: Which tool is the best for SNS investigation? This research indicates that no one tool is best. Even though CacheBack scored the highest rank in overall testing scenarios, it does not imply that CacheBack is the extraction tool for SNS investigation. As identified in the third-sub question, each tool has its strengths and weaknesses, and these strengths needs to be combined for effective digital forensic investigation.

The sixth sub-question is: What new functionality for tools might be useful in addressing the current concerns for examiners of Social Network Forensics? The field-testing conducted in chapter 4 highlights important considerations such as the possible need for live memory dumps or other forensic procedures. This is because the extraction result is relying on the users' computer configuration and memory capacity. Research found that Facebook chatting and other Internet artifacts are stored dependant on a number of variables such as how the web browser is closed after chatting, how the OS is configured and shut down, and how much memory is allocated

on a users' computer. The test result indicates that there are still some fundamental issues to be resolved. Due to the characteristic of SNSs, people may use several computers to connect to SNSs and several computers can be connected by a home network. Exiting from SNSs and powering off these machines may result in the loss of Internet connection evidence such as traffic session data, which would otherwise assist an investigator in determining who had access to what websites or who had been communicated with in SNSs. Hence, the ability to acquire evidence from the live network status would be particularly useful in capturing any activity happening in SNSs. The ability to combine each of the three tools strengths would be ideal.

### 5.1.3 Hypotheses

This section discusses each of the six hypotheses developed for each of the associated sub-questions outlined in Section 3.2. Hypothesis testing is based on field findings.

The findings gathered from the research-testing phase are checked against to the asserted hypotheses. Table 5.1 - 5.5 display the six hypotheses. Each table presents the associated hypothesis, the arguments for and against the hypothesis.

**Table 5.1: Hypothesis testing 1**

| **Hypothesis 1** | |
|---|---|
| Given the fact the data exchange in question creates largely volatile data, survivability of data created during normal user interaction with SNSs is unknown. The chosen tools face difficulties in recovering the entire evidence from SNSs. Nevertheless, sufficient data can still be acquired to determine the likelihood of criminal activities, and the timelines and artifacts for legal proceedings. An inductively strong case for prosecution may result, even though hard evidence may be incomplete. | |
| **Argument For:** | **Argument Against:** |
| None of the three tools were able to extract full data from SNSs.<br>Although entire evidence extraction was not available in testing scenarios, some tools performed well and provides sufficient data that can help determine criminal activities in SNSs. | Some test scenarios, such as Facebook Chat extraction were unable to provide sufficient data that can be used for legal proceedings. |
| **Summary:** | |
| Although tools were not able to extract entire baseline of data posted on SNSs, each tool was capable of extracting a large portion of the artifact generated on the SNSs. Furthermore, chat fragments found by the tool can provide a crucial clue to the investigator as to where to look for further information. Even though there are still a number of limitations in extracting evidence from SNSs, the arguments made 'for' is sufficient for acceptance of the hypothesis. | |

**Table 5.2: Hypothesis testing 2**

| **Hypothesis 2** | |
|---|---|
| Hardware and software requirements for each selected tool will vary and also vary with the data digital investigators have to analyse. Different requirements for hardware and software impact on the investigation process and collection result. It is expected that tools will support a particular operating system, and will not be able to find evidence when collecting evidence from different testing platforms. | |
| **Argument For:** | **Argument Against:** |
| Each chosen tool requires different configuration. For example, CacheBack requires disabling user access control (UAC) and Windows firewall and requires that UAC settings are completely disabled.<br>While EnCase Forensics and CacheBack requires a USB dongle, IEF does not require a dongle to use the tool.<br>All three chosen tools are only available on a Windows platform at the time of writing. | All three chosen tools require the investigator to log in with administrator's privilege.<br>Although all three tools are designed for the Windows operating system, all of the three tools have capability of analysing data from Mac - Hierarchical File System (HFS) file system. |
| **Summary:** | |
| Although each tool's system requirements are minimal, there are different requirements between three tools. For example, minimum CPU requirement vary, supported operating systems, minimum disk space, and memory space requirements are slightly different. Therefore, the hypothesis is proved to be accepted. | |

**Table 5.3: Hypothesis testing 3**

| **Hypothesis 3** | |
|---|---|
| EnCase will have much more functionality than the other two selected forensic tools. However, it is expected that each tool will have several core functions in common but some distinct from the others. | |
| **Argument For:** | **Argument Against:** |
| Encase provides better functionality in certain test scenarios such as keyword search, acquisition of evidence, extraction of website cache, wall post, comments, and email messages.<br>Each tool has common functions such as extraction of web browser artifacts, and provides consistent extraction results in repeatability test. | While EnCase rated high in certain test scenarios, field-testing results show that EnCase has weaknesses in extraction of picture and video posts on SNSs.<br>EnCase does not necessarily provide more functionalities than other two tools. CacheBack and IEF provide more tools in extracting internet related artifacts. |
| **Summary:** | |
| Field test result indicates that EnCase is not always able to achieve better extraction result than other two tools. EnCase was not able to extract any evidence in certain scenarios. The testing result clearly indicated that each tool have its own strength and weakness in extracting evidence from SNSs. The arguments made for and against prove the hypothesis is rejected. | |

**Table 5.4: Hypothesis testing 4**

| **Hypothesis 4** | |
|---|---|
| Tool evaluation approaches reviewed in Section 3.1 will facilitate clearly defined testing metrics for ranking each forensic tool in terms of it's functionality, accuracy and completeness. | |
| **Argument For:** | **Argument Against:** |
| Based on section 3.1, a test-rating scale is developed with a numeric value between 0 and 3 for each of the 11 testing scenarios. (see Table 4.5)<br>A number of similar approaches in evaluating tools have been reviewed in order to develop tool evaluation approaches in this research. Based on the method developed in Section 3.1, various techniques has been used to palliate the deleterious factors in the testing phase. | A test rating scale was not able to define the accuracy of the each case scenario. Therefore, a separate test case is made to test repeatability and accuracy of extraction results.<br>It can be possible to improve the evaluation approaches with more mathematical ranking scales. |
| **Summary:** | |
| Reviewing similar approaches in tool evaluation method provides an understanding of evaluation procedures and techniques allowing the author's own development of testing metrics and ranking scales for this research. Therefore, the hypothesis is proved to be accepted. | |

**Table 5.5: Hypothesis testing 5**

| **Hypothesis 5** | |
|---|---|
| EnCase Forensics software will perform better than the other two selected tools in the data acquisition process. CacheBack 3 and Internet Evidence Finder will perform better than EnCase in finding evidence from SNSs and in the presentation process. | |
| **Argument For:** | **Argument Against:** |
| EnCase provides a forensically sound acquisition process<br>CacheBack and IEF provide more intuitive reporting functionality than EnCase and made it easier for investigators to analyse extracted data. | None of the tools provide better extraction results in all 11-test scenarios than any other.<br>EnCase found more artifacts in extraction of wall post, comments, location information |
| **Summary:** | |
| The EnCase is capable of acquiring and preserving the data as digital evidence from the target hard drive. There are a number of areas that CacheBack performed better than other tools in finding evidence from SNSs, however CacheBack was not able to extract data from some particular test scenarios. Moreover, EnCase ranked higher extraction rate than IEF in finding evidence from SNSs. As the tools capability may vary depends on the test environment and scenarios, the arguments made for and against show the hypothesis is uncertain. | |

**Table 5.6: Hypothesis testing 6**

| **Hypothesis 6** | |
|---|---|
| The fairness and lack of bias in the evidence collection process will be useful in addressing the current concerns of acquiring evidence from SNSs. A function that enables the examiner to check the investigation process with the 5 common steps of digital forensics investigation identified in Section 2.2.6 would be useful. | |
| **Argument For:** | **Argument Against:** |
| Following the 5 common investigative processes enables forensic soundness of data extraction. | Due to the characteristics of SNSs, it is not possible to know where the artifact resides on each SNS. This also means the investigator cannot determine what laws to apply and thus still faces to jurisdictional issues. Thus, following 5 common steps still cannot address the current concerns of acquiring evidence from SNSs. |
| **Summary:** | |
| Although traditional digital forensics collection processes and standards may be used in extraction of evidence from SNSs, there are a number of specific challenges and issues in Social Network investigation. Tools tested in this research do not provide intuitive indication of investigation process within the tool. The arguments made for and against show the hypothesis is rejected. | |

Results of testing the six hypotheses indicate H1 (The chosen tools face difficulties in recovering the entire evidence from SNSs. Nevertheless, sufficient data can still be acquired to determine the likelihood of criminal activities, and the timelines and artifacts for legal proceedings.) is correct, H2 (Hardware and software requirement for each chosen tool will vary) is correct, H3 (EnCase will have much more functionality than other two selected forensic tools) is not correct, H4 (Tool evaluation approaches reviewed in Section 3.1 will inform clearly defined testing metrics for ranking each forensic tools) is correct, H5 (EnCase Forensics software will perform better than the other two selected tools in the data acquisition process) is not always correct, H6 (A function that enables the examiner to check the investigation process with the 5 common steps of digital forensics investigation identified in Section 2.2.6 would be useful) is not correct.

## 5.2 DISCUSSION OF THE FINDINGS FOR TOOL EVALUATION

The field-testing work carried out in the research phase revealed different capabilities from the three selected evidence extraction tools. The field finding tests were conducted, with the four phases defined earlier in Section 4.2, to evaluate the effectiveness of the extraction tools capabilities. The findings indicate that each of the 3 tools evaluated in this research has some capability in extracting evidence from SNSs, but is limited to extraction of some fragments of information posted on SNSs.

This section discusses and reviews the field findings of the three evidence extraction tools, and highlights operational shortfalls that would impede the recovery of significant evidentiary data from Social Networking Sites (SNSs). Arguments will be made for and against the hypotheses, and a summary has been provided based on the field-testing results. In addition, findings for each evaluated extraction tool are discussed and reviewed in Section 5.2.1 – 5.2.3, followed by a summary of the capabilities of each tool.

The first phase was to set up appropriate testing environments for testing the three extraction tools, and generate test data that could be used as a baseline. An existing desktop PC was first setup as a target computer and the Windows 7 Operating System installed. Although phase one did not involve answering the research question, having a proper testing environment and knowing the baseline for the expected evidence was a crucial part of this research, as a known baseline for the generated data then acts as the control. For example, knowing that there are only 20 Facebook chat messages to be found from the target hard drive, the author can then predict that if the test performs correctly it will only find a maximum of 20 chat histories. Otherwise, the author can indicate that there are some problems with either the testing environment or the tool configuration.

The second and third phases of testing were quantitative testing. Tests were performed and the generated test data collected from each tool. A scan of the target machine's hard drive was performed using the different scan functions provided by each tool. Total extracted evidence was counted and recorded against the expected number of data values, and the percentage of extracted data was calculated.

The fourth phase of testing was comparative testing. The total count of collected data from each tool was recorded and rated, based on the rating scale defined in Table 4.16. Recorded test results are compared with results taken from each of the 3 tools and presented in tabular and graphical chart format to give visual interpretation of test results. The charts presented in this phase show any significant differences in the quantity of extracted evidence for each tool.

Data analysis produced findings to determine the capabilities of the three tools. Although the comparison charts show that some tools performed markedly well and extracted more evidence than others, it would be reasonable to assume that evidence from SNSs is not always extractable by using these three tools, as shown in Figure 4.26.

Although each of the three tools is not specifically designed for extracting evidence from SNSs, the author believes that CacheBack offers the best potential, at this time, for future development as an SNS investigation tool. CacheBack achieved the highest rank in extracting evidence from SNSs at the time of writing, although perhaps not significantly greater than EnCase (36% Versus. 33%) when usability and automation features of the user interface are considered, it's easier to achieve an indicative result fast.

The following section discusses weaknesses and strengths for each tool, how the author analysed data, why each tool performed well or not well, what has been extracted from SNSs, and how this extracted data could be used as crucial evidence in a court of law. The following section reflects on aspects of the main purpose of the research, such as how well each tool met the aim, and the research questions proposed in Section 3.2.

### 5.2.1 CacheBack

Like other two tools tested in this research, CacheBack is an offline, Window based Internet evidence extraction tool that is designed to analyse Internet browser related artifacts. As described in section 3.4.1, FTK imager is used to mount the evidence image as a virtual drive on an investigation machine, so that CacheBack can scan the evidence from the virtual drive. CacheBack demonstrated a very intuitive user

interface, and provides enhanced functionalities in areas such as extracting artifacts that relied on web browser applications.

As can be seen from section 4.4.4, CacheBack rated the highest score among the three tools tested in this research. The figure 4.26 is shows that CacheBack rated the highest score in 5 of 11 testing scenarios including: extraction of web history, cookies, images, video, and Facebook chat artifacts. The built-in offline browser and HTML Gallery Viewer with Photograph Aspect Ratio Differential (PARD) support allows investigator to examine web pages both individually, and grouped as thumbnails, thereby making it even easier to conduct Internet based investigations. User definable customised SQL query functionality and the ability to query statement as favourites was a great advantage. Custom queries make it easy to analyse the number of extracted items for each case scenario and the 'save' option allows the author to use it for the repeatability testing conducted in the field testing phase.

Interaction with the CachBack tool was uncomplicated, and straightforward for the author. For example, the table view with sorting option, the ability to filter by file type and the ability to search evidence based on browser type makes the data analysis process simple and easy to navigate. The thumbnail view, HTML gallery view, and 'Filter by Host' option allow to observe the evidence from different viewpoints.

CacheBack also rated highest score in extraction of Facebook chatting artifacts. As seen in the Chapter 2, Facebook is very popular and the most widely used social networking site. Facebook chat is also very popular as it can be accessed easily in a variety of ways. Anyone with a Facebook account will be able to login and use the chat functionality in their web browser. Although Facebook does not provide chat history logs after a certain elapsed time, it is still possible to extract chatting information in a forensically sound manner. Facebook chat information is stored in the Internet Temp file, web browser cache, unallocated clusters, RAM, pagefile.sys, and hibernation file are all viable sources. Until these locations are cleared, Facebook chat information can be extracted.

CacheBack's Recover My Chat (RMC) testing result proves this. RMC provides a friendly and robust user interface with powerful chat extraction capabilities. RMC features rich HTML reporting built-in, with options to display the number of chats sent or received and the time spent chatting. Chats are stored in an Access

database for flexible query options and can be exported to a .CSV file for import into Excel. While both IEF and EnCase forensic failed to extract detailed Facebook chat artifacts, CacheBack's add-on product – RMC was able to extract all 20 chat messages with detailed information such as sender and receiver's ID and message send and received time. RMC also provided "forensic metadata" option, which allows digital forensic investigator to see senders ID or the recipient ID on a report view. This requires investigator to be logged into Facebook first using any valid account. ID lookup function concept is very similar to what IEF is providing, but CacheBack's RMC provides bit more user friendly option as investigator does not need to use separate tool to lookup sender or recipient ID.

While CacheBack rated highest in overall testing scenarios, there is scope to improve. For example, Cacheback was not able to scan the evidence image without third party tool intervention, other tools such as FTK imager has to be used in conjunction with the CacheBack tool. In this regard, it is reasonable to assume that CacheBack's evidence extraction capability is reliant on other tools that are used for that particular investigation.

### 5.2.2 Internet Evidence Finder

The official webpage for the 'Internet Evidence Finder' (IEF) on the JADsoftware website states that IEF can find Facebook Chat, Twitter Status updates, Gmail Email fragments, Internet Explorer InPrivate URLs, Firefox places.sqlite history, and Firefox sessionstore.js artifacts (JAD Software, 2011b). This implies IEF does not support, and is not designed to recover: image, video, comments, and location posted on SNSs, at the time of the writing. The search options given from IEF includes: 1) Quick Search, 2) Full Search, 3) Unallocated Clusters Only 4) Full Search – Sector level 5) Files and Folders search. This research used full search option. Internet Evidence Finder's full search functionality finds the entire physical hard drive, which includes any existing volume shadow copies in the system volume information folder, the Hiberfil.sys file, pagefile.sys, unallocated clusters, and file slack space. This research acquired target hard disk as an E01 format evidence image. IEF had to use additional software to map the E01 file as a virtual drive. For this purpose, FTK imager was used

to mount evidence image as a virtual drive, so that IEF can select the logical drive from the image file.

IEF provide a 'scan wizard', which allows the digital forensic investigator to select the artifact that is relevant to the case, and therefore, saves time and focuses the accuracy of the report. After the scan is completed, IEF provides an overview of search results, showing how many artifacts have been extracted and of which type. IEF organises all the extracted files into separate folders based on the type of evidence (See Appendix C-4). Reporting functionality was acceptably friendly and straightforward. As soon as a scan is completed, the IEF tool provides an option to view reports in the IEF report viewer. Report viewer also gives the examiner the ability to export reports as a web file or CSV, and in Microsoft Excel format.

IEF provides a user-friendly interface for the digital forensic investigator. Menus provided in IEF were sufficiently self-explanatory, and the 'help' function gives more detailed information when required. The ability to select artifact types allows investigators to skip unnecessary artifacts that are not relevant to the case, also saving investigation time. The ability to extract evidence from SNSs is unsatisfactory. From figure 4.26, it can be shown that Internet artifacts (except the Facebook Chat and Gmail fragment) are not effectively supported and therefore IEF was not able to extract evidence from SNSs. This matter needs to be addressed since the core functionality of IEF is to find Internet Evidence that would link a suspect to the crime. Although, IEF was able to find 20 of 20 Facebook chat artifacts, crucial information such as sender's detail, message send time, and receive time, were not extracted in this test case. This is because Facebook chat does not actually log chatting messages anywhere in the user's computer. Thus, IEF cannot guarantee every single sent or received message and it is possible for crucial information such as send and receive time to be omitted.

Facebook chat messages recovered from IEF remain as artifacts on the hard drive in the Systems volume information. Although IEF failed to extract detailed chat information, it sign-posted where the chat information was to be found (See Appendix C-6). Chat message location is identified from IEF, with the preceding the message block. This allowed author to manually examine the byte-level values. FTK Imager is then used to locate all 20 found chatting messages from the evidence image. It seems

that IEF was not able to find detailed information from the target machine because Windows has strict security safeguards against accessing systems volume information files, and therefore IEF was not able to extract detailed chat information. EnCase and FTK imager can access these strictly protected files, however it appears that IEF lacks capability in accessing these windows protected file and therefore having difficulties with reading detailed information.

Appendix C-15 shows the text data from the original source location that is extracted from FTK imager. Facebook chatting message was found as a fragment of a chat message and this text file was more than sufficient to get detailed information about Facebook chat information.

### 5.2.3 EnCase

EnCase Forensic, produced by Guidance Software was evaluated along with 2 other Internet evidence extraction tools. EnCase achieved the 2nd highest rank in the 3 evaluated tools and shown it's strength in Email and Cache extraction in this research.

EnCase's comprehensive Internet history search option is used to examine the Internet artifacts from the entire storage device (including the slack space and unallocated space). Search results are shown in the Records tab, which separates extracted evidence by browser types. Although EnCase presents evidence in a separate folder, web browser information was not always accurate in the test case for extracting web history, cache and cookies. This resulted in EnCase performing exceptionally well in extracting the Internet artifiacts from the Internet explorer, EnCase could not distinguish well in identifying the origin of the evidence from Google Chrome, Firefox or Apple Safari web browser.

All extracted evidence data from EnCase provides crucial information such as creation time, last access time, and the number of times the user has visited a given site (See Appendix C-9). The tool prompts to examine the files extracted from SNSs. Appendix C-10 illustrates how images posted on SNSs can be analysed within the EnCase. A hash analysis technique is used to speed up the investigation time. A hash value is calculated on the evidence disk and compared with a collection of hash values (hash set) from the original image files. This hash search results shows notable files in a gallery view, which provides a very effective way of investigating images.

EnCase also attempted to extract evidence left by the use of Facebook chat. It is commonly known that Facebook uses JavaScript Object Notation (JSON) for sending messages and many investigators are faced with decoding the JSON language behind the Facebook chat engine. Encase has written a code for the purpose of parsing the JSON data automatically to recover and report on Facebook chat artifacts. The Enscript written by EnCase locates all the Facebook chat messages from the evidence image file and converts them into a more human ready format. Although two versions of Facebook Chat Parser (version 1.4 and 2.1) have been used to extract 20 Facebook Chat evidence samples generated for this test, EnCase was not able to extract any Facebook Chat evidence.

Testing results from both IEF and EnCase illustrates the variables involved in recovering live web based information from a static forensic copy of a computer system. It brings to light the issue of OS user configuration (pagefile and hibernation file), and highlights important considerations such as the possible need for live memory dumps or other forensic procedures. From the field findings chapter, this study found that Facebook imprints its chat on a hard drive in 5 main locations (pagefile.sys/hiberfil.sys files, allocated clusters, file slack space, temporary Internet files). Where the files are stored depends on variables such as how the web browser is closed after chat, and how the OS is configured and shut down. Even though EnCase can find Facebook chat artifacts in the majority of cases, EnCase failed to acquire any of the 20 chat messages generated for the purpose of this research. The test result indicates that there are still some fundamental issues to be resolved, as EnCase cannot always find the chat data from the target hard drive. A suspects' machine environment such as configuration of the target computer's hibernation file, or size of memory used in the target machine can impact on the capability of extraction tools.

EnCase performed reasonably well in extracting the Internet browsing artifacts such as Internet History, Cache and Cookies. Automated Internet history search function provided by Encase allows to the extraction of various types of Internet artifacts logged when websites are accessed through web browsers. EnCase shows strength is extracting Microsoft Internet Explorer's artifacts in particular allowing the examiner to quickly and easily analyse the browser history, and web cache information. However, there is not an easy way to identify types of browser the

evidence is extracted from, as most of the collected browsing data is stored under the Internet Explorer's folder.

EnCase achieved the highest rank in extracting emails. EnCase provides the ability to find, analyse, display and document various types of emails, including Microsoft Outlook, Outlook express, plus webmail such as Yahoo, Hotmail and Netscape. EnCase has an email search function that locates emails files, mount them, and show the results on the Records tab within EnCase. EnCase discovered 20 of 20 email items within the evidence image file, shows the messages and administrative data in the Table Pane (See Appendix C-11). Looking at the extracted message's report gives more detailed information such as subject of email, creation time, sent and received time, as well as name of the senders and receivers.

EnCase also achieved highset rank in extracting Location information, Wall posts, and Comment posted on SNSs. Unfortunately, there is no way in EnCase to run an automated process to access the above information when posted on SNSs. Since EnCase provides a powerful keyword string search to location information anywhere on the physical and logical image file, a keyword search was performed to find key word strings that match the keyword used in the data generation phase. A number of keywords were added into EnCase and keyword search found all matched keywords found from the case image file and presented them in Table Pane (See Appendix C-12). It is of interest to compare the full path where the location, wall post, and comments posted on SNSs. Most of the location information was extracted from the first_degree[1].js file from the temporary internet files folder (Appendix C-12), Wall post and status updates were found from unallocated clusters, browser's cache file (Apple Safari) and history index file (Google Chrome), or system volume information. Comments posted on SNSs are found from Safari history files (Appendix C-14).

It is clear that artifacts remains on hard drive are dependant on the types of browser used for accessing SNSs (Appendix C-13). This test used keyword searches to see whether EnCase could extract information posted on SNSs. However it should be possible to improve the functionality in EnCase to automate this process by using EnScripts or some other built in search methods such as Email or Internet history search functions.

## 5.3 RECOMMENDATIONS FOR FURTHER RESEARCH

Although the research test has succeeded in fulfilling its aim and answering the research questions proposed in section 3.2, there are still areas of research in the future.

Expected outcomes discussed in Section 3.5 indicate that tools capability to extract evidence from SNSs will be limited. After conducting field-testing, the analysis of test result indicated that this outcome is correct. Obtaining complete evidence from SNSs was not possible, however collected evidence from one tool provides clues for where to look in order to get more information. For example, none of the three chosen tools were able to extract a detailed Facebook chat history, however identifying the location of the Facebook chat artifact found from IEF (See Appendix C-6) gives information to the investigator as to where and how to find the evidence manually (See Appendix C-15). Another expected outcome was that no one particular tool would be ranked significantly higher than other tools. As described in section 4.4.4, each tool has strengths and weaknesses and these indicate the need for multiple tools for best investigative results. However, some tools are able to extract more data than others because particular functionality in that tool was utilised for extracting SNSs related artifacts. Since the field-testing result show the capabilities of each of the three chosen tools, this result could be used as a reference for future improvement for the evidence extraction tools. Digital forensic investigators can utilise the most suitable tools for the particular case they have, or, can also utilise multiple tools to extract more artifacts from SNSs. The design and implementation of combining strengths from each three selected tools would prove to be a very useful further development of the application.

The three chosen evidence extraction tools evaluated in this research is a small number compared to currently available evidence extraction tools in the market. There is a possibility that other tools can extract more evidence than the chosen tools, have better functionality, and be able to extract evidence from SNSs in a live mode. At the current stage, it is noted that none of the three selected tools are specifically designed for extracting evidence from SNSs. The three chosen tools were able to find some artifacts from SNSs as each tool supports evidence extraction from web browser related artifacts. For example, CacheBack was originally designed as a standalone tool

to rebuild webpages from an Internet browser's cache, IEF is designed to search a hard drive or files for Internet related artifacts, and EnCase was designed for a wide range of forensic investigation from data collection to examination of evidence.

All three tools tested in this research are powerful and intuitive to a forensic investigator tracking Internet activities in general. However, the test results show that all of three tools do not have automated analysis functionality for SNSs. Some tools support extraction of chat messages, but not comment or location information posted on SNSs. Some tools can extract status update and comments posted on SNSs but all the extraction had to be done manually as there was no automated function. The main shortcomings of both CacheBack and IEF are their lack of support for acquisition of evidence and lack of ability to mount the evidence image within the tool. As both CacheBack and IEF were not supporting a standalone-mounting option, reliance on other mounting software such as FTK or MIP was unavoidable. The shortcoming identified from EnCase was lack of support in automated procedures in analysing evidence extracted from SNSs.

Future research to develop a tool combining strengths identified for each tool, as well as supporting multiple web browsers with automated search for SNS artifacts would extend the tool's capability immensely. Extending the capabilities to using the tools on a different operating system such as Macintosh computer or Linux operating system would be a crucial part in the future research as more people trend toward the use of Mac or Linux as a personal computer. Even though extending the tools to utilize native mobile phone extract support would be beyond the scope of this research, this would be a crucial part of extracting evidence from SNSs as people are not only connecting to SNSs via Web browsers but also connecting to them via mobile phones with number of different applications.

With tools that can extract data from SNSs, investigators need a careful analysis of obtainable data in order to verify whether the genuine post is extracted from SNSs. This is because tools can only extract the data from the SNSs but cannot verify whether the information posted on SNSs is true information. For example people can post false location information on SNSs. In this regard, further research is required to verify the post inserted into SNSs. Finally, this research found that extraction of Chat messages is difficult as they are typically not saved on the hard

drive, and also artifacts are stored in many different places depending on a number of variables. Some tools were able to extract all messages but no other details, some tools could recover send dates and times for chat messages as well as users ID, and detailed messages. Hopefully, the research findings could contribute to the future development of a social network artifact extraction tool or to the enhancement of existing tools.

## 5.4 CONCLUSION

This chapter discusses an overview of the key research findings, which are useful in Social Network forensic investigation. Based on chapter four, field-testing results a comprehensive overview of the each chosen tools capabilities was made. Strengths, weaknesses and limitations of each tool have been highlighted in section 5.2. Chapter five has provided extensive discussion about each tool's extraction capability to retrieve data from SNSs. In addition to this, through the research carried out in the field-testing section, all research questions outlined in section 3.2 have been answered fully and adequately. In section 5.1.3, the 6 hypotheses developed in section 3.2 are tested. Testing hypotheses shows that H1, H2 and H4 are accepted while H3 and H6 are rejected. H5 testing shows those hypotheses are correct most of times but not always correct.

Social Network forensics is a relatively recent topic in digital forensics and tools are also early stages of maturity. At the time of writing, the author noted that there are no tools that are particularly designed for extracting artifacts from SNSs. The three chosen existing evidence extraction tools can extract some of the artifacts from SNSs. However, significant enhancement is expected to improve extraction capabilities and therefore meet investigation requirements. The future development of Social Network forensic tools must evolve with multiple web browsers' support, mobile devices, and a user friendly interface, allowing extracted data to be analysed in a most effective and forensically sound manner. As social networking sites increase in popularity, new versions of tools for extracting artifact from SNSs also continue to improve. Forensic investigators must understand the functionality and capability of these tools adequately, before the tools are used. Knowledge has been gained here, about how to extract evidence from SNSs, and a variety of methods of testing have been explored and compared to evaluate the extraction capabilities of the three chosen tools. Based on the body of knowledge gained from chapter 4 and 5, possible

development ideas and research avenues have been suggested in section 5.3 to allow for the future research in the area of Social Network forensics.

Chapter 6 concludes the research project and presents a summary of the research and the significant findings that have been discovered. Research findings reported in chapter 4 will be summarised and limitations to the research will be outlined. Other possibilities for research within the discipline area will be discussed creating a link to continued research in Social Network Forensics.

# Chapter Six

# CONCLUSION

## 6.0 INTRODUCTION

The chosen field of research is focused on the evaluation of capabilities of evidence extraction tools that can extract data from Social Networking Sites (SNSs). Understanding the capabilities of tools can help forensic investigators to use the tool in the most effective way, so that they can produce repeatable results and admissible evidence to the courts of law. In order to compare extraction capabilities for each of 3 tools, a base line of known evidence was generated and testing performed to determine which tool could extract data from the 10 different test scenarios. In conjunction with the 10 extraction test scenarios, another component of testing has been performed to check the tools ability to extract evidence in a repeatable and reproducible manner as this component is considered to be a crucial part of digital forensics.

Chapter 1 and 2 identify the importance of the research in the chosen research area. Due to the ever increasing number of people using SNSs, the number of crimes involving SNSs are also increasing, and creates potential investigation issues, as potential evidence posted on SNSs is inclined to be volatile. Chapter 3 reviewed five similar approaches for evaluating digital forensic tools to guide how this research could be conducted. Based on the literature review conducted in Chapter 2, and research method developed in Chapter 3, three selected evidence extraction tools are evaluated and the research findings are presented in Chapter 4. Chapter 5 discussed researching findings and provides a summary of the field-testing outcomes with the recommendations for future research.

Chapter 6 presents the final conclusion for the research conducted. The field-testing results, previously presented in chapter four and discussed in chapter five are summarised in section 6.1. Based on the research findings, the answer to the research question is summarised and concluded in section 6.2. Section 6.3 discusses limitations identified during field-testing phase, followed by proposed relevant recommendations for the use of these forensic tools including capability changes by the noted limitations and performances, as well as providing recommendation for future research in the same topic area.

## 6.1 SUMMARY OF RESEARCH FINDINGS

During the field-testing phase, research demonstrated procedures for collecting evidence from SNSs using the existing forensic tools such as EnCE, CacheBack, and Internet Evidence Finder. These forensic tools are evaluated and compared through an analysis of the sample testing data that results from their use in a laboratory simulation. As a part of testing the capability of the tools, a testing environment was set up with sample-generated data that can be used as a known baseline. The testing environment has been configured based on a literature review conducted in Chapter 2 to make sure evaluation procedures in this research can be conducted in a forensically sound manner.

Three evidence extraction tools have been evaluated in the field-testing phase with 4 popular main web browsers. The research has found that none of the three extraction tools are adequate for extracting sufficient evidence from SNSs. Hence, investigators have a need to combine multiple tools in order to maximise the extraction results. It is important to note that the tools evaluated in this research are not specifically built for extracting evidence from SNSs.

Extraction testing was performed with 11 testing scenarios for each tool. The extraction result is counted and recorded against the expected baseline number and the percentage of extracted data is calculated. CacheBack extracted the highest amount of extracted data in overall rate of 1.36 (36%), EnCase rated 1.27 (33%) followed by IEF, which rated 0.91 (23%). After field-testing, the testing results are analysed to identify what tools performing well in which testing scenarios. 10 evidence extractability-testing scenarios have a corresponding main investigation component, and 1 additional testing scenario was developed to check the forensic soundness of the tool. The 10 evidence extractability-testing scenarios are: web history, cache, cookies, images, video, wall post, comments, location, Facebook chat, and emails. The 1 additional testing scenario was to check the tools ability to produce extraction result in a repeatable and reproducible manner. Findings show that all of the three chosen tools consistently performed well in repeatability testing, however they score inconsistently on 10 extractability testing scenarios. CacheBack scored consistently high in

extracting evidence from the web browsers (web history, cookies, image, and video), EnCase performed well in extracting evidence from unallocated space where Cache, location, and wall post update was extracted. IEF scored consistently low except in the Facebook chat extraction scenario. Both CacheBack and IEF were able to extract 20 of 20 Facebook chat messages, however only CacheBack's Recover My Chat (RMC) was able to extract detailed chat information. A summary of results is shown in Figure 4.26.

Research found that EnCase is not always able to find Facebook chat artifacts and other information posted on SNSs. EnScript provided with EnCase was used to extract Facebook chat artifacts, however it failed to extract any of 20 chat messages generated in this research. EnCase could not distinguish artifacts associated with Mozilla Firefox, Apple Safari, Microsoft Internet Explorer or Google Chrome web browser. Some artifacts from Mozilla Firefox were stored on an Internet Explorer's folder and web browser's artifacts from Google Chrome and Apple Safari browser was not extracted. EnCase performed very well in extracting location information, wall post and comment posted on SNSs by using manual keyword search. Some usability problems with the EnCase tool are also noted. Manual keyword search was performed to extract information posted on SNSs. It would not be practical in real world to manually analyse the evidence with every possible keyword search as data storage capacities are growing geometrically. Therefore, an automated process is required for scanning social networking artifacts from the evidence image.

IEF rated the lowest score among the three selected tools, but it does provide crucial information about Facebook chat artifacts. While IEF demonstrated it's strength in extracting Facebook chat, IEF was not able to extract detailed crucial information from the extracted chat messages, such as sender's detail, message send time, and receive time. Even though IEF failed to extracted detailed information, it provides the location where the artifact has been found. Since IEF provided the locale for the artifacts, it enables investigator to use other tools such as FTK to manually analyse the Facebook chat artifacts. The scanning capabilities of IEF were very powerful. IEF provides a number of scan options that investigator can use to save

time. Scan options include searching the entire hard drive, specific folders, memory dumps, and sector level scans. The extracted result is presented within the IEF report view in a user friendly and informative way. Report results can be exported to other applications' formats such as Microsoft Excel or a CSV file. This function is also provided by EnCase and CacheBack tools and this is a clear benefit for the investigator as no other special tool is required to interpret the report generated by the tool.

CacheBack resulted in the highest rank among the three tested tools in most testing scenarios. CacheBack supports all 4 web browsers used in this research and is able to filter extracted result based on the type of web browser. CacheBack also provies an intuitive interface with a powerful custom query tool, which makes it easier for the investigator to analyse extracted artifacts with an easy to understand visual user interface. Some concerns found with CacheBack are that CacheBack is reliant on other tools, as it does not have native capability to read the evidence image file itself. The Facebook chat extraction result is partly reliant on EnCase as it had to be scanned using EnScript. However, CacheBack's beta product Recover My Chat (RMC) resolved this issue. Instead of relying on an EnScript that had to be used with EnCase tool, Facebook chat could be recovered by RMC itself. This add-on service provides disk level access as well as logical file access to NTFS and FAT32 partitioned hard disks, which also provides an option to extract chat artifacts from a number of other chat programmes such as MSN and Yahoo Messenger. However, this programme still requires an additional mounting tool, as RMC does not have capability to run directly on forensic images (such as .E01 images).

## 6.2 ANSWER TO THE RESEARCH QUESTION

The purpose of the main research questions is to find out extraction capability of the three chosen tools that can be used to discover crucial evidence from social networking sites such as Twitter, LinkedIn, Google Plus, and Facebook. Evaluating the usability of the extraction tool is also one of the research areas that this research identified from the field-testing phase. As noted in Section 4.2.2.11, and stated by the National Institute of Standards and Technology, tools test results must be repeatable

and reproducible. All three of the selected evidence extraction tools chosen for this research demonstrate that all of the three tools can extract evidence in a repeatable and reproducible manner, thus demonstrating that all three tools are considered as forensically sound tools.

In order to answer the main research question, 6 sub questions and 6 associated hypotheses have been derived. 11 testing scenarios are designed for testing whether the tools are extracting evidence from SNSs from different perspectives. Section 5.1.1 describes and discusses the result of tools capability identified during the field-testing phase. In order to answer the research question, 11 testing scenarios have been tested with each tool and a weighted numerical total is given based on the outcome of each case scenario. Two measurements of tools extraction capability have been used in this research: The total amount of data extracted from each testing scenario and an analysis capability of each tool. Analysis has been performed on the extracted data to compare the results with the baseline data generated for the purpose of this research. The testing results indicated that CacheBack has performed better than or equal to the EnCase or IEF in extraction of Web history, Cookies, Images, and Videos posted on SNSs as well as extracting Facebook chat artifacts. EnCase performed well in extraction of Cache, Wall posts, Comments, Location and Emails, but presented problems in the automation process. IEF performed worse then other two evidence extraction tools but has similar results in extracting Facebook chat artifacts, Cache and Cookies. All of the three chosen tools have capability of extracting evidence in a repeatable and reproducible manner.

Since each of the selected tool's product website describes their tool as easily extracting Internet related evidence, the author expected that all of three tools will be able to extract more than 50% of the expected extraction result, and some tools would work much better than others in particular test scenarios. IEF scored the lowest result in most of the test scenarios and could not extract detailed information from Facebook chat. During the field testing conducted in chapter 4, the research found some unexpected results especially in extraction of Facebook chat as the artifacts were found from unexpected locations and none of literature review identified the systems volume information folder as a possible location where Facebook chat artifact can reside. It was also noted that EnCase failed to extract Facebook artifacts and IEF failed

to extract detailed chat information. This may be caused by Window's strict security safeguards against accessing files from the systems volume information folder. Although the overall extraction rate is lower than what has been initially thought, all the tools are tested against the same testing scenarios with the same rating scale, so a consistent and accurate result is expected. The field-testing results presented in this research are limited to the three chosen tools and recommendations and conclusions from the research is sorely based on the testing results from the three tools. Thus, it is possible that other tools available on market may support evidence extraction from SNSs.

In summary, each of the 11 field testing scenarios provided findings to assist in answering the main research question, sub-questions and its hypotheses. It is concluded that each of the three tools evaluated in this research have the capability of extracting evidence from SNSs. However, there are still a number of issues in extracting evidence from SNSs including data loss, missing detailed information, approaches to detecting false positive information posted on SNSs. The knowledge gained from the research analysis phase was used to outline limitations of this research in next section.

## 6.3 LIMITATIONS OF RESEARCH

Limitations of this research have been identified in Section 3.6 based on the review of similar studies and the literature review conducted in Chapter 2. The field-testing results show that the limitations identified early in the section 3.6 are still apparent, and remain important after conducting the testing phase.

Firstly, it is noted that none of the tools are designed specifically for Social network investigation. While CacheBack and IEF are focused on extracting evidence from Internet artifacts left on the users' hard drive, the EnCase tool is focused on the entire functionality particularly in creating the raw file and analysing the raw file or evidence image. EnCase has a wide range of functionality that covers extraction of Internet artifacts as well. However, none of the three tools are solely and exclusively focused on extracting and analysing artifacts from SNSs. Therefore, the three tools capability of extracting evidence from SNSs is limited to providing only what each tool can extract with their offline extraction functionalities, meaning that tools cannot

completely extract evidence from SNSs, thus, overall extraction rate presented in chapter 4 is lower than what is initially expected.

There were also limitations as a result of scope of this research. This research has tested tools with 11 test scenarios. 11 test scenarios may not be enough to judge the capability of the tools, as it may not include testing extraction capability of particular SNSs or chatting programmes. For example, some tools may have strong capabilities in extracting evidence from Yahoo messenger or MSN messenger chat programmes, whereas other tools may have strengths in extracting evidence from MySpace or Foursquare-like social networking sites. Since the objective of this research is to identify and evaluate evidence extraction capabilities with the 11 developed test scenarios, no additional test scenarios been added. It is therefore noted that there is a limitation in identifying every possible extraction capability of the tools in all different types of SNSs.

Another limitation is that the result can be different on a case-by-case basis. As identified earlier in the chapter 5, information posted on SNSs can reside on the computer hard disk dependant on a number of variables such as memory installed on users computer or computer settings such hibernation and the virtual memory space configuration. Although this research could not test the extraction capabilities against every possible SNSs, the author feels that the major SNSs have been tested with 11 developed test scenario result gives highest probability of accuracy in evidence extraction tool capabilities. The limitations identified in the research will provide directions for future research, outlined in the next section.

## 6.4 FUTURE RESEARCH

Based on the field-test result presented in chapter 4 and identified limitations of this research, scope for improvement of each evaluated tool, and possible areas for future research are discussed in section 5.3. Further research could look at expanding the capability of the tools that can extract evidence from SNSs, including extracting evidence from different browsers as well as different platforms of operating system.

It is also identified in the tool testing phase that current tools have limitation in extracting evidence when in the ‘offline’ mode; meaning that tools can only extract data that resides on the users hard drive, when the user is offline. One exceptionally

important area of much needed research is the development of live acquisition functionality that can extract evidence online in real time. Live acquisition from the Internet must be a high priority in all three tools tested in any future research. It would also be of universal benefit to have an all-in-one, tightly integrated and standalone tool that can be used as the data-mining tool for SNS investigation.

With the growing popularity of SNSs, and the likely future required for web-centric forensic investigation, further research in enhancing the tools capabilities online, with options to forensically track and capture live web data, and the users behaviour on SNSs would be implicit in tool development. This includes extending the functionality of tools that can extract artifacts that are specific for SNSs, such as wall posts, Internet cache, pictures, outlook mail, webmail, chat, Internet history, peer to peer, movie analysis, facial recognition and location analysis. Tools must be automated to extract data from SNSs in order to minimise the user's manual input error as well as to maximise the efficiency of the investigation. With the emerging technologies, opportunities of potential criminal misuse via SNSs are most likely to increase. Research limitations identified in Section 6.3 have shown that much future development of tools needed to accommodate popularity of SNSs with emerging new technologies.

The legality and standardisation of acquiring evidence from SNSs is a further area needing to be addressed by future research, although this is non-technical in nature, and driven by regulatory compliance imperatives initially. It is necessary to draw up a suitable international charter and standard for social network forensics, and interaction with relevant areas of law and the professional code of ethics will greatly contribute to our society in clarify the substantive truth. This will also minimise ambiguity in SNS investigations with overlapping or contested jurisdictional boundaries. Further to this, aggressive promotion of a qualification system and certification that is designed for social network investigation would be recommended, in order to get active and continued participation from digital forensic experts.

## 6.5 CONCLUSION

The main objective of this research was to evaluate tools in a systematic and forensically sound manner to measure the capability of extracting evidence from SNSs in different test scenarios. Through the background research performed in Chapter 2 and Chapter 3 an understanding was gained of how data is stored when people access SNSs, and the methods of evaluating evidence extraction tool capabilities. A method of 'extraction tools testing' was reviewed, and the baseline of data was generated on a target machine. The capability of the three chosen tools was tested and compared against the baseline data. A weighted numerical total is given based on the outcome of each case scenario before conclusions were drawn about the capability of each tool as a whole.

Research found that each tool has some capability in extracting evidence from SNSs, but is limited to some fragments of information posted on SNSs. It is noted that extracting completed data from SNSs is not possible with current tools tested in this research, due to the characteristics of SNSs, that data posted on the cloud space is volatile and not always remains on users hard disk. While it is positive news that each tool tested in this research has some capability in extraction of data posted on SNSs, tools need further development in parallel with rapidly changing technologies, in order to keep up to date with those emerging technologies.

Chapter six has concluded this research, which reflects on aspects of the research project such as how well each tool has met the aim and answer the research question and sub-questions laid out for this research in Section 3.2. Test scenario analysis results have been summarised and limitations of research are also highlighted. Revisions of test findings, research questions are discussed as well as proposing areas for future research. The research findings presented in this research may be valuable for law enforcement agents and digital forensic investigators to identify current issues and limitations of the tools, and for software vendors to recognise the limitations of the tools, so that thy can improve the tools for better extraction capability. Chapter 6 connects findings from this research to the potential areas of future research in the topic area.

# References


AccessData. (2011). Forensic Toolkit (FTK) Computer Forensics Software. Retrieved 2 July, 2011, from http://accessdata.com/products/computer-forensics/ftk

Ahn, Y.-Y., Han, S., Kwak, H., Moon, S., & Jeong, H. (2007). *Analysis of topological characteristics of huge online social networking services*. Paper presented at the Proceedings of the 16th international conference on World Wide Web, Banff, Alberta, Canada.

Anklam, P. (2007). *Net work: A practical guide to creating and sustaining networks at work and in the world*. Boston: Elsevier/Butterworth Heinemann.

Bascand, G. (2010). *Household Use of Information and Communication Technology: 2009*. Wellington: Statistics New Zealand

Bassett, R., Bass, L., & O'Brien, P. (2006). Computer Forensics: An Essential Ingredient for Cyber Security. *Journal of Information Science and Technology, 3*(1), 26.

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

Berghel, H. (2003). The discipline of Internet forensics. *Commun. ACM, 46*(8), 15-20. doi: 10.1145/859670.859687

Berghel, H. (2008). BRAP Forensics [Article]. *Communications of the ACM, 51*(6), 15-20.

Blincoe, R. (2008). Convicted forensics expert defends record. Retrieved 16 March, 2011, from http://www.v3.co.uk/v3-uk/news/1979776/convicted-forensics-expert-defends-record

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

Brown, C. L. T. (2009). *Computer Evidence: Collection and Preservation* (2nd ed.). Rockland, MA: Charles River Media, Inc.

Bryson, C., & Stevens, S. (2002). *Handbook of computer crime investigation : forensic tools and technology* London: Academic Press.

Busby, C., & Bellamy, P. (2011). *New Zealand Parliamentarians and Online Social Media*. Wellington, New Zealand: Parliamentary Library

CacheBack. (2011). Overview of CacheBack Retrieved 12 April, 2011, from http://www.cacheback.ca/overview.asp?id=3

Carrier, B. D., & Spafford, E. H. (2004). *An Event-based Digital Forensic Investigation framework.* Paper presented at the Digital Forensic Research Workshop, West Lafayett , Purdue University, USA.

Carter, H. L., Foulger, T. S., & Ewbank, A. D. (2008). Have you Googled your teacher lately? *Phi Delta Kappan, 89*(9), 681-683.

Casey, E. (2000). *Digital Evidence and Computer Crime: Forensic Science, Computers*. Orlando, FL: Academic Press, Inc.

Casey, E. (2002). *Handbook of computer crime investigation : forensic tools and technology*: San Diego, Calif. ; London : Academic, 2002.

Casey, E. (2004). *Digital evidence and computer crime : forensic science, computers and the Internet*: London ; San Diego, Calif. : Academic Press, c2004.

Cheng, J., Hoffman, J., LaMarche, T., Tavil, A., Yavad, A., & Kim, S. (2009). *Forensics Tools for Social Network Security Solutions*. Paper presented at the Proceedings of Student-Faculty Research Day, White Plains, NY 10606, USA.

Chua, M. (2009). Social networking sites a hotbed for cyber crime. Retrieved 19 July, 2011, from http://www.networkworld.com/news/2009/012309-social-networking-sites-a-hotbed.html

Cox, N. (2006). Cyber-crime Jurisdiction in New Zealand *Cyber-crime Jurisdiction: A Global Survey* (1st ed., Vol. 11, pp. 177 - 188 ). The Hague: T.M.C Asser Press.

Coyle, C. L., & Vaughn, H. (2008). Social networking: Communication revolution or evolution? *Bell Labs Technical Journal, 13*(2), 13-17. doi: 10.1002/bltj.20298

CyberSecurity-Institute. (2004). Code of Ethics and Conduct. Retrieved 15 March, 2011, from http://www.cybersecurityinstitute.biz/training/ethicsconduct.htm

Daniel, L. E., & Daniel, L. E. (2012). Chapter 31 - Internet History (Web and Browser Caching) *Digital Forensics for Legal Professionals* (pp. 213-218). Boston: Syngress.

De Montalk, J. (2011). MPs take to Twitter and Facebook [Article]. *New Zealand Doctor*, 14-14.

T. Deverson. (Ed.). (1999). New York: Oxford University Press.

e-fense. (2011). Helix3 Pro. Retrieved 3 July, 2011, from http://www.e-fense.com/helix3pro.php

eMarketer. (2011). Facebook Drives US Social Network Ad Spending Past $3 Billion in 2011. Retrieved 19 June, 2011, from http://www.emarketer.com/Article.aspx?R=1008180

EnCase Forensic for Law Enforcement. (2011). *Guidance Software*. Retrieved from http://www.guidancesoftware.com/WorkArea/linkit.aspx?LinkIdentifier=ID&ItemID=674

EnCase study guide. (2011). *Guidance Software*. Retrieved from http://www.encaseenterprise.com/downloads/getpdf.aspx?fl=.pdf

Forbes, T. (2011). Expert witness issues. *Law Society Gazette*(Feb 11).

Golden G. Richard, I., & Roussev, V. (2006). Next-generation digital forensics. *Commun. ACM, 49*(2), 76-80. doi: 10.1145/1113034.1113074

Guidance Software. (2011). EnCase® Forensic features. Retrieved 2 July, 2011, from http://www.guidancesoftware.com/forensic.htm - tab=1

Guo, Y., & Slay, J. (2010). Data Recovery Function Testing for Digital Forensic Tools. In K.-P. Chow & S. Shenoi (Eds.), *Advances in Digital Forensics VI* (Vol. 337, pp. 297-311): Springer Boston.

Guo, Y., Slay, J., & Beckett, J. (2009). Validation and verification of computer forensic software tools--Searching Function. *Digital Investigation, 6*(Supplement 1), S12-S22. doi: 10.1016/j.diin.2009.06.015

Haggerty, J. (2010). *Digital Forensics Investigations of Social Networks: Learning from Other Disciplines*. Paper presented at the Centre for Security, Communications and Network Research, University of Plymouth.

Hershensohn, J. (2005). *IT Forensics: the collection of and presentation of digital evidence*. Paper presented at the Information Security for South Africa - ISSA.

Intelligence, D. (2006). UltraBlock User Guide. In D. I. Ltd (Ed.), (p. 1): Digital Intelligence Ltd.

International Organization for Standardization. (1994). Accuracy (trueness and precision) of measurement methods and results - Part 2: Basic method for the determination of repeatability and reproducibility of a standard measurement method (Vol. ISO 5725-2:1994, p. 42).

Irons, A. (2007). *Teaching of computing - Teaching computer ethics to computer forensics student.* Paper presented at the 8th Annual Conference, University of Southampton, UK.

JAD Software. (2011a). Internet Evidence Finder v4 – Standard Edition. Retrieved 10 April, 2011, from http://www.jadsoftware.com/go/?page_id=141

JAD Software. (2011b). Internet Evidence Finder v4 – Standard Edition. Retrieved 30 October, 2011, from http://www.jadsoftware.com/go/?page_id=141

Jadhav, A. S., & Sonar, R. M. (2011). Framework for evaluation and selection of the software packages: A hybrid knowledge based system approach. *Journal of Systems and Software, 84*(8), 1394-1407. doi: 10.1016/j.jss.2011.03.034

Jones, K. J. (2003). Forensic Analysis of Internet Explorer Activity Files. from http://www.mcafee.com/us/resources/white-papers/foundstone/wp-pasco.pdf

Lewis, K., Kaufman, J., Gonzalez, M., Wimmer, A., & Christakis, N. (2008). Tastes, ties, and time: A new social network dataset using Facebook.com. *Social Networks, 30*(4), 330-342. doi: 10.1016/j.socnet.2008.07.002

Mason, R. O. (1986). Four ethical issues of the information age. *Management Information Systems Quarterly, 10*(1), 5-12.

McCarthy, H. (2009). Issues in digital evidence investigation Retrieved 12 March, 2011, from http://deforensics.blogspot.com/2009/01/issues-in-digital-evidence.html

McDonald, G., & Pak, P. C. (1996). It's all fair in love, war, and business: Cognitive philosophies in ethical decision making *Journal of Business Ethics, 15*(9), 973-996.

McKemmish, R. (1999). What is Forensic Computing? *Australian Institute of Criminology*(118), 1.

McKemmish, R. (2008). When is Digital Evidence Forensically Sound? In I. Ray & S. Shenoi (Eds.), *Advances in Digital Forensics IV* (Vol. 285, pp. 3-15): Springer Boston.

Meghanathan, N., Allam, S. R., & Moore, L. A. (2009). Tools and techniques for network forensics. *International Journal of Network Security & Its Applications (IJNSA), 1*(1), 14.

Micro Systemation XRY. (2011). What is XRY? Retrieved 18 July, 2011, from http://www.msab.com/xry/what-is-xry

Millard, D. E., & Ross, M. (2006). *Web 2.0: hypertext by any other name?* Paper presented at the Proceedings of the seventeenth conference on Hypertext and hypermedia, Odense, Denmark.

Net application. (2011). Top Browser Share Trend. Retrieved 23 October, 2011, from http://www.netmarketshare.com/browser-market-share.aspx?qprid=1

Neuman, W. L. (2003). *Social research methods: Qualitative and quantitative approaches* (5 ed.). New York: Allyn & Bacon.

NIJ. (2008). *Electronic crime scene investigation: a guide for first responders*. Washington, DC: U.S. Department of Justice

NIST. (2001). General test methodology for computer forensic tools. Retrieved 21 Oct 2011, from http://www.cftt.nist.gov/Test Methodology 7.doc

Norulzahrah M. Zainudin, M. M., David Llewellyn-Jones. (2010). *A Digital Forensic Investigation Model for Online Social Networking*. Liverpool John Moores University. Liverpool, United Kingdom.

Oh, J., Lee, S., & Lee, S. (2011). Advanced evidence collection and analysis of web browser activity. *Digital Investigation, 8, Supplement*(0), S62-S70. doi: 10.1016/j.diin.2011.05.008

Park, H. W., & Kluver, R. (2009). Trends in online networking among South Korean politicians -- A mixed-method approach. *Government Information Quarterly, 26*(3), 505-515. doi: 10.1016/j.giq.2009.02.008

Pollitt, M. (2008). Applying Traditional Forensic Taxonomy to Digital Forensics. In I. Ray & S. Shenoi (Eds.), *Advances in Digital Forensics IV* (Vol. 285, pp. 17-26): Springer Boston.

Rahaf, H., & Harfoush, R. (2009). *Yes we did an inside look at how social media built the Obama brand*: Berkeley, CA : New Riders, 2009.

Ravi Kumar Jain, B. (2007). Web Browser as a Forensic Computing Tool [Article]. *ICFAI Journal of Information Technology*, 47-57.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence, 1*(3), 10.

Sansurooah, K. (2006). *Taxonomy of computer forensics methodologies and procedures for digital evidence seizure.* Paper presented at the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia.

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping Process of Digital Forensic Investigation Framework. *IJCSNS International Journal of Computer Science and Network Security, 8*(10), 163-169.

Statistics Korea. (2009). Internet Usage statistics. Retrieved 17 June, 2011, from http://meta.kosis.kr/bzmt/main.jsp?surv_id=12005&curYear=2009

Sultana, D. (2010). *1.8 Million New Zealanders interacting via social networking sites*: The Nielsen Company

SWGDE. (2007). SWGDE and SWGIT Digital & Multimedia Evidence Glossary. Retrieved 26 June, 2011, from http://www.swgde.org/documents/archived-documents/2007-11-01 SWGDESWGIT Digital_Multimedia Evidence Glossary v2.2.pdf

Tassel, J. V. (2006). *Digital Rights Management: Protecting & Monetizing Content*. Boston: Focal.

Thomson, A. J., & Schmoldt, D. L. (2001). Ethics in computer software design and development. *Computers and Electronics in Agriculture, 30*(1-3), 85-102. doi: 10.1016/s0168-1699(00)00158-7

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*. New York: Springer.

William Lawrence, N., & Neuman, W. L. (2003). *Social research methods : qualitative and quantitative approaches / W. Lawrence Neuman*: Boston : Allyn and Bacon, c2003.

Wilsdon, T., & Slay, J. (2006). *Validation of forensic computing software utilizing black box testing technique*. Paper presented at the Proceedings of 4th Australian Digital Forensics Conference, Perth, Australia.

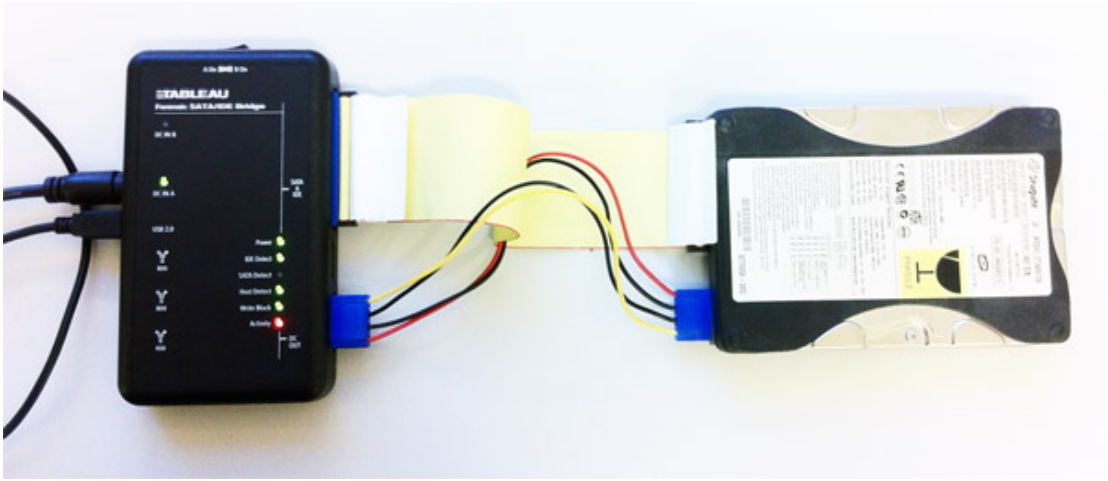
Wireshark. (2011). About Wireshark. Retrieved 2 July, 2011, from http://www.wireshark.org/about.html

**Appendix**

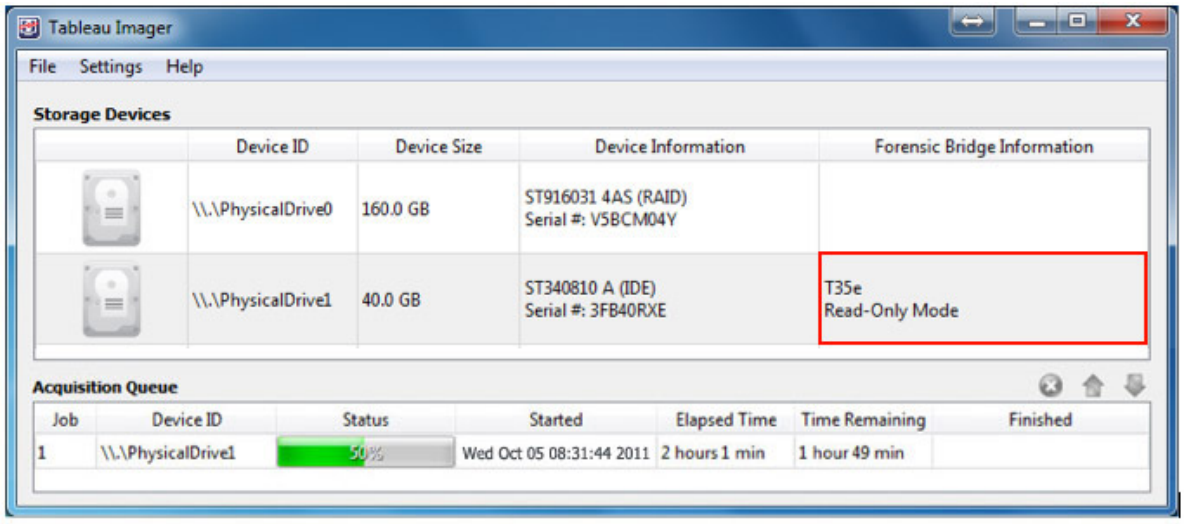
# Appendix A - Testing Environments

## Appendix A-1 Data collection / Acquisition setting

Evidence hard drive has been extracted from the desktop pc and connected with the Tableau IDA forensic bridge for evidence imaging job. The below image shows the T35e connected to a 40GB hard disk extracted from PC (DELL). The Tableau is then connected to an imaging workstation (out of picture) via the provided USB cable. Power is provided to the extracted hard drive via the Tableau device as shown. For correct connectivity the IDE Detect, Host Detect and Write Block LEDs should be illuminated.

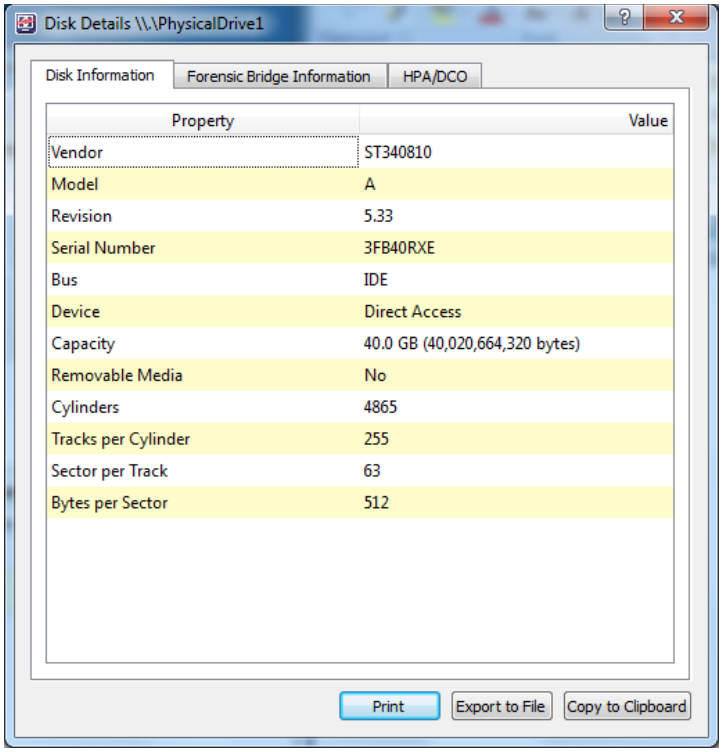


A Tableau Imaging software version 1.11 has been used to work with Tableau IDE forensic bridge. Below screenshot shows the Tableau software on the imaging workstation confirming Tableau connectivity to the target drive. Under 'Forensic Bridge Information' the entry for the T35e says 'Read Only Mode', which indicates that this hard drive is in forensically sound acquisition mode.

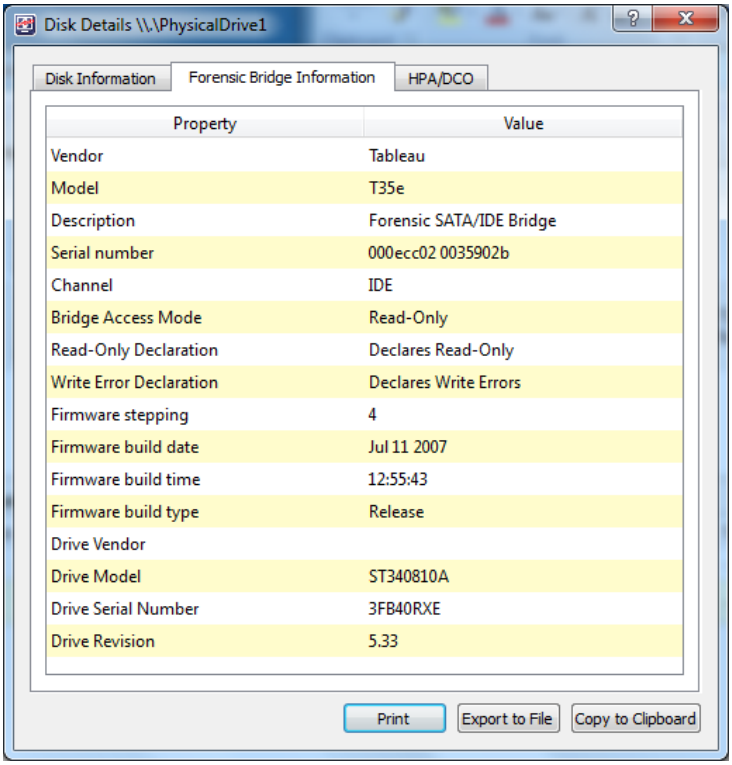


## Appendix A-2 Target Disk & Forensic Bridge information

Target evidence hard disk details captured from Tableau Imaging software




Target Disk Information




Forensic Bridge Information

## Device details shown in Tableau TIM Imaging software

```
--------------------------------Disk Information--------------------------------
Vendor: ST340810
Model: A
Revision: 5.33
Serial Number: 3FB40RXE
Bus: IDE
Device: Direct Access
Capacity: 40.0 GB (40,020,664,320 bytes)
Removable Media: No
Cylinders: 4865
Tracks per Cylinder: 255
Sector per Track: 63
Bytes per Sector: 512
------------------------------Bridge Information--------------------------------
Vendor: Tableau
Model: T35e
Description: Forensic SATA/IDE Bridge
Serial number: 000ecc02 0035902b
Channel: IDE
Bridge Access Mode: Read-Only
Read-Only Declaration: Declares Read-Only
Write Error Declaration: Declares Write Errors
Firmware stepping: 4
Firmware build date: Jul 11 2007
Firmware build time: 12:55:43
Firmware build type: Release
Drive Vendor:
Drive Model: ST340810A
Drive Serial Number: 3FB40RXE
Drive Revision: 5.33
------------------------------HPA/DCO Information-------------------------------
HPA Supported: Yes
HPA in Use: No           DCO Supported: Yes
DCO in Use: No           Security Supported: Yes
Security in Use: No
Reported Capacity: 40.0 GB (40,020,664,320 bytes)
HPA Capacity: 40.0 GB (40,020,664,320 bytes)
DCO Capacity: 40.0 GB (40,020,664,320 bytes)
```

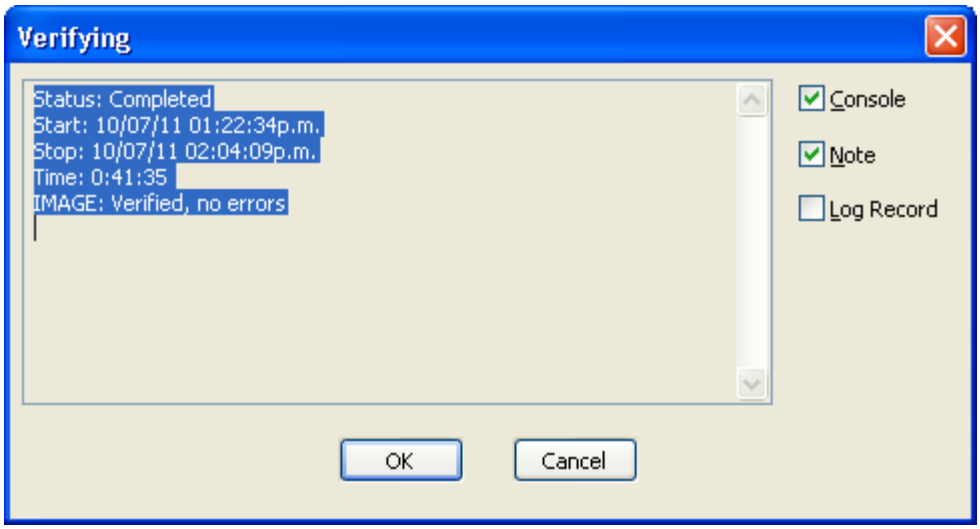
## Appendix A-3 Tableau Imager log

The report created imaging the target Hard drive using the Tableau T9 write block and the Tableau imaging software provides the information that is expected from a forensic imaging solution; start and end time, case ID and notes, source hard drive data including HPA / DCO / ATA status, T9 Write Block information and completed image data including MD5 / SHA 1 hashes.

```
----------------------Start of Tableau Imager Log entry-----------------------
Task: Disk to File
Status: Ok
Created: Wed Oct 05 08:31:44 2011
Started: Wed Oct 05 08:31:44 2011
Closed: Wed Oct 05 08:58:22 2011
Elapsed: 27 min
User: Jung Son
Case ID: JS-SNS-Evidence extraction from Windows 7 HDD
Case Notes: SNS-Evidence extraction from Windows 7 HDD
Imager App: Tableau Imager
Imager Ver: 1.11

--------------------------Source Disk---------------------------
Model: ST340810 A
S/N: 3FB40RXE
Firmware Revision: 5.33
Capacity in bytes reported Pwr-ON: 40,020,664,320 (40.0 GB)
Capacity in bytes reported by HPA: 40,020,664,320 (40.0 GB)
Capacity in bytes reported by DCO: 40,020,664,320 (40.0 GB)
HPA in use: No
DCO in use: No
ATA Security in use: No
Cable/Interface type: IDE
Blank check status: Not Blank

---------------Forensic Bridge / Write-Blocker-----------------
Vendor: Tableau
Model: T35e
Description: Forensic SATA/IDE Bridge
Serial number: 000ecc02 0035902b
Bridge Access Mode: Read-Only
Firmware build date: Jul 11 2007
Firmware build time: 12:55:43

----------------------Disk-to-File Results----------------------
Output file format: .e01/ewf
Compression: Maximize Speed
Chunk size in bytes: 2,147,483,648 (2.1 GB)
Chunks written: 17
Filename of first chunk: C:\Users\j.son\Desktop\PC-Evidence\IMAGE.E01
Total errors: 0
MD5:  82f764ce941751775b3f76400dea611d
SHA1: 8ea2df44a99d59796ea853ee7629b77968d690b6
-----------------------End of Tableau Imager Log entry------------------------
```

## Appendix A-4 Evidence image verification / Integrity check

For the purposes of validating the integrity of the image, a second image verification task has been performed using EnCase 6.19 and validated that the image verified by EnCase matched the hash of the image created with Tableau Imager.




| | |
|---|---|
| Name | IMAGE |
| Description | Physical Disk, 78,165,360 Sectors 37.3GB |
| Logical Size | 0 |
| Initialized Size | 0 |
| Physical Size | 512 |
| Starting Extent | 0S0 |
| File Extents | 1 |
| References | 0 |
| Physical Location | 0 |
| Physical Sector | 0 |
| Evidence File | IMAGE |
| File Identifier | 0 |
| Code Page | 0 |
| Full Path | JS-oct-07-2011\IMAGE |

**Device**

| | |
|---|---|
| Name | IMAGE |
| Actual Date | 10/05/11 08:31:44a.m. |
| Target Date | 10/05/11 08:31:44a.m. |
| File Path | B:\PC-Evidence Image\IMAGE.E01 |
| Case Number | JS-SNS-Evidence extraction from Windows 7 HDD |
| Examiner Name | Jung Son |
| Notes | SNS-Evidence extraction from Windows 7 HDD |
| Drive Type | Fixed |
| File Integrity | Completely Verified, 0 Errors |
| **Acquisition MD5** | **82f764ce941751775b3f76400dea611d** |
| **Verification MD5** | **82f764ce941751775b3f76400dea611d** |
| EnCase Version | 3.22g |

| | |
|---|---|
| System Version | Windows 7 |
| Write Blocked | Tableau |
| Is Physical | • |
| Raid Stripe Size | 0 |
| Error Granularity | 1 |
| Process ID | 0 |
| Index File | C:\Documents and Settings\mfit\Desktop\encase result-jung\IMAGE.Index |
| Read Errors | 0 |
| Missing Sectors | 0 |
| CRC Errors | 0 |
| Compression | Good |
| Total Size | 40,020,664,320 Bytes (37.3GB) |
| Total Sectors | 78,165,360 |
| Disk Signature | 24A3CAE0 |
| Partitions | Valid |

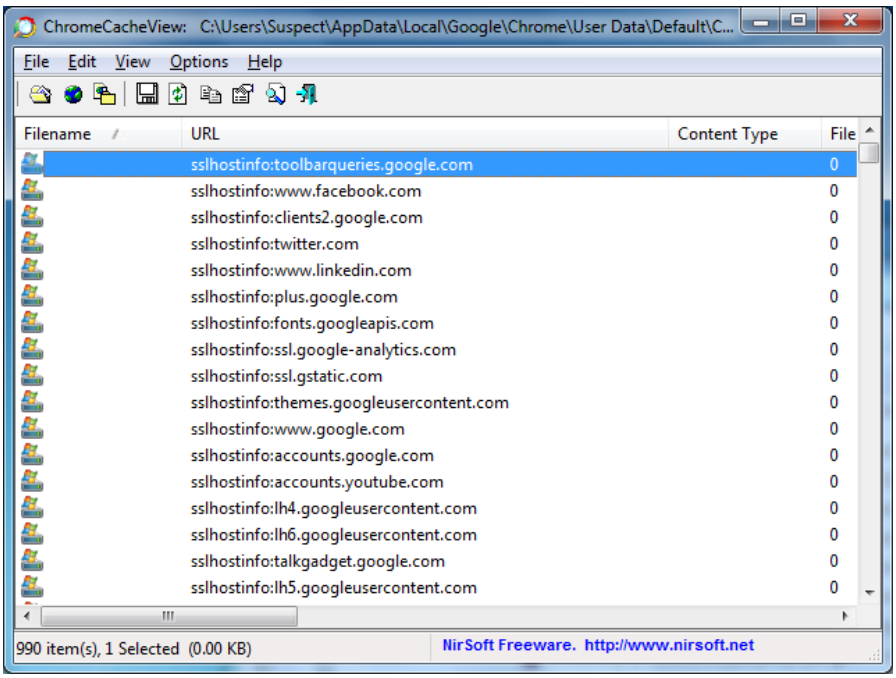
**Partitions**

| Name | Id | Type | Start Sector | Total Sectors | Size |
|---|---|---|---|---|---|
| | 07 | NTFS | 2,048 | 204,800 | 100MB |
| | 07 | NTFS | 206,848 | 77,955,072 | 37.2GB |

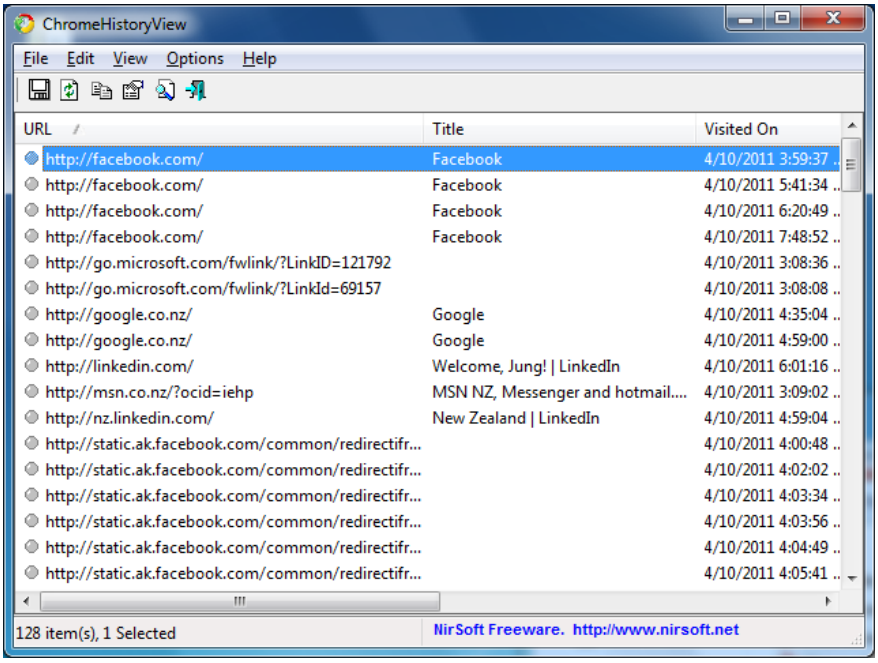
# Appendix B - Testing Data

## Appendix B-1 Expected Web History/Cache/Cookie from the Target Computer

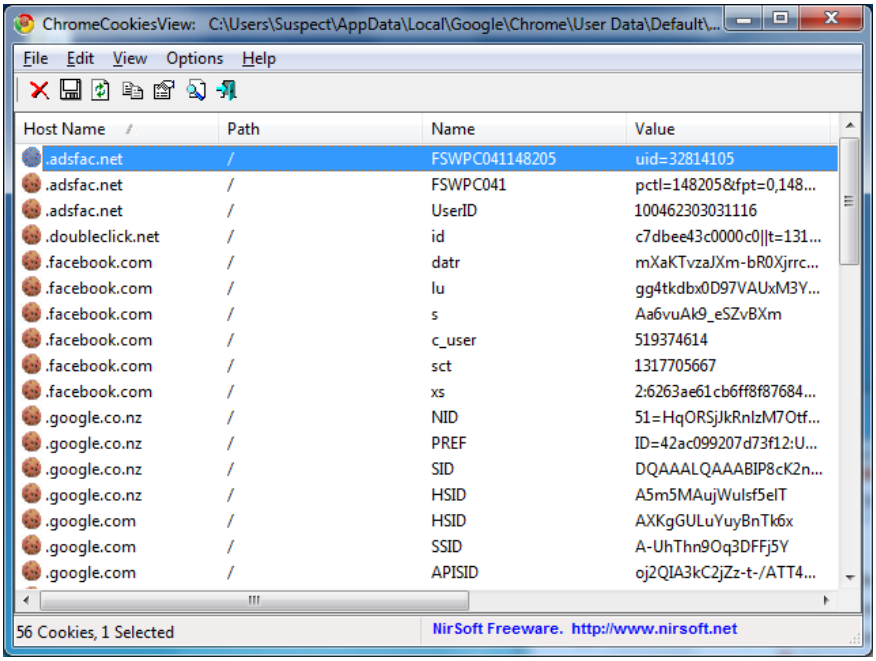
| | | History | Cache | Session/Cookies |
|---|---|---|---|---|
| Facebook | Firefox | 20 | 369 | 7 |
| | Chrome | 52 | 335 | 6 |
| | Safari | 11 | 264 | 0 |
| | IE | 21 | 316 | 1 |
| Twitter | Firefox | 33 | 49 | 10 |
| | Chrome | 35 | 46 | 9 |
| | Safari | 12 | 53 | 1 |
| | IE | 15 | 31 | 3 |
| LinkedIn | Firefox | 17 | 273 | 17 |
| | Chrome | 15 | 257 | 12 |
| | Safari | 11 | 300 | 0 |
| | IE | 6 | 173 | 3 |
| Google Plus | Firefox | 19 | 127 | 5 |
| | Chrome | 15 | 62 | 4 |
| | Safari | 2 | 6 | 1 |
| | IE | 3 | 86 | 1 |



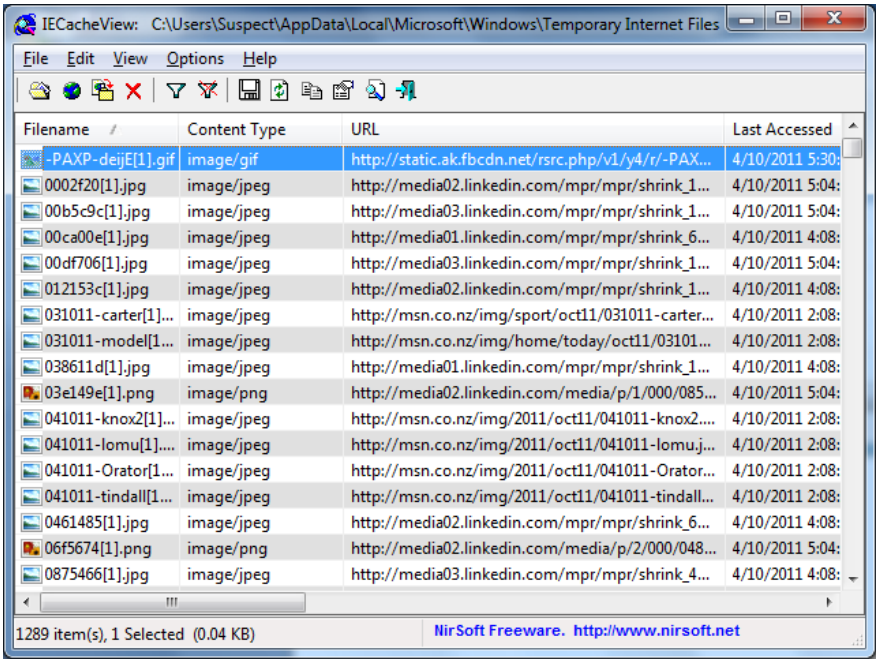

**Chrome Cache**



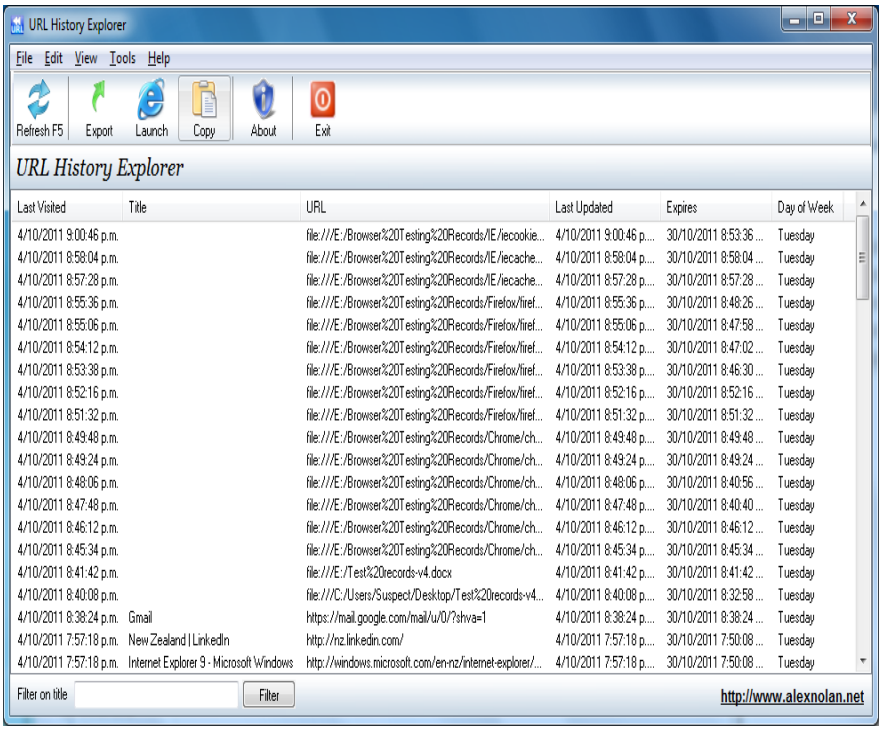

**Chrome History**



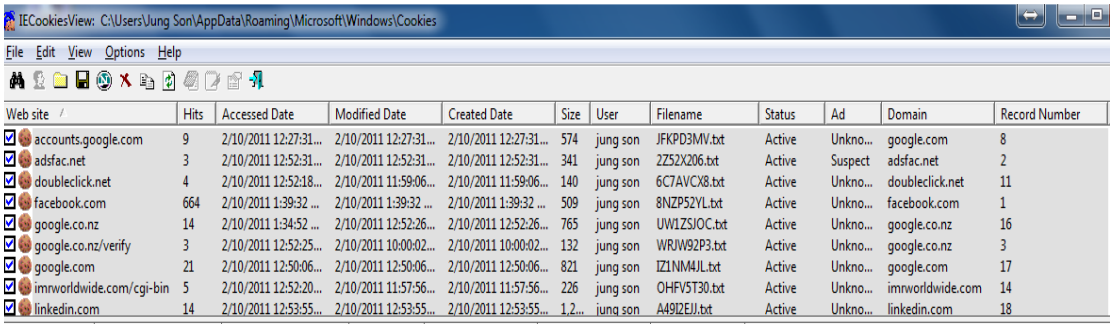

**Chrome Cookies**



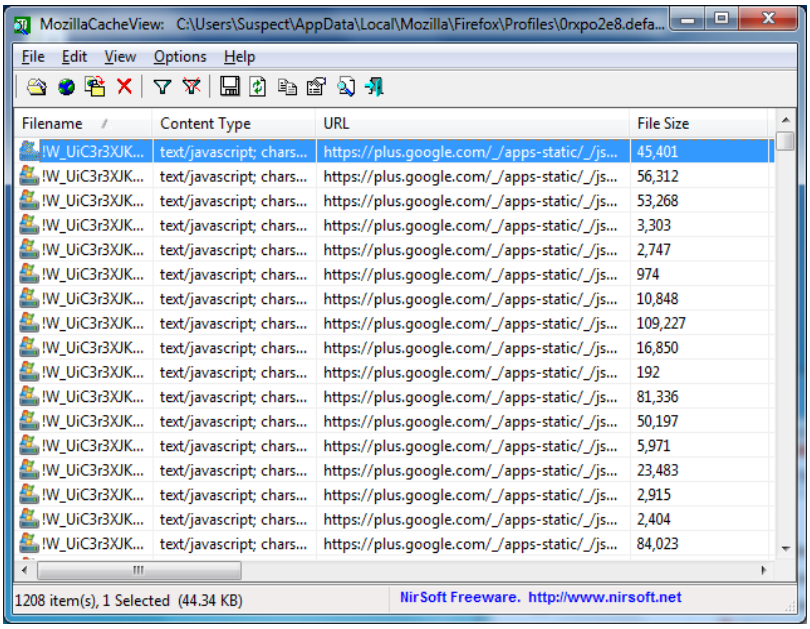

**IE Cache**



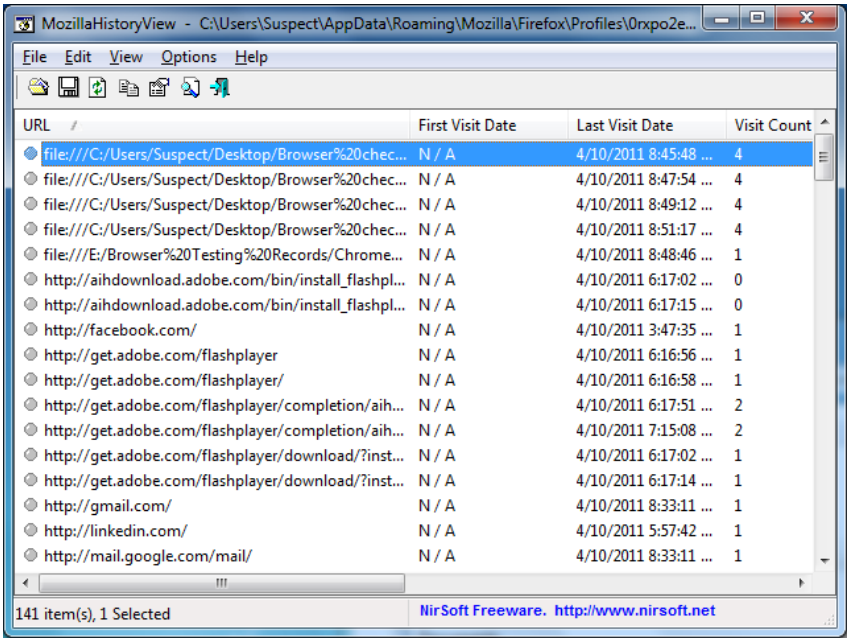

**IE History**



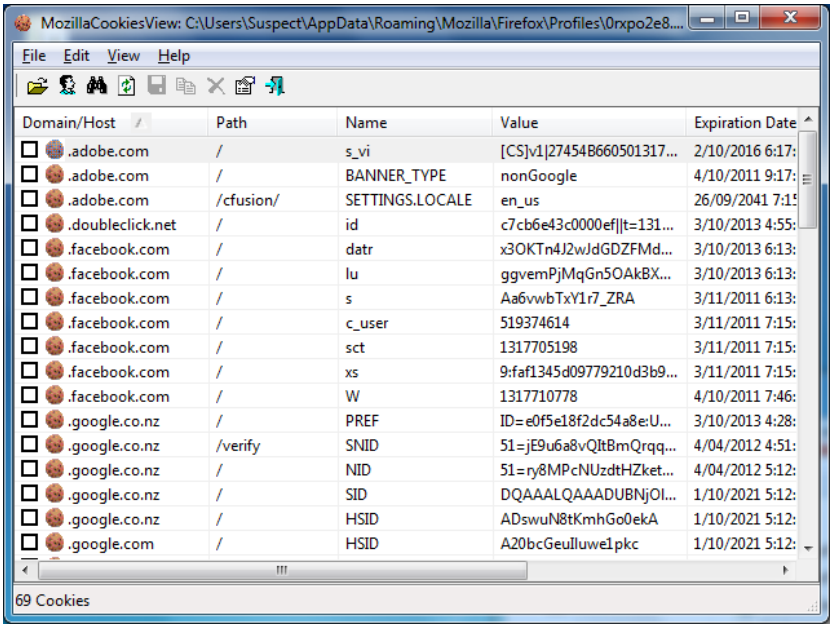

**IE Cookies**



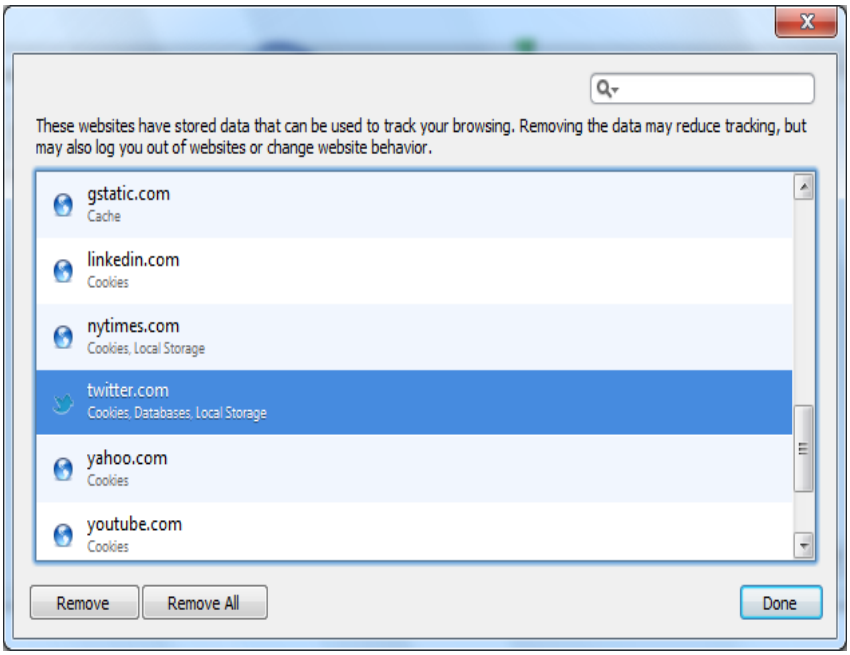

**Firefox Cache**



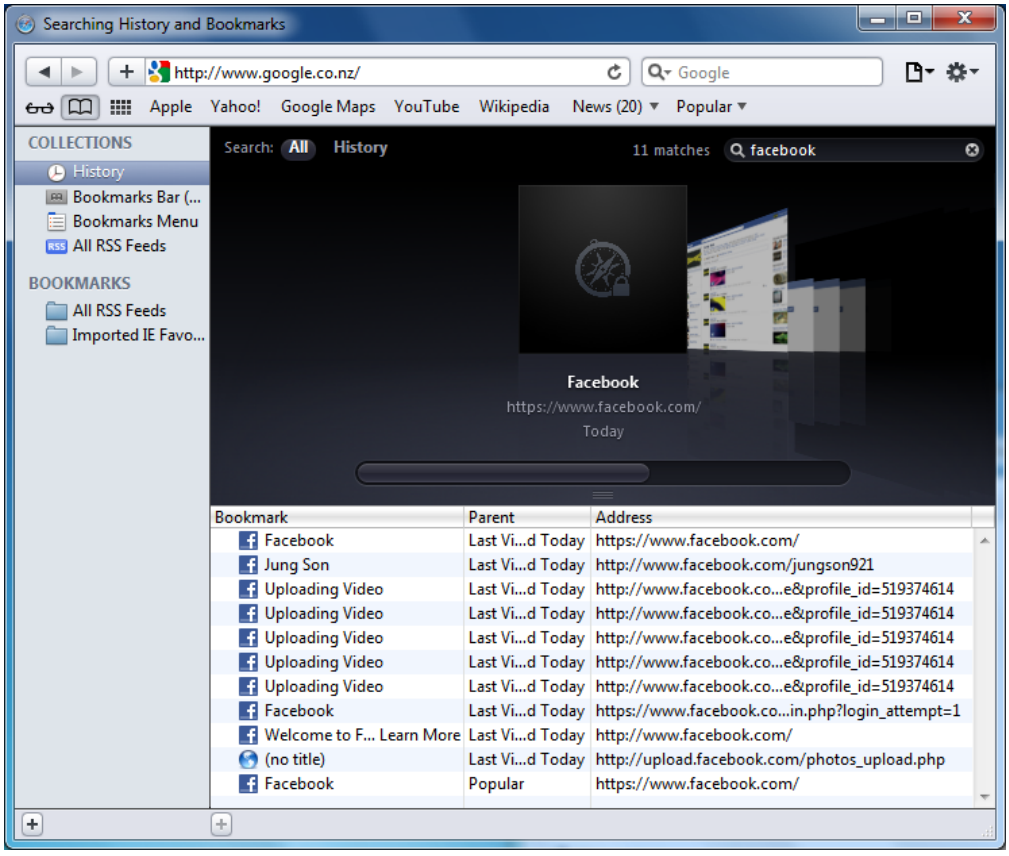

**Firefox History**




**Firefox Cookies**




**Safari Cache**




**Safari History**

## Appendix B-2 Prepared Facebook Chatting data

Prepared Facebook chatting messages - 5 conversations made from each of 4 different browsers.

| Browser | # | Sender | Receiver | Time | Message |
|---|---|---|---|---|---|
| Firefox | 1 | HisungKo | Jung Son | 05/Oct/2011 – 9:04pm | Or this Facebook slow |
| | 2 | Jung Son | HisungKo | 05/Oct/2011 – 9:05pm | OMG!!! did you know that I am doing this for my research? and to publish? |
| | 3 | HisungKo | Jung Son | 05/Oct/2011 – 9:06pm | Ha ha |
| | 4 | Jung Son | HisungKo | 05/Oct/2011 – 9:07pm | do you think I can use this as evidence? OMG! I have to do the whole thing again! Thanks!! |
| | 5 | HisungKo | Jung Son | 05/Oct/2011 – 9:08pm | Cool wife |
| Chrome | 1 | Jung Son | HisungKo | 05/Oct/2011 – 9:03pm | What are you doing now? I mean before you chat with me? |
| | 2 | HisungKo | Jung Son | 05/Oct/2011 – 9:04pm | I will cut ur |
| | 3 | HisungKo | Jung Son | 05/Oct/2011 – 9:04pm | U will never have |
| | 4 | HisungKo | Jung Son | 05/Oct/2011 – 9:04pm | U happy with dat? |
| | 5 | HisungKo | Jung Son | 05/Oct/2011 – 9:04pm | Internet too slow |
| Safari | 1 | HisungKo | Jung Son | 05/Oct/2011 – 9:09pm | I know I'm a great help |
| | 2 | Jung Son | HisungKo | 05/Oct/2011 – 9:10pm | seriously I have to delete the entire window system and do the same thing I have done yesterday again! |
| | 3 | Jung Son | HisungKo | 05/Oct/2011 – 9:10pm | THANKS!!! |
| | 4 | HisungKo | Jung Son | 05/Oct/2011 – 9:11pm | U could ve warn me |
| | 5 | HisungKo | Jung Son | 05/Oct/2011 – 9:11pm | U said just to have chat |
| IE | 1 | Jung Son | HisungKo | 05/Oct/2011 – 9:01pm | dlTekrk so wkwl Qkfdkwnj! TkfEoRkwl!! |
| | 2 | HisungKo | Jung Son | 05/Oct/2011 – 9:02pm | Wat? |
| | 3 | HisungKo | Jung Son | 05/Oct/2011 – 9:02pm | Ok. |
| | 4 | HisungKo | Jung Son | 05/Oct/2011 – 9:02pm | Wat kinda business? |
| | 5 | Jung Son | HisungKo | 05/Oct/2011 – 9:03pm | de ddal bang business |

## Appendix B-3 Prepared Wall Post Status update

Wall post and Status update has been posted manually to prepare test data. Posts have been made from 4 different browsers with 5 evidenced posts on each service.

| Service | Evidence | | Firefox 7.0.1 | Chrome 14.0 | Safari 5.1 | IE 9 |
|---|---|---|---|---|---|---|
| Facebook | Evidence 1 | Time | 4/Oct/2011 – 3:49pm | 4/Oct/2011 – 4:03pm | 4/Oct/2011 – 4:09pm | 4/Oct/2011 – 4:17pm |
| | | Post | Forensic investigation test post Facebook – 01 (firefox) | Forensic investigation test post Facebook – 01 (Chrome) | Forensic investigation test post Facebook – 01 (Safari) | Forensic investigation test post Facebook – 01 (IE) |
| | Evidence 2 | Time | 4/Oct/2011 – 3:54pm | 4/Oct/2011 – 4:03pm | 4/Oct/2011 – 4:10pm | 4/Oct/2011 – 4:19pm |
| | | Post | Forensic investigation test post Facebook – 02 (firefox) | Forensic investigation test post Facebook – 02 (Chrome) | Forensic investigation test post Facebook – 02 (Safari) | Forensic investigation test post Facebook – 02 (IE) |
| | Evidence 3 | Time | 4/Oct/2011 – 3:55pm | 4/Oct/2011 – 4:04pm | 4/Oct/2011 – 4:11pm | 4/Oct/2011 – 4:20pm |
| | | Post | Forensic investigation test post Facebook – 03 (firefox) | Forensic investigation test post Facebook – 03 (Chrome) | Forensic investigation test post Facebook – 03 (Safari) | Forensic investigation test post Facebook – 03 (IE) |
| | Evidence 4 | Time | 4/Oct/2011 – 3:56pm | 4/Oct/2011 – 4:05pm | 4/Oct/2011 – 4:12pm | 4/Oct/2011 – 4:22pm |
| | | Post | Forensic investigation test post Facebook – 04 (firefox) | Forensic investigation test post Facebook – 04 (Chrome) | Forensic investigation test post Facebook – 04 (Safari) | Forensic investigation test post Facebook – 04 (IE) |
| | Evidence 5 | Time | 4/Oct/2011 – 3:57pm | 4/Oct/2011 – 4:06pm | 4/Oct/2011 – 4:14pm | 4/Oct/2011 – 4:23pm |
| | | Post | Forensic investigation test post Facebook – 05 (firefox) | Forensic investigation test post Facebook – 05 (Chrome) | Forensic investigation test post Facebook – 05 (Safari) | Forensic investigation test post Facebook – 05 (IE) |
| Twitter | Evidence 1 | Time | 4/Oct/2011 – 4:30pm | 4/Oct/2011 – 4:36pm | 4/Oct/2011 – 4:41pm | 4/Oct/2011 – 4:46pm |
| | | Post | Forensic investigation test post Twitter – 01 (firefox) | Forensic investigation test post Twitter – 01 (Chrome) | Forensic investigation test post Twitter – 01 (Safari) | Forensic investigation test post Twitter – 01 (IE) |
| | Evidence 2 | Time | 4/Oct/2011 – 4:32pm | 4/Oct/2011 – 4:37pm | 4/Oct/2011 – 4:42pm | 4/Oct/2011 – 4:48pm |
| | | Post | Forensic investigation test post Twitter – 02 (firefox) | Forensic investigation test post Twitter – 02 (Chrome) | Forensic investigation test post Twitter – 02 (Safari) | Forensic investigation test post Twitter – 02 (IE9) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Evidence 3 | Time | 4/Oct/2011 – 4:32pm | 4/Oct/2011 – 4:38pm | 4/Oct/2011 – 4:43pm | 4/Oct/2011 – 4:49pm |
| | | Post | Forensic investigation test post Twitter – 03 (firefox) | Forensic investigation test post Twitter – 03 (Chrome) | Forensic investigation test post Twitter – 03 (Safari) | Forensic investigation test post Twitter – 03 (IE9) |
| | Evidence 4 | Time | 4/Oct/2011 – 4:33pm | 4/Oct/2011 – 4:39pm | 4/Oct/2011 – 4:44pm | 4/Oct/2011 – 4:49pm |
| | | Post | Forensic investigation test post Twitter – 04 (firefox) | Forensic investigation test post Twitter – 04 (Chrome) | Forensic investigation test post Twitter – 04 (Safari) | Forensic investigation test post Twitter – 04 (IE9) |
| | Evidence 5 | Time | 4/Oct/2011 – 4:34pm | 4/Oct/2011 – 4:40pm | 4/Oct/2011 – 4:45pm | 4/Oct/2011 – 4:50pm |
| | | Post | Forensic investigation test post Twitter – 05 (firefox) | Forensic investigation test post Twitter – 05 (Chrome) | Forensic investigation test post Twitter – 05 (Safari) | Forensic investigation test post Twitter – 05 (IE9) |
| LinkedIn | Evidence 1 | Time | 4/Oct/2011 – 4:54pm | 4/Oct/2011 – 4:59pm | 4/Oct/2011 – 5:04pm | 4/Oct/2011 – 5:08pm |
| | | Post | Forensic investigation test post linkedin – 01 (firefox) | Forensic investigation test post linkedin – 01 (Chrome) | Forensic investigation test post linkedin – 01 (Safari) | Forensic investigation test post linkedin – 01 (IE) |
| | Evidence 2 | Time | 4/Oct/2011 – 4:55pm | 4/Oct/2011 – 5:00pm | 4/Oct/2011 – 5:04pm | 4/Oct/2011 – 5:09pm |
| | | Post | Forensic investigation test post linkedin – 02 (firefox) | Forensic investigation test post linkedin – 02 (Chrome) | Forensic investigation test post linkedin – 02 (Safari) | Forensic investigation test post linkedin – 02 (IE) |
| | Evidence 3 | Time | 4/Oct/2011 – 4:56pm | 4/Oct/2011 – 5:01pm | 4/Oct/2011 – 5:05pm | 4/Oct/2011 – 5:09pm |
| | | Post | Forensic investigation test post linkedin – 03 (firefox) | Forensic investigation test post linkedin – 03 (Chrome) | Forensic investigation test post linkedin – 03 (Safari) | Forensic investigation test post linkedin – 03 (IE) |
| | Evidence 4 | Time | 4/Oct/2011 – 4:57pm | 4/Oct/2011 – 5:01pm | 4/Oct/2011 – 5:06pm | 4/Oct/2011 – 5:10pm |
| | | Post | Forensic investigation test post linkedin – 04 (firefox) | Forensic investigation test post linkedin – 04 (Chrome) | Forensic investigation test post linkedin – 04 (Safari) | Forensic investigation test post linkedin – 04 (IE) |
| | Evidence 5 | Time | 4/Oct/2011 – 4:58pm | 4/Oct/2011 – 5:02pm | 4/Oct/2011 – 5:07pm | 4/Oct/2011 – 5:11pm |
| | | Post | Forensic investigation test post linkedin – 05 (firefox) | Forensic investigation test post linkedin – 05 (Chrome) | Forensic investigation test post linkedin – 05 (Safari) | Forensic investigation test post linkedin – 05 (IE) |

| | | | | | | |
|---|---|---|---|---|---|---|
| Google + | Evidence 1 | Time | 4/Oct/2011 – 5:14pm | 4/Oct/2011 – 5:21pm | 4/Oct/2011 – 5:26pm | 4/Oct/2011 – 5:32pm |
| | | Post | Forensic investigation test post Google Plus – 01 (firefox) | Forensic investigation test post Google Plus – 01 (Chrome) | Forensic investigation test post Google Plus – 01 (Safari) | Forensic investigation test post Google Plus – 01 (IE) |
| | Evidence 2 | Time | 4/Oct/2011 – 5:15pm | 4/Oct/2011 – 5:21pm | 4/Oct/2011 – 5:27pm | 4/Oct/2011 – 5:33pm |
| | | Post | Forensic investigation test post Google Plus – 02 (firefox) | Forensic investigation test post Google Plus – 02 (Chrome) | Forensic investigation test post Google Plus – 02 (Safari) | Forensic investigation test post Google Plus – 02 (IE) |
| | Evidence 3 | Time | 4/Oct/2011 – 5:16pm | 4/Oct/2011 – 5:22pm | 4/Oct/2011 – 5:27pm | 4/Oct/2011 – 5:33pm |
| | | Post | Forensic investigation test post Google Plus – 03 (firefox) | Forensic investigation test post Google Plus – 03 (Chrome) | Forensic investigation test post Google Plus – 03 (Safari) | Forensic investigation test post Google Plus – 03 (IE) |
| | Evidence 4 | Time | 4/Oct/2011 – 5:16pm | 4/Oct/2011 – 5:23pm | 4/Oct/2011 – 5:27pm | 4/Oct/2011 – 5:33pm |
| | | Post | Forensic investigation test post Google Plus – 04 (firefox) | Forensic investigation test post Google Plus – 04 (Chrome) | Forensic investigation test post Google Plus – 04 (Safari) | Forensic investigation test post Google Plus – 04 (IE) |
| | Evidence 5 | Time | 4/Oct/2011 – 5:17pm | 4/Oct/2011 – 5:23pm | 4/Oct/2011 – 5:28pm | 4/Oct/2011 – 5:33pm |
| | | Post | Forensic investigation test post Google Plus – 05 (firefox) | Forensic investigation test post Google Plus – 05 (Chrome) | Forensic investigation test post Google Plus – 05 (Safari) | Forensic investigation test post Google Plus – 05 (IE) |

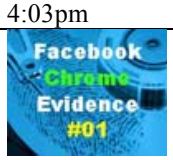
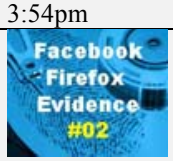
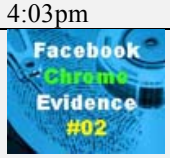
## Appendix B-4 Comments / Reply / Like

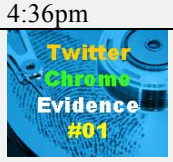
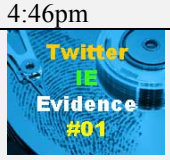
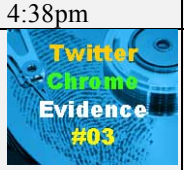
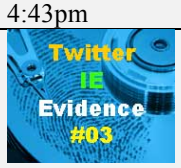
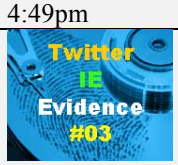
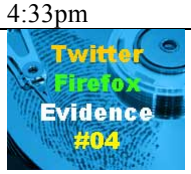
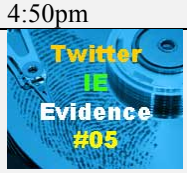
| Service | # | | Firefox 7.0.1 | Chrome 14.0 | Safari 5.1 | IE 9 |
|---|---|---|---|---|---|---|
| Facebook | 1 | Time | 4/Oct/2011 – 5:38pm | 4/Oct/2011 – 5:41pm | 4/Oct/2011 – 5:43pm | 4/Oct/2011 – 5:45pm |
| | | Comment /Like | Facebook Comment - Firefox - 01 | Facebook Comment - Chrome - 01 | Facebook Comment - Safari - 01 | Facebook Comment - IE - 01 |
| | 2 | Time | 4/Oct/2011 – 5:38pm | 4/Oct/2011 – 5:42pm | 4/Oct/2011 – 5:43pm | 4/Oct/2011 – 5:45pm |
| | | Comment /Like | Facebook Comment - Firefox - 02 | Facebook Comment - Chrome - 02 | Facebook Comment - Safari - 02 | Facebook Comment - IE - 02 |
| | 3 | Time | 4/Oct/2011 – 5:39pm | 4/Oct/2011 – 5:42pm | 4/Oct/2011 – 5:43pm | 4/Oct/2011 – 5:45pm |
| | | Comment /Like | Facebook Comment - Firefox - 03 | Facebook Comment - Chrome - 03 | Facebook Comment - Safari - 03 | Facebook Comment - IE - 03 |
| | 4 | Time | 4/Oct/2011 – 5:39pm | 4/Oct/2011 – 5:42pm | 4/Oct/2011 – 5:43pm | 4/Oct/2011 – 5:45pm |
| | | Comment /Like | Facebook Comment - Firefox - 04 | Facebook Comment - Chrome - 04 | Facebook Comment - Safari – 04 | Facebook Comment - IE - 04 |
| | 5 | Time | 4/Oct/2011 – 5:40pm | 4/Oct/2011 – 5:42pm | 4/Oct/2011 – 5:44pm | 4/Oct/2011 – 5:45pm |
| | | Comment /Like | Facebook Comment - Firefox - 05 | Facebook Comment - Chrome - 05 | Facebook Comment - Safari - 05 | Facebook Comment - IE - 05 |
| Twitter | 1 | Time | 4/Oct/2011 – 5:47pm | 4/Oct/2011 – 5:50pm | 4/Oct/2011 – 5:53pm | 4/Oct/2011 – 5:56pm |
| | | Comment | @jung921 Twitter Comment - Firefox - 01 | @jung921 Twitter Comment - Chrome - 01 | @jung921 Twitter Comment - Safari - 01 | @jung921 Twitter Comment - IE - 01 |
| | 2 | Time | 4/Oct/2011 – 5:47pm | 4/Oct/2011 – 5:50pm | 4/Oct/2011 – 5:53pm | 4/Oct/2011 – 5:56pm |
| | | Comment | @jung921 Twitter Comment - Firefox - 02 | @jung921 Twitter Comment - Chrome - 02 | @jung921 Twitter Comment - Safari - 02 | @jung921 Twitter Comment - IE - 02 |
| | 3 | Time | 4/Oct/2011 – 5:47pm | 4/Oct/2011 – 5:50pm | 4/Oct/2011 – 5:53pm | 4/Oct/2011 – 5:56pm |
| | | Comment | @jung921 Twitter Comment - Firefox - 03 | @jung921 Twitter Comment - Chrome - 03 | @jung921 Twitter Comment - Safari - 03 | @jung921 Twitter Comment - IE - 03 |
| | 4 | Time | 4/Oct/2011 – 5:47pm | 4/Oct/2011 – 5:50pm | 4/Oct/2011 – 5:53pm | 4/Oct/2011 – 5:56pm |
| | | Comment | @jung921 Twitter Comment - Firefox - 04 | @jung921 Twitter Comment - Chrome - 04 | @jung921 Twitter Comment - Safari - 04 | @jung921 Twitter Comment - IE - 04 |
| | 5 | Time | 4/Oct/2011 – 5:47pm | 4/Oct/2011 – 5:51pm | 4/Oct/2011 – 5:53pm | 4/Oct/2011 – 5:56pm |
| | | Comment | @jung921 Twitter | @jung921 Twitter | @jung921 Twitter | @jung921 Twitter |

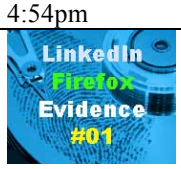
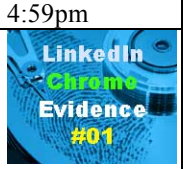
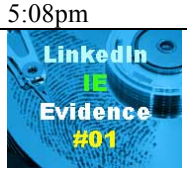
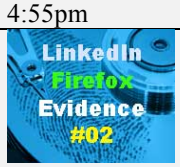
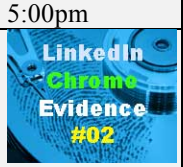
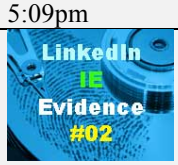
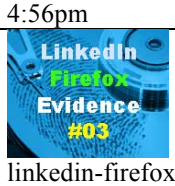
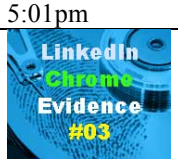
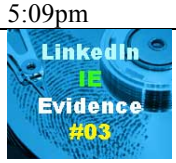
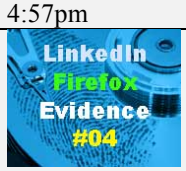
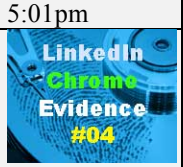
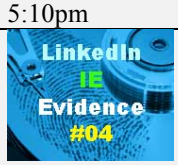
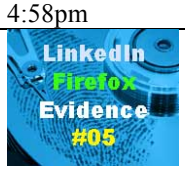
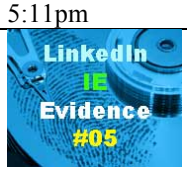
| | | | | | | |
|---|---|---|---|---|---|---|
| | | | Comment - Firefox - 05 | Comment - Chrome - 05 | Comment - Safari - 05 | Comment - IE - 05 |
| LinkedIn | 1 | Time | 4/Oct/2011 – 5:59pm | 4/Oct/2011 – 6:01pm | 4/Oct/2011 – 6:04pm | 4/Oct/2011 – 6:05pm |
| | | Comment /Like | Linkedin Comment - Firefox - 01 | Linkedin Comment - Chrome - 01 | Linkedin Comment - Safari - 01 | Linkedin Comment - IE - 01 |
| | 2 | Time | 4/Oct/2011 – 5:59pm | 4/Oct/2011 – 6:01pm | 4/Oct/2011 – 6:04pm | 4/Oct/2011 – 6:05pm |
| | | Comment /Like | Linkedin Comment - Firefox - 02 | Linkedin Comment - Chrome - 02 | Linkedin Comment - Safari - 02 | Linkedin Comment - IE - 02 |
| | 3 | Time | 4/Oct/2011 – 5:59pm | 4/Oct/2011 – 6:01pm | 4/Oct/2011 – 6:04pm | 4/Oct/2011 – 6:05pm |
| | | Comment /Like | Linkedin Comment - Firefox - 03 | Linkedin Comment - Chrome - 03 | Linkedin Comment - Safari - 03 | Linkedin Comment - IE - 03 |
| | 4 | Time | 4/Oct/2011 – 6:00pm | 4/Oct/2011 – 6:01pm | 4/Oct/2011 – 6:04pm | 4/Oct/2011 – 6:05pm |
| | | Comment /Like | Linkedin Comment - Firefox - 04 | Linkedin Comment - Chrome - 04 | Linkedin Comment - Safari - 04 | Linkedin Comment - IE - 04 |
| | 5 | Time | 4/Oct/2011 – 6:00pm | 4/Oct/2011 – 6:02pm | 4/Oct/2011 – 6:05pm | 4/Oct/2011 – 6:05pm |
| | | Comment /Like | Linkedin Comment - Firefox - 05 | Linkedin Comment - Chrome - 05 | Linkedin Comment - Safari - 05 | Linkedin Comment - IE - 05 |
| Google + | 1 | Time | 4/Oct/2011 – 6:08pm | 4/Oct/2011 – 6:09pm | 4/Oct/2011 – 6:11pm | 4/Oct/2011 – 6:11pm |
| | | Comment | GPlus-Comment-Firefox-01 | GPlus-Comment-Chrome-01 | GPlus-Comment-Safari-01 | GPlus-Comment-IE-01 |
| | 2 | Time | 4/Oct/2011 – 6:08pm | 4/Oct/2011 – 6:09pm | 4/Oct/2011 – 6:11pm | 4/Oct/2011 – 6:12pm |
| | | Comment | GPlus-Comment-Firefox-02 | GPlus-Comment-Chrome-02 | GPlus-Comment-Safari-02 | GPlus-Comment-IE-02 |
| | 3 | Time | 4/Oct/2011 – 6:08pm | 4/Oct/2011 – 6:09pm | 4/Oct/2011 – 6:11pm | 4/Oct/2011 – 6:12pm |
| | | Comment | GPlus-Comment-Firefox-03 | GPlus-Comment-Chrome-03 | GPlus-Comment-Safari-03 | GPlus-Comment-IE-03 |
| | 4 | Time | 4/Oct/2011 – 6:08pm | 4/Oct/2011 – 6:09pm | 4/Oct/2011 – 6:11pm | 4/Oct/2011 – 6:12pm |
| | | Comment | GPlus-Comment-Firefox-04 | GPlus-Comment-Chrome-04 | GPlus-Comment-Safari-04 | GPlus-Comment-IE-04 |
| | 5 | Time | 4/Oct/2011 – 6:08pm | 4/Oct/2011 – 6:10pm | 4/Oct/2011 – 6:11pm | 4/Oct/2011 – 6:12pm |
| | | Comment | GPlus-Comment-Firefox-05 | GPlus-Comment-Chrome-05 | GPlus-Comment-Safari-05 | GPlus-Comment-IE-05 |

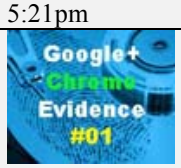
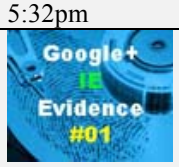
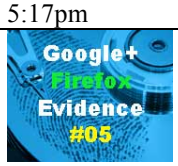
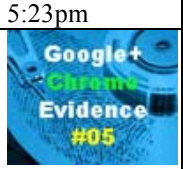
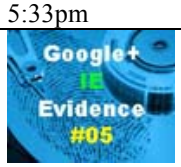
## Appendix B-5 Uploaded/Watched pictures (prepared)

Testing pictures have been uploaded manually into each of 4 different SNSs. Images have been uploaded from 4 different browsers with 5 different images on each site.

| Service | Evidence | | Firefox 7.0.1 | Chrome 14.0 | Safari 5.1 | IE 9 |
|---|---|---|---|---|---|---|
| Facebook | Evidence 1 | Time | 4/Oct/2011 – 3:49pm | 4/Oct/2011 – 4:03pm | 4/Oct/2011 – 4:09pm | 4/Oct/2011 – 4:17pm |
| | | Image |  facebook-firefox-01.jpg |  facebook-chrome-01.jpg |  facebook-safari-01.jpg |  facebook-ie-01.jpg |
| | Evidence 2 | Time | 4/Oct/2011 – 3:54pm | 4/Oct/2011 – 4:03pm | 4/Oct/2011 – 4:10pm | 4/Oct/2011 – 4:19pm |
| | | Image |  facebook-firefox-02.jpg |  facebook-chrome-02.jpg |  facebook-safari-02.jpg |  facebook-ie-02.jpg |
| | Evidence 3 | Time | 4/Oct/2011 – 3:55pm | 4/Oct/2011 – 4:04pm | 4/Oct/2011 – 4:11pm | 4/Oct/2011 – 4:20pm |
| | | Image |  facebook-firefox-03.jpg |  facebook-chrome-03.jpg |  facebook-safari-03.jpg |  facebook-ie-03.jpg |
| | Evidence 4 | Time | 4/Oct/2011 – 3:56pm | 4/Oct/2011 – 4:05pm | 4/Oct/2011 – 4:12pm | 4/Oct/2011 – 4:22pm |
| | | Image |  facebook-firefox-04.jpg |  facebook-chrome-04.jpg |  facebook-safari-04.jpg |  facebook-ie-04.jpg |
| | Evidence 5 | Time | 4/Oct/2011 – 3:57pm | 4/Oct/2011 – 4:06pm | 4/Oct/2011 – 4:14pm | 4/Oct/2011 – 4:23pm |
| | | Image |  facebook-firefox-05.jpg |  facebook-chrome-05.jpg |  facebook-safari-05.jpg |  facebook-ie-05.jpg |

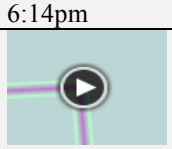
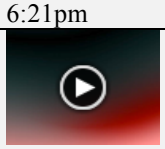
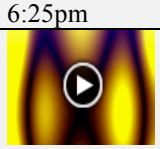
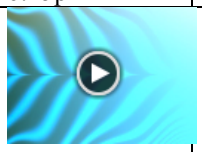
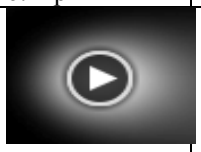
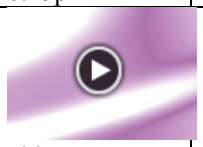
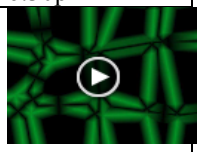
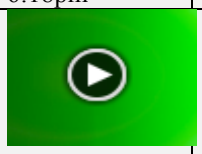
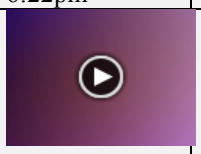
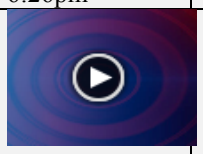
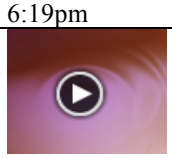
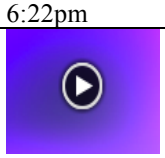
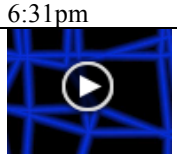
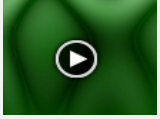
| | | | | | | |
|---|---|---|---|---|---|---|
| Twitter | Evidence 1 | Time | 4/Oct/2011 – 4:30pm | 4/Oct/2011 – 4:36pm | 4/Oct/2011 – 4:41pm | 4/Oct/2011 – 4:46pm |
| | | Image |  twitter-firefox-01.jpg |  twitter-chrome-01.jpg |  twitter-safari-01.jpg |  twitter-ie-01.jpg |
| | Evidence 2 | Time | 4/Oct/2011 – 4:32pm | 4/Oct/2011 – 4:37pm | 4/Oct/2011 – 4:42pm | 4/Oct/2011 – 4:48pm |
| | | Image |  twitter-firefox-02.jpg |  twitter-chrome-02.jpg |  twitter-safari-02.jpg |  twitter-ie-02.jpg |
| | Evidence 3 | Time | 4/Oct/2011 – 4:32pm | 4/Oct/2011 – 4:38pm | 4/Oct/2011 – 4:43pm | 4/Oct/2011 – 4:49pm |
| | | Image |  twitter-firefox-03.jpg |  twitter-chrome-03.jpg |  twitter-safari-03.jpg |  twitter-ie-03.jpg |
| | Evidence 4 | Time | 4/Oct/2011 – 4:33pm | 4/Oct/2011 – 4:39pm | 4/Oct/2011 – 4:44pm | 4/Oct/2011 – 4:49pm |
| | | Image |  twitter-firefox-04.jpg |  twitter-chrome-04.jpg |  twitter-safari-04.jpg |  twitter-ie-04.jpg |
| | Evidence 5 | Time | 4/Oct/2011 – 4:34pm | 4/Oct/2011 – 4:40pm | 4/Oct/2011 – 4:45pm | 4/Oct/2011 – 4:50pm |
| | | Image |  twitter-firefox-05.jpg |  twitter-chrome-05.jpg |  twitter-safari-05.jpg |  twitter-ie-05.jpg |

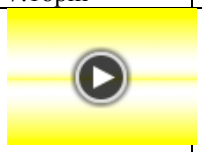
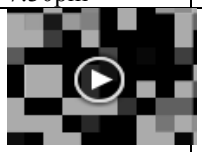
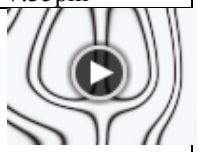
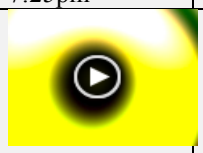
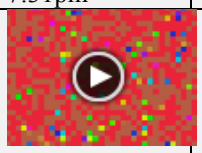
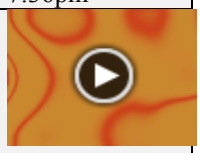
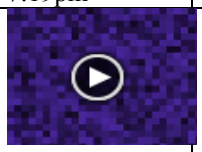
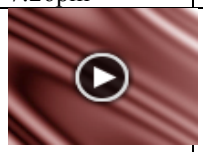
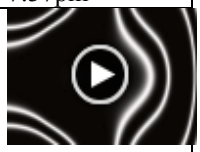
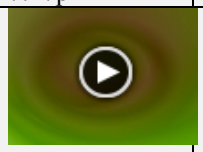
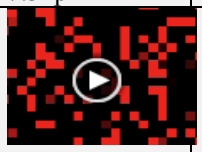
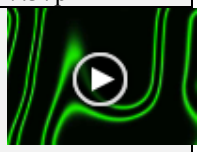
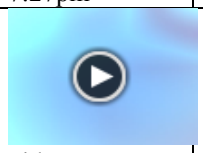
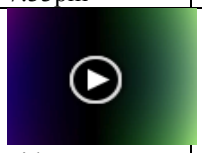
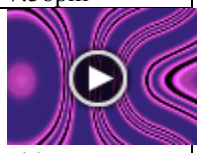
| | | | | | | |
|---|---|---|---|---|---|---|
| LinkedIn | Evidence 1 | Time | 4/Oct/2011 – 4:54pm | 4/Oct/2011 – 4:59pm | 4/Oct/2011 – 5:04pm | 4/Oct/2011 – 5:08pm |
| | | Image |  linkedin-firefox-01.jpg |  linkedin-chrome-01.jpg |  linkedin-safari-01.jpg |  linkedin-ie-01.jpg |
| | Evidence 2 | Time | 4/Oct/2011 – 4:55pm | 4/Oct/2011 – 5:00pm | 4/Oct/2011 – 5:04pm | 4/Oct/2011 – 5:09pm |
| | | Image |  linkedin-firefox-02.jpg |  linkedin-chrome-02.jpg |  linkedin-safari-02.jpg |  linkedin-ie-02.jpg |
| | Evidence 3 | Time | 4/Oct/2011 – 4:56pm | 4/Oct/2011 – 5:01pm | 4/Oct/2011 – 5:05pm | 4/Oct/2011 – 5:09pm |
| | | Image |  linkedin-firefox-03.jpg |  linkedin-chrome-03.jpg |  linkedin-safari-03.jpg |  linkedin-ie-03.jpg |
| | Evidence 4 | Time | 4/Oct/2011 – 4:57pm | 4/Oct/2011 – 5:01pm | 4/Oct/2011 – 5:06pm | 4/Oct/2011 – 5:10pm |
| | | Image |  linkedin-firefox-04.jpg |  linkedin-chrome-04.jpg |  linkedin-safari-04.jpg |  linkedin-ie-04.jpg |
| | Evidence 5 | Time | 4/Oct/2011 – 4:58pm | 4/Oct/2011 – 5:02pm | 4/Oct/2011 – 5:07pm | 4/Oct/2011 – 5:11pm |
| | | Image |  linkedin-firefox-05.jpg |  linkedin-chrome-05.jpg |  linkedin-safari-05.jpg |  linkedin-ie-05.jpg |

| | | | | | | |
|---|---|---|---|---|---|---|
| Google+ | Evidence 1 | Time | 4/Oct/2011 – 5:14pm | 4/Oct/2011 – 5:21pm | 4/Oct/2011 – 5:26pm | 4/Oct/2011 – 5:32pm |
| | | Image |  googleplus-firefox-01.jpg |  googleplus-chrome-01.jpg |  googleplus-safari-01.jpg |  googleplus-ie-01.jpg |
| | Evidence 2 | Time | 4/Oct/2011 – 5:15pm | 4/Oct/2011 – 5:21pm | 4/Oct/2011 – 5:27pm | 4/Oct/2011 – 5:33pm |
| | | Image |  googleplus-firefox-02.jpg |  googleplus-chrome-02.jpg |  googleplus-safari-02.jpg |  googleplus-ie-02.jpg |
| | Evidence 3 | Time | 4/Oct/2011 – 5:16pm | 4/Oct/2011 – 5:22pm | 4/Oct/2011 – 5:27pm | 4/Oct/2011 – 5:33pm |
| | | Image |  googleplus-firefox-03.jpg |  googleplus-chrome-03.jpg |  googleplus-safari-03.jpg |  googleplus-ie-03.jpg |
| | Evidence 4 | Time | 4/Oct/2011 – 5:16pm | 4/Oct/2011 – 5:23pm | 4/Oct/2011 – 5:27pm | 4/Oct/2011 – 5:33pm |
| | | Image |  googleplus-firefox-04.jpg |  googleplus-chrome-04.jpg |  googleplus-safari-04.jpg |  googleplus-ie-04.jpg |
| | Evidence 5 | Time | 4/Oct/2011 – 5:17pm | 4/Oct/2011 – 5:23pm | 4/Oct/2011 – 5:28pm | 4/Oct/2011 – 5:33pm |
| | | Image |  googleplus-firefox-05.jpg |  googleplus-chrome-05.jpg |  googleplus-safari-05.jpg |  googleplus-ie-05.jpg |

## Appendix B-6 Uploaded/Watched videos (Prepared)

Testing videos have been uploaded manually into each of 4 different SNSs. Videos have been uploaded from 4 different browsers with 5 different videos on each site.

| Service | Evidence | | Firefox 7.0.1 | Chrome 14.0 | Safari 5.1 | IE 9 |
|---|---|---|---|---|---|---|
| Facebook | Evidence 1 | Time | 4/Oct/2011 – 6:14pm | 4/Oct/2011 – 6:21pm | 4/Oct/2011 – 6:25pm | 4/Oct/2011 – 6:29pm |
| | | Video |  video-facebook-firefox-01.wmv |  video-facebook-chrome-01.wmv |  video-facebook-safari-01.wmv |  video-facebook-ie-01.wmv |
| | Evidence 2 | Time | 4/Oct/2011 – 6:15pm | 4/Oct/2011 – 6:22pm | 4/Oct/2011 – 6:25pm | 4/Oct/2011 – 6:30pm |
| | | Video |  video-facebook-firefox-02.wmv |  video-facebook-chrome-02.wmv |  video-facebook-safari-02.wmv |  video-facebook-ie-02.wmv |
| | Evidence 3 | Time | 4/Oct/2011 – 6:18pm | 4/Oct/2011 – 6:22pm | 4/Oct/2011 – 6:26pm | 4/Oct/2011 – 6:31pm |
| | | Video |  video-facebook-firefox-03.wmv |  video-facebook-chrome-03.wmv |  video-facebook-safari-03.wmv |  video-facebook-ie-03.wmv |
| | Evidence 4 | Time | 4/Oct/2011 – 6:19pm | 4/Oct/2011 – 6:22pm | 4/Oct/2011 – 6:26pm | 4/Oct/2011 – 6:31pm |
| | | Video |  video-facebook-firefox-04.wmv |  video-facebook-chrome-04.wmv |  video-facebook-safari-04.wmv |  video-facebook-ie-04.wmv |
| | Evidence 5 | Time | 4/Oct/2011 – 6:19pm | 4/Oct/2011 – 6:23pm | 4/Oct/2011 – 6:27pm | 4/Oct/2011 – 6:31pm |
| | | Video |  video-facebook-firefox-05.wmv |  video-facebook-chrome-05.wmv |  video-facebook-safari-05.wmv |  video-facebook-ie-05.wmv |

| | | | | | | |
|---|---|---|---|---|---|---|
| Twitter | * Video upload is not supported in Twitter | | | | | |
| LinkedIn | * Video upload is not supported in LinkedIn | | | | | |
| Google + | Evidence 1 | Time | 4/Oct/2011 – 7:18pm | 4/Oct/2011 – 7:24pm | 4/Oct/2011 – 7:30pm | 4/Oct/2011 – 7:35pm |
| | | Image |  video-googleplus-firefox-01.wmv |  video-googleplus-chrome-01.wmv |  video-googleplus-safari-01.wmv |  video-googleplus-ie-01.wmv |
| | Evidence 2 | Time | 4/Oct/2011 – 7:19pm | 4/Oct/2011 – 7:25pm | 4/Oct/2011 – 7:31pm | 4/Oct/2011 – 7:36pm |
| | | Image |  video-googleplus-firefox-02.wmv |  video-googleplus-chrome-02.wmv |  video-googleplus-safari-02.wmv |  video-googleplus-ie-02.wmv |
| | Evidence 3 | Time | 4/Oct/2011 – 7:19pm | 4/Oct/2011 – 7:26pm | 4/Oct/2011 – 7:31pm | 4/Oct/2011 – 7:37pm |
| | | Image |  video-googleplus-firefox-03.wmv |  video-googleplus-chrome-03.wmv |  video-googleplus-safari-03.wmv |  video-googleplus-ie-03.wmv |
| | Evidence 4 | Time | 4/Oct/2011 – 7:20pm | 4/Oct/2011 – 7:27pm | 4/Oct/2011 – 7:32pm | 4/Oct/2011 – 7:37pm |
| | | Image |  video-googleplus-firefox-04.wmv |  video-googleplus-chrome-04.wmv |  video-googleplus-safari-04.wmv |  video-googleplus-ie-04.wmv |
| | Evidence 5 | Time | 4/Oct/2011 – 7:20pm | 4/Oct/2011 – 7:27pm | 4/Oct/2011 – 7:33pm | 4/Oct/2011 – 7:38pm |
| | | Image |  video-googleplus-firefox-05.wmv |  video-googleplus-chrome-05.wmv |  video-googleplus-safari-05.wmv |  video-googleplus-ie-05.wmv |

## Appendix B-7 Prepared GPS location data

GPS information has been posted manually to prepare test data. Location information has been made from 4 different browsers with different locations for each service.

| Service | Evidence | | Firefox 7.0.1 | Chrome 14.0 | Safari 5.1 | IE 9 |
|---|---|---|---|---|---|---|
| Facebook | Evidence 1 | Time | 4/Oct/2011 – 3:49pm | 4/Oct/2011 – 4:03pm | 4/Oct/2011 – 4:09pm | 4/Oct/2011 – 4:17pm |
| | | Location | The Paddington | AUT Tower | Auckland, New Zealand | University of Auckland Library |
| | Evidence 2 | Time | 4/Oct/2011 – 3:54pm | 4/Oct/2011 – 4:03pm | 4/Oct/2011 – 4:10pm | 4/Oct/2011 – 4:19pm |
| | | Location | AUT Tower | University of Auckland Clock Tower | Sky Tower | AUT Tower |
| | Evidence 3 | Time | 4/Oct/2011 – 3:55pm | 4/Oct/2011 – 4:04pm | 4/Oct/2011 – 4:11pm | 4/Oct/2011 – 4:20pm |
| | | Location | Auckland CBD | Auckland CBD | Owen G. Glenn Building | The Paddington |
| | Evidence 4 | Time | 4/Oct/2011 – 3:56pm | 4/Oct/2011 – 4:05pm | 4/Oct/2011 – 4:12pm | 4/Oct/2011 – 4:22pm |
| | | Location | Eden Park | The Paddington | Viaduct Harbour | SKYCITY Auckland |
| | Evidence 5 | Time | 4/Oct/2011 – 3:57pm | 4/Oct/2011 – 4:06pm | 4/Oct/2011 – 4:14pm | 4/Oct/2011 – 4:23pm |
| | | Location | The Cloud | Auckland CBD | Eden Park | Les Mills – New Zealand |
| Twitter | * GPS information not supported by Twitter by web browser | | | | | |
| LinkedIn | * GPS information not supported by LinkedIn Website | | | | | |
| Google + | Evidence 1 | Time | 4/Oct/2011 – 5:14pm | 4/Oct/2011 – 5:21pm | 4/Oct/2011 – 5:26pm | 4/Oct/2011 – 5:32pm |
| | | Location | 57 Victoria St W, Auckland | 57 Victoria St W, Auckland | Not supported | 17-25 Boston Rd, Grafton |
| | Evidence 2 | Time | 4/Oct/2011 – 5:15pm | 4/Oct/2011 – 5:21pm | 4/Oct/2011 – 5:27pm | 4/Oct/2011 – 5:33pm |
| | | Location | 57 Victoria St W, Auckland | 57 Victoria St W, Auckland | Not supported | 17-25 Boston Rd, Grafton |
| | Evidence 3 | Time | 4/Oct/2011 – 5:16pm | 4/Oct/2011 – 5:22pm | 4/Oct/2011 – 5:27pm | 4/Oct/2011 – 5:33pm |
| | | Location | 57 Victoria St W, Auckland | 57 Victoria St W, Auckland | Not supported | 17-25 Boston Rd, Grafton |
| | Evidence 4 | Time | 4/Oct/2011 – 5:16pm | 4/Oct/2011 – 5:23pm | 4/Oct/2011 – 5:27pm | 4/Oct/2011 – 5:33pm |
| | | Location | 57 Victoria St W, Auckland | 57 Victoria St W, Auckland | Not supported | 17-25 Boston Rd, Grafton |
| | Evidence 5 | Time | 4/Oct/2011 – 5:17pm | 4/Oct/2011 – 5:23pm | 4/Oct/2011 – 5:28pm | 4/Oct/2011 – 5:33pm |
| | | Location | 57 Victoria St W, Auckland | 57 Victoria St W, Auckland | Not supported | 17-25 Boston Rd, Grafton |

## Appendix B-8 Prepared MS Outlook / Webmail (Gmail)

10 email messages has been received from each SNS. Email has been viewed and stored on both MS Outlook and Google Webmail.

| Service | Evidence | Date/Time | Message |
|---|---|---|---|
| Facebook | 1 | 4/Oct/2011 – 8:02pm | facebook email 1 |
| | 2 | 4/Oct/2011 – 8:02pm | facebook email 2 |
| | 3 | 4/Oct/2011 – 8:04pm | facebook email 3 |
| | 4 | 4/Oct/2011 – 8:04pm | facebook email 4 |
| | 5 | 4/Oct/2011 – 8:05pm | facebook email 5 |
| | 6 | 4/Oct/2011 – 8:05pm | facebook email 6 |
| | 7 | 4/Oct/2011 – 8:06pm | facebook email 7 |
| | 8 | 4/Oct/2011 – 8:06pm | facebook email 8 |
| | 9 | 4/Oct/2011 – 8:07pm | facebook email 9 |
| | 10 | 4/Oct/2011 – 8:07pm | facebook email 10 |
| Twitter | 1 | 4/Oct/2011 – 8:10pm | twitter email 1 - evidence email message from twitter |
| | 2 | 4/Oct/2011 – 8:10pm | twitter email 2 - evidence email message from twitter |
| | 3 | 4/Oct/2011 – 8:11pm | twitter email 3 - evidence email message from twitter |
| | 4 | 4/Oct/2011 – 8:11pm | twitter email 4 - evidence email message from twitter |
| | 5 | 4/Oct/2011 – 8:11pm | twitter email 5 - evidence email message from twitter |
| | 6 | 4/Oct/2011 – 8:11pm | twitter email 6 - evidence email message from twitter |
| | 7 | 4/Oct/2011 – 8:11pm | twitter email 7 - evidence email message from twitter |
| | 8 | 4/Oct/2011 – 8:11pm | twitter email 8 - evidence email message from twitter |
| | 9 | 4/Oct/2011 – 8:11pm | twitter email 9 - evidence email message from twitter |
| | 10 | 4/Oct/2011 – 8:11pm | twitter email 10 - evidence email message from twitter |
| LinkedIn | 1 | 4/Oct/2011 – 8:15pm | LinkedIn Email 01 - evidence email message from Linked In - Maori Party co-leader Dr Pita Sharples view that Maori are unfairly treated by police is supported by local research, according to Rethinking Crime and Punishment. |
| | 2 | 4/Oct/2011 – 8:15pm | LinkedIn Email 02 - evidence email message from Linked In - The man dubbed the "accidental millionaire" after he allegedly skipped the country when Westpac mistakenly loaded $10 million into his account |
| | 3 | 4/Oct/2011 – 8:16pm | LinkedIn Email 03 - evidence email message from Linked In - No Dan and no Richie for today's game |
| | 4 | 4/Oct/2011 – 8:16pm | LinkedIn Email 04 - evidence email message from Linked In - A pair of children on the Ferris wheel and two people in the plane were trapped |
| | 5 | 4/Oct/2011 – 8:17pm | LinkedIn Email 05 - evidence email message from Linked In - A man in south China's Hainan province braves strong winds and rain from typhoon Nesat. |
| | 6 | 4/Oct/2011 – 8:17pm | LinkedIn Email 06 - evidence email message from Linked In - A senior aide to Palestinian Authority President Mahmoud Abbas demanded |
| | 7 | 4/Oct/2011 – 8:18pm | LinkedIn Email 07 - evidence email message from Linked In - Prime Minister John Key says the Government is not embarrassed by the downgrading of New Zealand's credit rating. |
| | 8 | 4/Oct/2011 – 8:18pm | LinkedIn Email 08 - evidence email message from Linked In - The collapse of two cathedrals in Christchurch, including the Catholic Basilica, has put pressure on insurers. |

| | | | |
|---|---|---|---|
| | 9 | 4/Oct/2011 – 8:21pm | LinkedIn Email 09 - evidence email message from Linked In - Waikato Telecom shareholders wanted assurances from visiting chief executive Paul Reynolds |
| | 10 | 4/Oct/2011 – 8:22pm | LinkedIn Email 10 - evidence email message from Linked In - A medical device used to monitor the King of Pop has been called "inadequate" by a medical expert testifying in the trial against the singer's doctor. |
| Google + | 1 | 4/Oct/2011 – 8:26pm | Google plus email 1 |
| | 2 | 4/Oct/2011 – 8:27pm | Google plus email 2 |
| | 3 | 4/Oct/2011 – 8:27pm | Google plus email 3 |
| | 4 | 4/Oct/2011 – 8:27pm | Google plus email 4 |
| | 5 | 4/Oct/2011 – 8:27pm | Google plus email 5 |
| | 6 | 4/Oct/2011 – 8:28pm | Google plus email 6 |
| | 7 | 4/Oct/2011 – 8:30pm | Google plus email 7 |
| | 8 | 4/Oct/2011 – 8:30pm | Google plus email 8 |
| | 9 | 4/Oct/2011 – 8:30pm | Google plus email 9 |
| | 10 | 4/Oct/2011 – 8:31pm | Google plus email 10 |

# Appendix C - Testing Procedure & Results

## Appendix C-1 Cacheback – Browser Cache/History/Cookie extraction

```
######################
##  Cache Records   ##
######################

Facebook Cache only (Firefox)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%facebook%') AND ([URLs].CacheType LIKE '%firefox%') (41 records)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%fbcdn%') AND ([URLs].CacheType LIKE '%firefox%')  (293 records)
Total: 334 records

Facebook Cache only (Chrome)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%facebook%') AND ([URLs].CacheType LIKE '%chrome%') (0 record)

Facebook Cache only (safari)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%facebook%') AND ([URLs].CacheType LIKE '%safari%') (0 record)

Facebook Cache only (IE)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%facebook%') AND ([URLs].CacheType LIKE '%IE%') (24 record)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%fbcdn%') AND ([URLs].CacheType LIKE '%IE%') (160 record)
Total: 184 records
```

---

```
Twitter Cache only (Firefox)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%twitter%') AND ([URLs].CacheType LIKE '%firefox%') (14 records)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%http://t.co%') AND ([URLs].CacheType LIKE '%firefox%') (7 records)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%p.twimg%') AND ([URLs].CacheType LIKE '%firefox%') (13 records)

Twitter Cache only (Chrome)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%twitter%') AND ([URLs].CacheType LIKE '%chrome%') (0 record)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%http://t.co%') AND ([URLs].CacheType LIKE '%chrome%') (0 record)

Twitter Cache only (Safari)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%twitter%') AND ([URLs].CacheType LIKE '%safari%') (0 record)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%http://t.co%') AND ([URLs].CacheType LIKE '%safari%') (0 record)

Twitter Cache only (IE)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%twitter%') AND ([URLs].CacheType LIKE '%IE%') (9 records)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%http://t.co%') AND ([URLs].CacheType LIKE '%IE%') (4 records)
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%p.twimg%') AND ([URLs].CacheType LIKE '%ie%') (4 records)
Total: 17 records
```

LinkedIn Cache only (Firefox)
```
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%linkedin%') AND ([URLs].CacheType LIKE '%firefox%') (263 records)
```

LinkedIn Cache only (Chrome)
```
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%linkedin%') AND ([URLs].CacheType LIKE '%chrome%') (0 record)
```

LinkedIn Cache only (Safari)
```
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%linkedin%') AND ([URLs].CacheType LIKE '%safari%') (0 record)
```

LinkedIn Cache only (IE)
```
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%linkedin%') AND ([URLs].CacheType LIKE '%IE%') (26 records)
```

---

Google Plus Cache only (Firefox)
```
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%plus.google%') AND ([URLs].CacheType LIKE '%firefox%') (70 records)
```

Google Plus Cache only (Chrome)
```
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%plus.google%') AND ([URLs].CacheType LIKE '%chrome%') (0 records)
```

Google Plus Cache only (Safari)
```
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%plus.google%') AND ([URLs].CacheType LIKE '%safari%') (0 records)
```

Google Plus Cache only (IE)
```
SELECT * FROM [URLs] WHERE ([URLs].IsCache = True) AND ([URLs].URL LIKE
'%plus.google%') AND ([URLs].CacheType LIKE '%IE%') (12 records)
```

```
######################
## History Records  ##
######################
Facebook History (Firefox)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%facebook%') AND ([URLs].CacheType LIKE '%firefox%') (11 records)

Facebook History (Chrome)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%facebook%') AND ([URLs].CacheType LIKE '%chrome%') (12 records)

Facebook History (Safari)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%facebook%') AND ([URLs].CacheType LIKE '%safari%') (8 records)

Facebook History (IE)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%facebook%') AND ([URLs].CacheType LIKE '%IE%') (0 records)
```

---

```
Twitter History (Firefox)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%twitter%') AND ([URLs].CacheType LIKE '%firefox%') (23 records)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%http://t.co%') AND ([URLs].CacheType LIKE '%firefox%') (6 records)

Twitter History (Chrome)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%twitter%') AND ([URLs].CacheType LIKE '%chrome%') (21 records)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%http://t.co%') AND ([URLs].CacheType LIKE '%chrome%') (5 records)

Twitter History (Safari)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%twitter%') AND ([URLs].CacheType LIKE '%safari%') (7 records)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%http://t.co%') AND ([URLs].CacheType LIKE '%safari%') (5 records)

Twitter History (IE)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%twitter%') AND ([URLs].CacheType LIKE '%IE%') (0 records)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%http://t.co%') AND ([URLs].CacheType LIKE '%IE%') (0 records)
```

---

```
LinkedIn History (Firefox)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%linkedin%') AND ([URLs].CacheType LIKE '%firefox%') (17 records)

LinkedIn History (Chrome)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%linkedin%') AND ([URLs].CacheType LIKE '%chrome%') (13 records)

LinkedIn History (Safari)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%linkedin%') AND ([URLs].CacheType LIKE '%safari%') (11 records)

LinkedIn History (IE)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%linkedin%') AND ([URLs].CacheType LIKE '%IE%') (0 records)
```

```
Google Plus History (Firefox)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%plus.google%') AND ([URLs].CacheType LIKE '%firefox%') (10 records)

Google Plus History (Chrome)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%plus.google%') AND ([URLs].CacheType LIKE '%chrome%') (8 records)

Google Plus History (Safari)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%plus.google%') AND ([URLs].CacheType LIKE '%safari%') (2 records)

Google Plus History (IE)
SELECT * FROM URLs WHERE IsHistory = True AND IsCache = False AND ([URLs].URL
LIKE '%plus.google%') AND ([URLs].CacheType LIKE '%IE%') (0 records)
```

**######################**
**##  Cookie Records  ##**
**######################**

Facebook Cookies (Firefox)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%facebook%') AND ([URLs].CacheType LIKE '%firefox%') (7 records)

Facebook Cookies (Chrome)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%facebook%') AND ([URLs].CacheType LIKE '%chrome%') (6 records)

Facebook Cookies (Safari)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%facebook%') AND ([URLs].CacheType LIKE '%safari%') (0 records)

Facebook Cookies (IE)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%facebook%') AND ([URLs].CacheType LIKE '%IE%') (1 record)

---

Twitter Cookies (Firefox)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%twitter%') AND ([URLs].CacheType LIKE '%firefox%') (10 records)

Twitter Cookies (Chrome)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%twitter%') AND ([URLs].CacheType LIKE '%chrome%') (9 records)

Twitter Cookies (Safari)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%twitter%') AND ([URLs].CacheType LIKE '%safari%') (0 record)

Twitter Cookies (IE)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%twitter%') AND ([URLs].CacheType LIKE '%IE%') (1 record)

---

LinkedIn Cookies (Firefox)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%linkedin%') AND ([URLs].CacheType LIKE '%firefox%') (17 records)

LinkedIn Cookies (Chrome)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%linkedin%') AND ([URLs].CacheType LIKE '%chrome%') (12 records)

LinkedIn Cookies (Safari)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%linkedin%') AND ([URLs].CacheType LIKE '%safari%') (0 record)

LinkedIn Cookies (IE)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%linkedin%') AND ([URLs].CacheType LIKE '%ie%') (3 records)

---

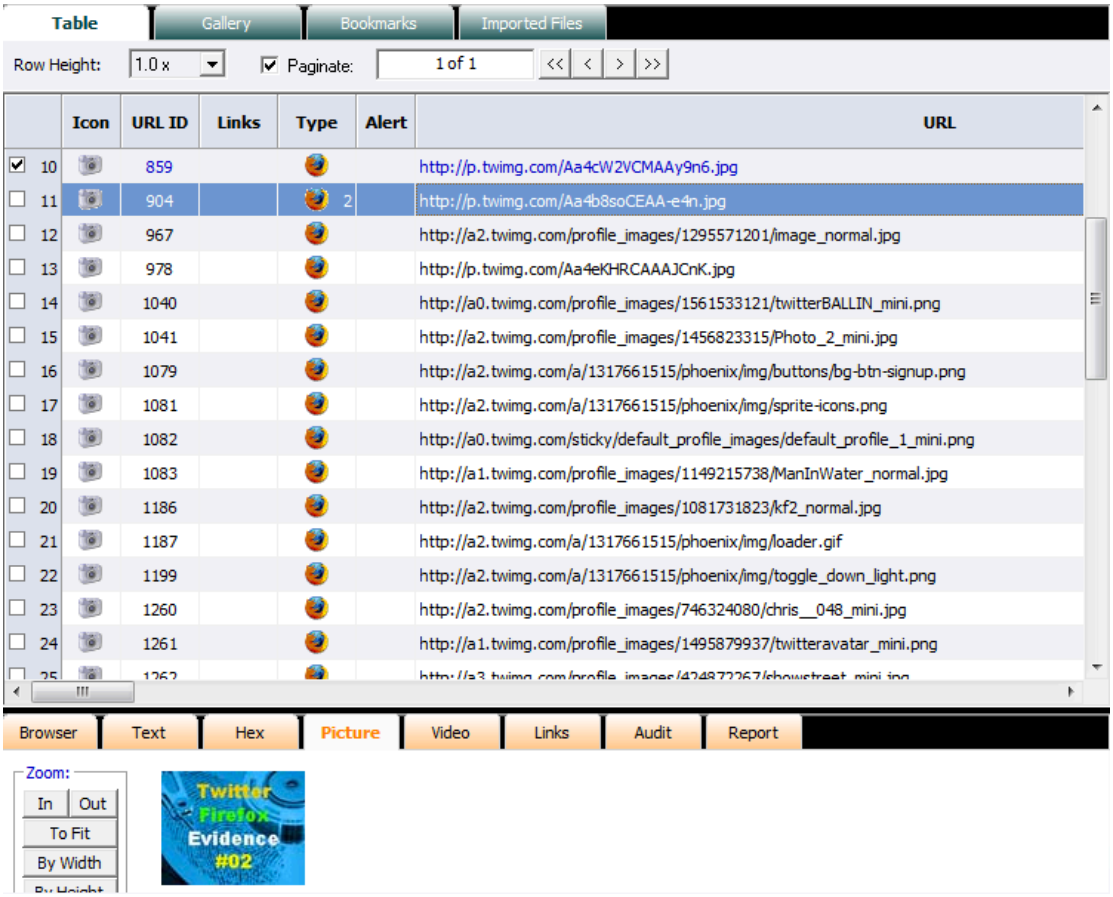
Google Plus Cookies (Firefox)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%plus.google%') AND ([URLs].CacheType LIKE '%Firefox%') (5 records)

Google Plus Cookies (Chrome)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE '%plus.google%') AND ([URLs].CacheType LIKE '%chrome%') (4 records)

Google Plus Cookies (Safari)

```
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE
'%plus.google%') AND ([URLs].CacheType LIKE '%safari%') (0 record)

Google Plus Cookies (IE)
SELECT * FROM [URLs] WHERE ([URLs].IsCookie = True) AND ([URLs].URL LIKE
'%plus.google%') AND ([URLs].CacheType LIKE '%IE%') (1 record)
```

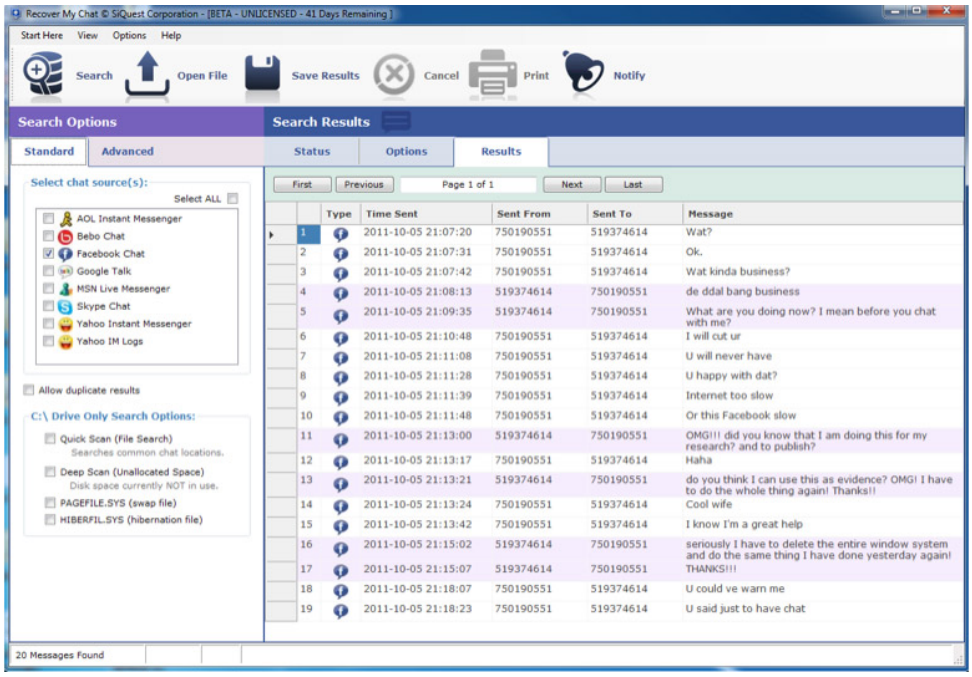
# Appendix C-2 Cacheback - Pictures / Video extraction




```
###################
# Firefox testing #
###################
Facebook (Firefox) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE
'%fbcdn.net/hphotos%') AND ([URLs].CacheType LIKE '%firefox%') AND LCase(CacheFileExt)
<> 'ico' AND CacheFileExists = True ORDER BY URL_ID;

Twitter (Firefox) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE '%twimg%')
AND ([URLs].CacheType LIKE '%firefox%') AND LCase(CacheFileExt) <> 'ico' AND
CacheFileExists = True ORDER BY URL_ID;

LinkedIn (Firefox) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE
'%media.linkedin.com/media-proxy%') AND ([URLs].CacheType LIKE '%firefox%') AND
LCase(CacheFileExt) <> 'ico' AND CacheFileExists = True ORDER BY URL_ID;

Google Plus (Firefox) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE '%googleplus-
firefox%') AND ([URLs].CacheType LIKE '%firefox%') AND LCase(CacheFileExt) <> 'ico'
AND CacheFileExists = True ORDER BY URL_ID;

###################
# Chrome testing  #
###################
Facebook (Chrome) Photos
```

```
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE
'%fbcdn.net/hphotos%') AND ([URLs].CacheType LIKE '%chrome%') AND LCase(CacheFileExt)
<> 'ico' AND CacheFileExists = True ORDER BY URL_ID;

Twitter (Chrome) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE '%twimg%')
AND ([URLs].CacheType LIKE '%chrome%') AND LCase(CacheFileExt) <> 'ico' AND
CacheFileExists = True ORDER BY URL_ID;

LinkedIn (Chrome) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE
'%media.linkedin.com/media-proxy%') AND ([URLs].CacheType LIKE '%chrome%') AND
LCase(CacheFileExt) <> 'ico' AND CacheFileExists = True ORDER BY URL_ID;

Google Plus (Chrome) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE '%plus%') AND
([URLs].CacheType LIKE '%chrome%') AND LCase(CacheFileExt) <> 'ico' AND
CacheFileExists = True ORDER BY URL_ID;

####################
# Safari testing  #
####################
Facebook (safari) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE
'%fbcdn.net/hphotos%') AND ([URLs].CacheType LIKE '%safari%') AND LCase(CacheFileExt)
<> 'ico' AND CacheFileExists = True ORDER BY URL_ID;

Twitter (safari) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE '%twimg%')
AND ([URLs].CacheType LIKE '%safari%') AND LCase(CacheFileExt) <> 'ico' AND
CacheFileExists = True ORDER BY URL_ID;

LinkedIn (safari) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE
'%media.linkedin.com/media-proxy%') AND ([URLs].CacheType LIKE '%safari%') AND
LCase(CacheFileExt) <> 'ico' AND CacheFileExists = True ORDER BY URL_ID;

Google Plus (safari) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE '%plus%') AND
([URLs].CacheType LIKE '%safari%') AND LCase(CacheFileExt) <> 'ico' AND
CacheFileExists = True ORDER BY URL_ID;

###############
# IE testing #
###############
Facebook (IE) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE
'%fbcdn.net/hphotos%') AND ([URLs].CacheType LIKE '%IE Cache%') AND
LCase(CacheFileExt) <> 'ico' AND CacheFileExists = True ORDER BY URL_ID;

Twitter (IE) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE '%twimg%')
AND ([URLs].CacheType LIKE '%IE Cache%') AND LCase(CacheFileExt) <> 'ico' AND
CacheFileExists = True ORDER BY URL_ID;

LinkedIn (IE) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE
'%media.linkedin.com/media-proxy%') AND ([URLs].CacheType LIKE '%IE Cache%') AND
LCase(CacheFileExt) <> 'ico' AND CacheFileExists = True ORDER BY URL_ID;

Google Plus (IE) Photos
SELECT * FROM [URLs] WHERE ([URLs].IsPicture = True) AND ([URLs].URL LIKE '%plus%') AND
([URLs].CacheType LIKE '%IE Cache%') AND LCase(CacheFileExt) <> 'ico' AND
CacheFileExists = True ORDER BY URL_ID;


####################
# Video components #
####################
SELECT * FROM URLs WHERE IsMovie = True AND CacheFileExists = True ORDER BY URL_ID;
```

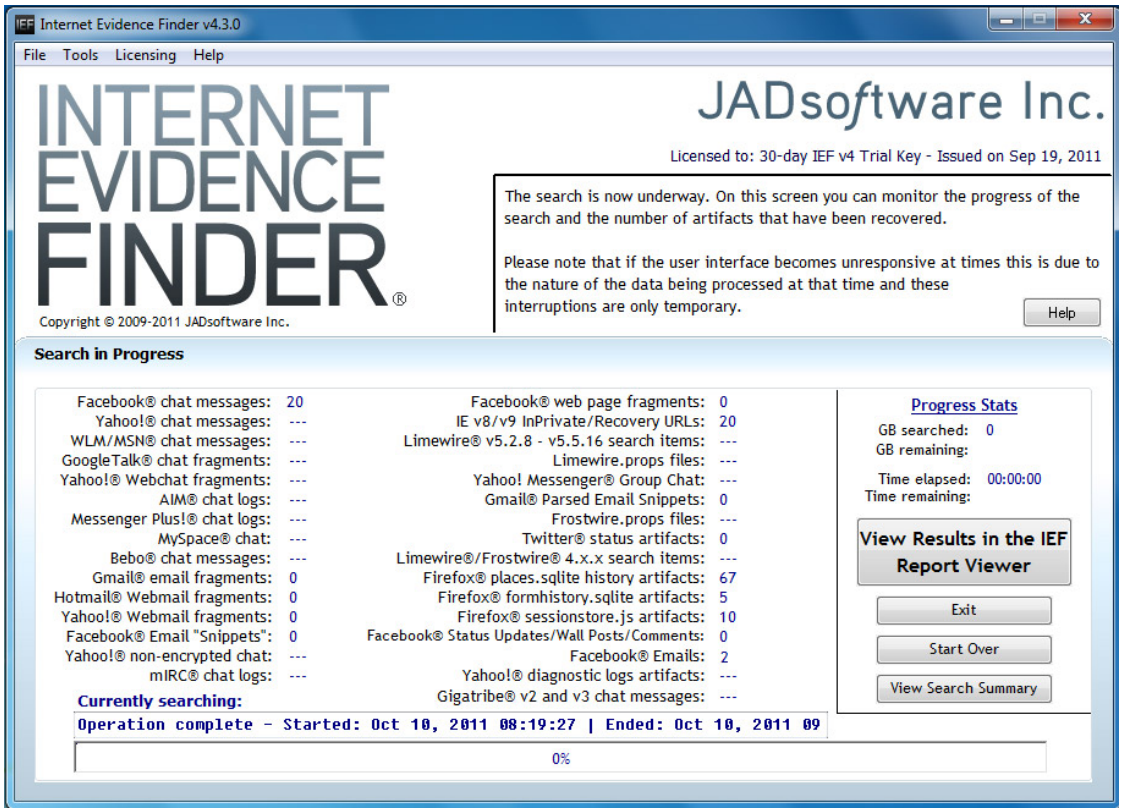
## Appendix C-3 CacheBack – Facebook Chatting extraction

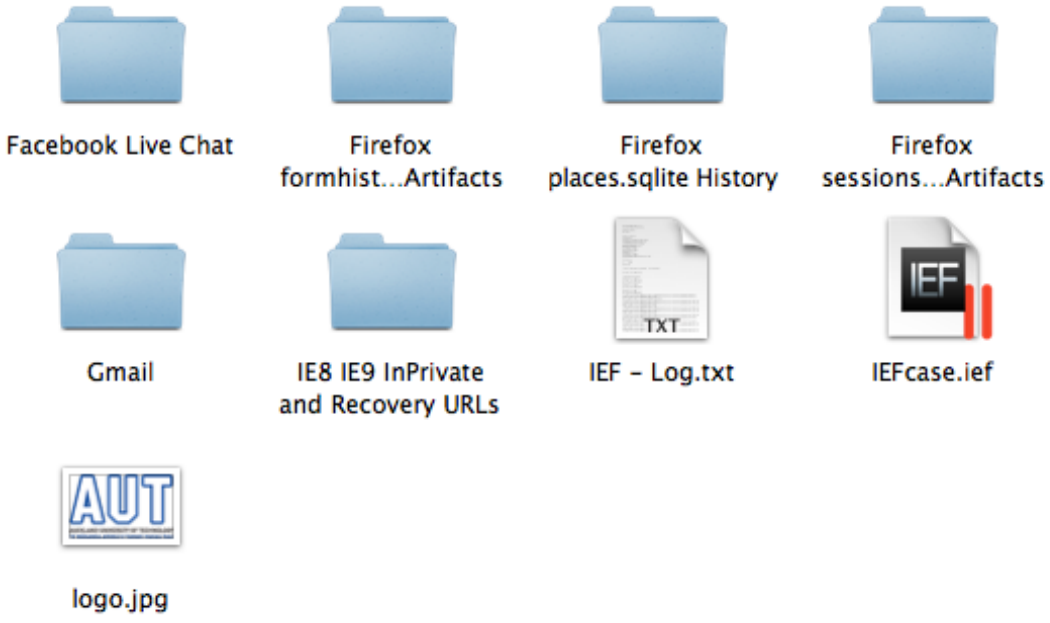



First Previous Page 1 of 1 Next Last

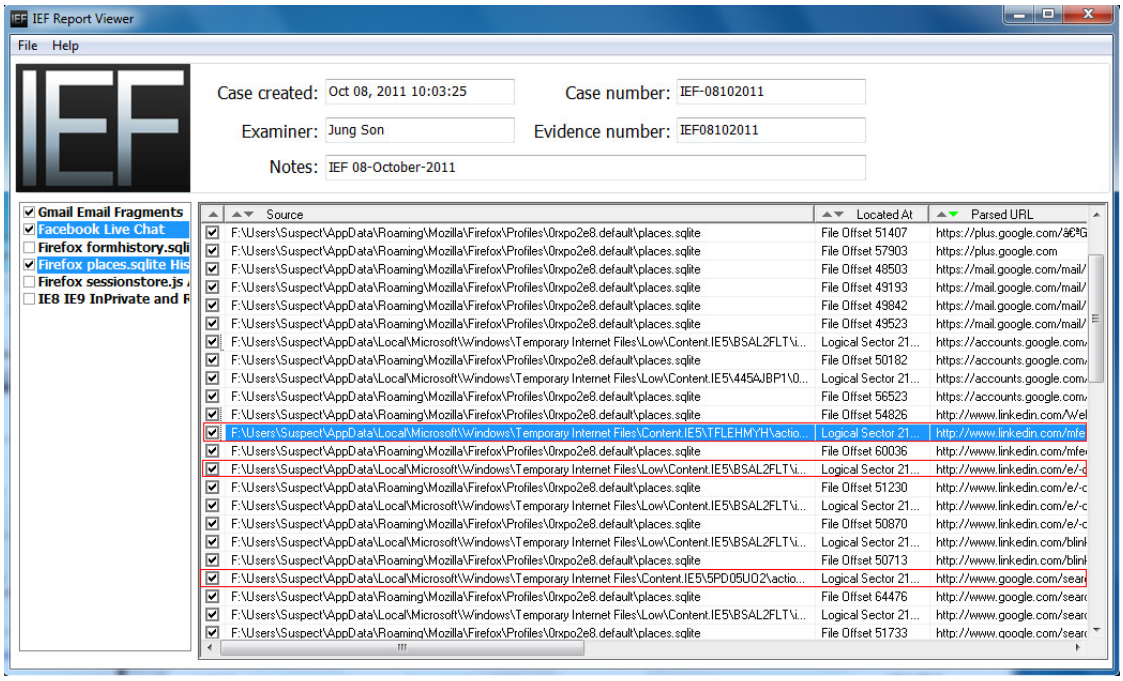
| | Type | Time Sent | Sent From | Sent To | Message |
|---|---|---|---|---|---|
| 1 | | 2011-10-05 21:07:20 | 750190551 | 519374614 | Wat? |
| 2 | | 2011-10-05 21:07:31 | 750190551 | 519374614 | Ok. |
| 3 | | 2011-10-05 21:07:42 | 750190551 | 519374614 | Wat kinda business? |
| 4 | | 2011-10-05 21:08:13 | 519374614 | 750190551 | de ddal bang business |
| 5 | | 2011-10-05 21:09:35 | 519374614 | 750190551 | What are you doing now? I mean before you chat with me? |
| 6 | | 2011-10-05 21:10:48 | 750190551 | 519374614 | I will cut ur |
| 7 | | 2011-10-05 21:11:08 | 750190551 | 519374614 | U will never have |
| 8 | | 2011-10-05 21:11:28 | 750190551 | 519374614 | U happy with dat? |
| 9 | | 2011-10-05 21:11:39 | 750190551 | 519374614 | Internet too slow |
| 10 | | 2011-10-05 21:11:48 | 750190551 | 519374614 | Or this Facebook slow |
| 11 | | 2011-10-05 21:13:00 | 519374614 | 750190551 | OMG!!! did you know that I am doing this for my research? and to publish? |
| 12 | | 2011-10-05 21:13:17 | 750190551 | 519374614 | Haha |
| 13 | | 2011-10-05 21:13:21 | 519374614 | 750190551 | do you think I can use this as evidence? OMG! I have to do the whole thing again! Thanks!! |
| 14 | | 2011-10-05 21:13:24 | 750190551 | 519374614 | Cool wife |
| 15 | | 2011-10-05 21:13:42 | 750190551 | 519374614 | I know I'm a great help |
| 16 | | 2011-10-05 21:15:02 | 519374614 | 750190551 | seriously I have to delete the entire window system and do the same thing I have done yesterday again! |
| 17 | | 2011-10-05 21:15:07 | 519374614 | 750190551 | THANKS!!! |
| 18 | | 2011-10-05 21:18:07 | 750190551 | 519374614 | U could ve warn me |
| 19 | | 2011-10-05 21:18:23 | 750190551 | 519374614 | U said just to have chat |

## Appendix C-4 Internet Evidence Finder Search Results

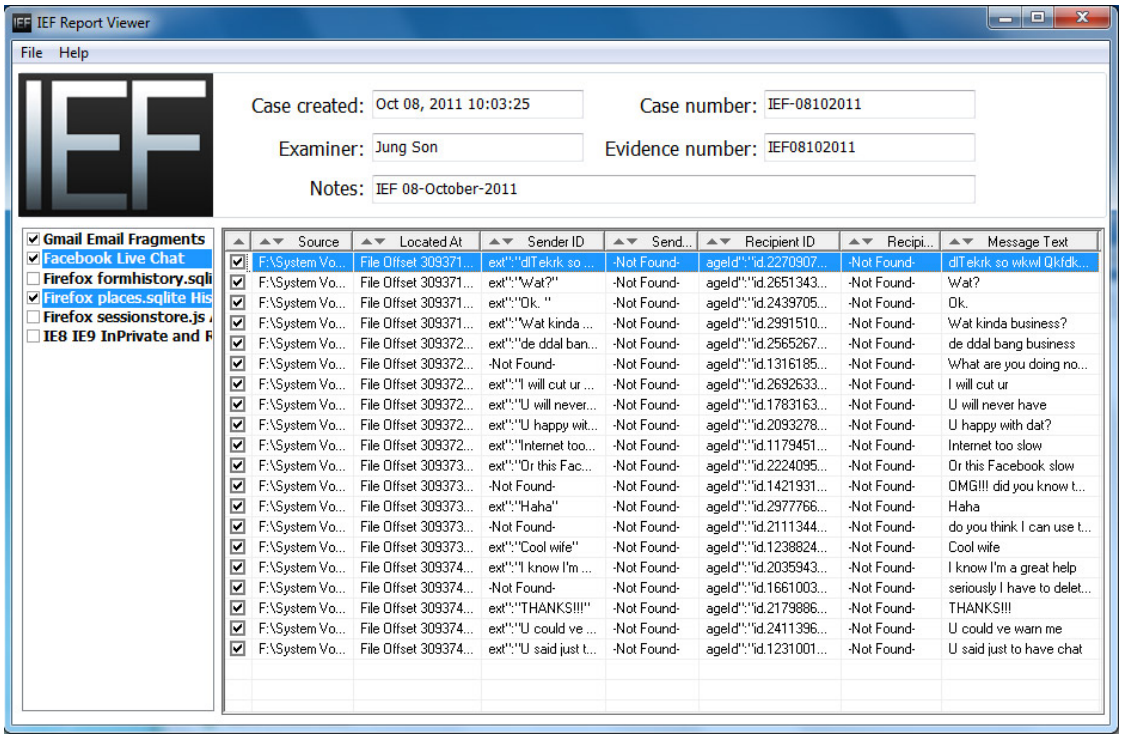


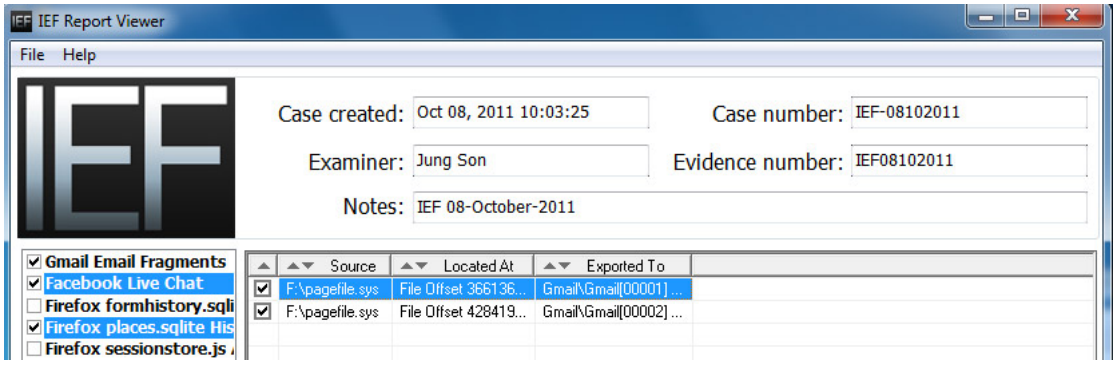
## Appendix C-5 Internet Evidence Finder – Cache Items found




## Appendix C-6 Internet Evidence Finder – Facebook Chatting records



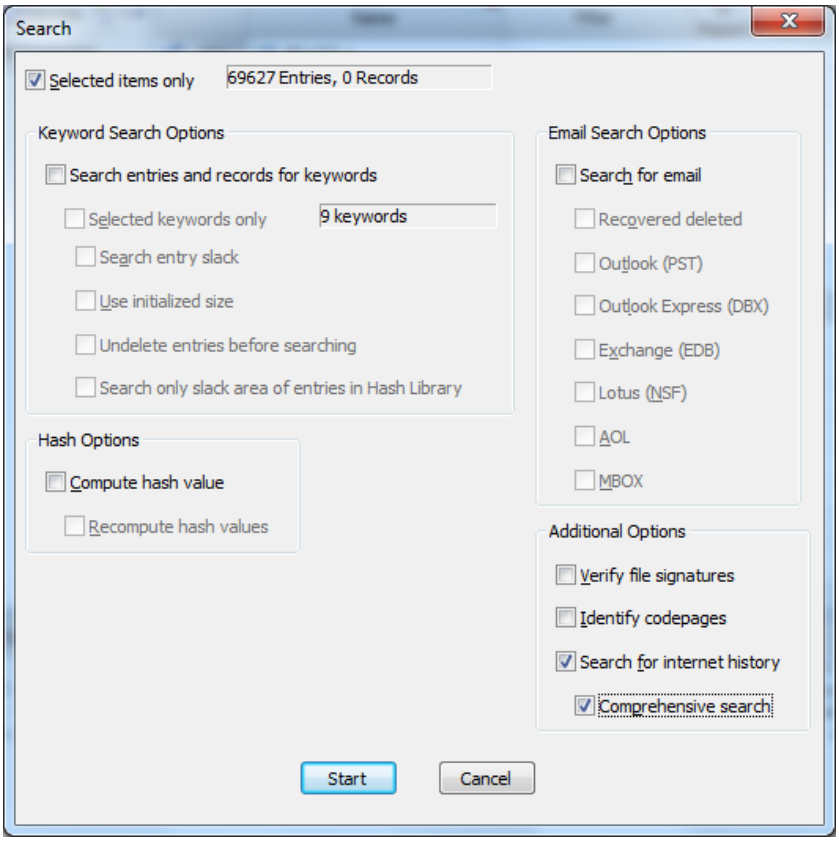
## Appendix C-7 Internet Evidence Finder – Webmail records



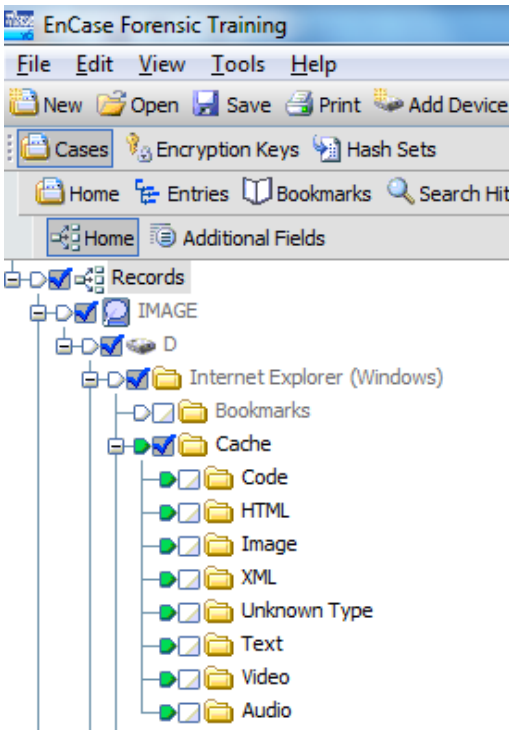

## Appendix C-8 Google Plus email found from Internet Evidence Finder

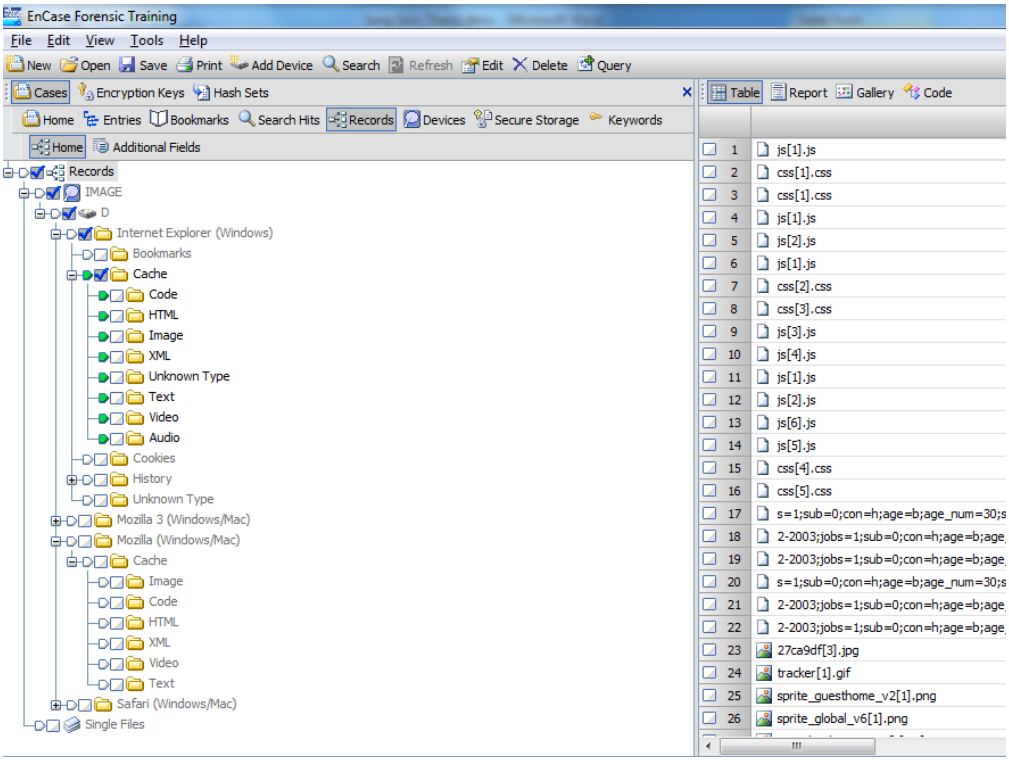

```
,"<span dir="ltr"><span class="yP" email="member@linkedin.com">Hi Sung Ko via
LinkedIn</span></span>","&raquo; ","LinkedIn Email 10 - evidence email message from
Linked In","",0,"","","Oct 4","Tue, Oct 4, 2011 at 8:21 PM",1317713795965724,,[[["em"]
```

## Appendix C-9 EnCase - Internet Browser Cache/History/Cookie extraction



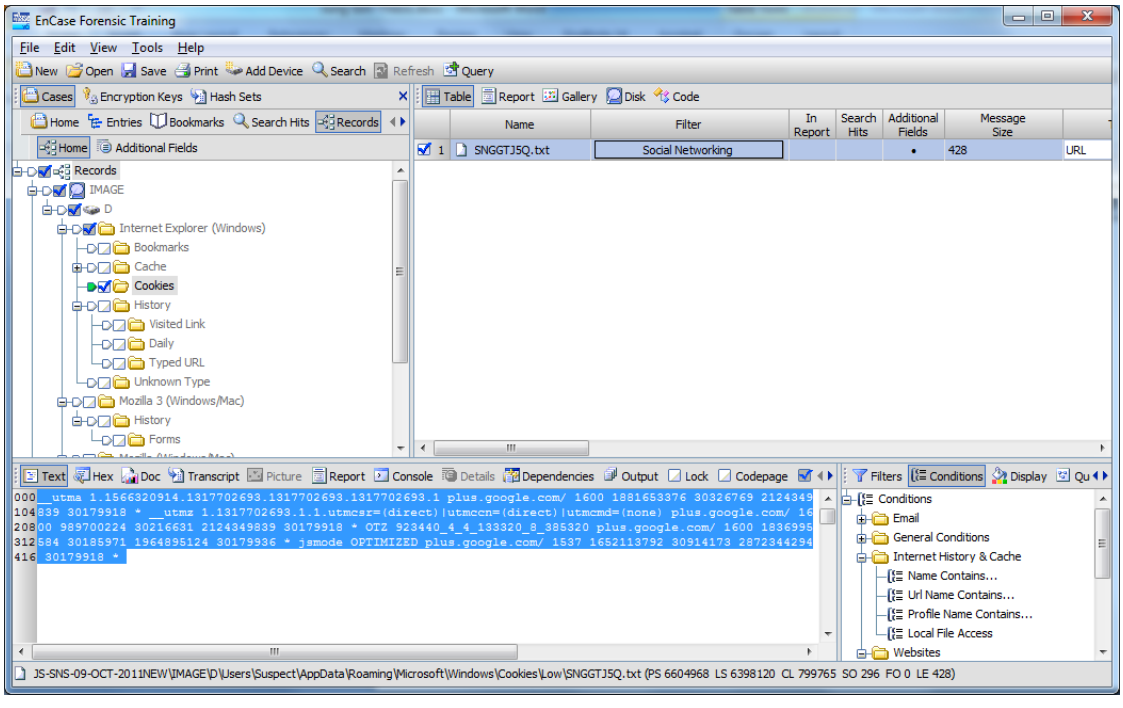

**Encase Internet cache search**



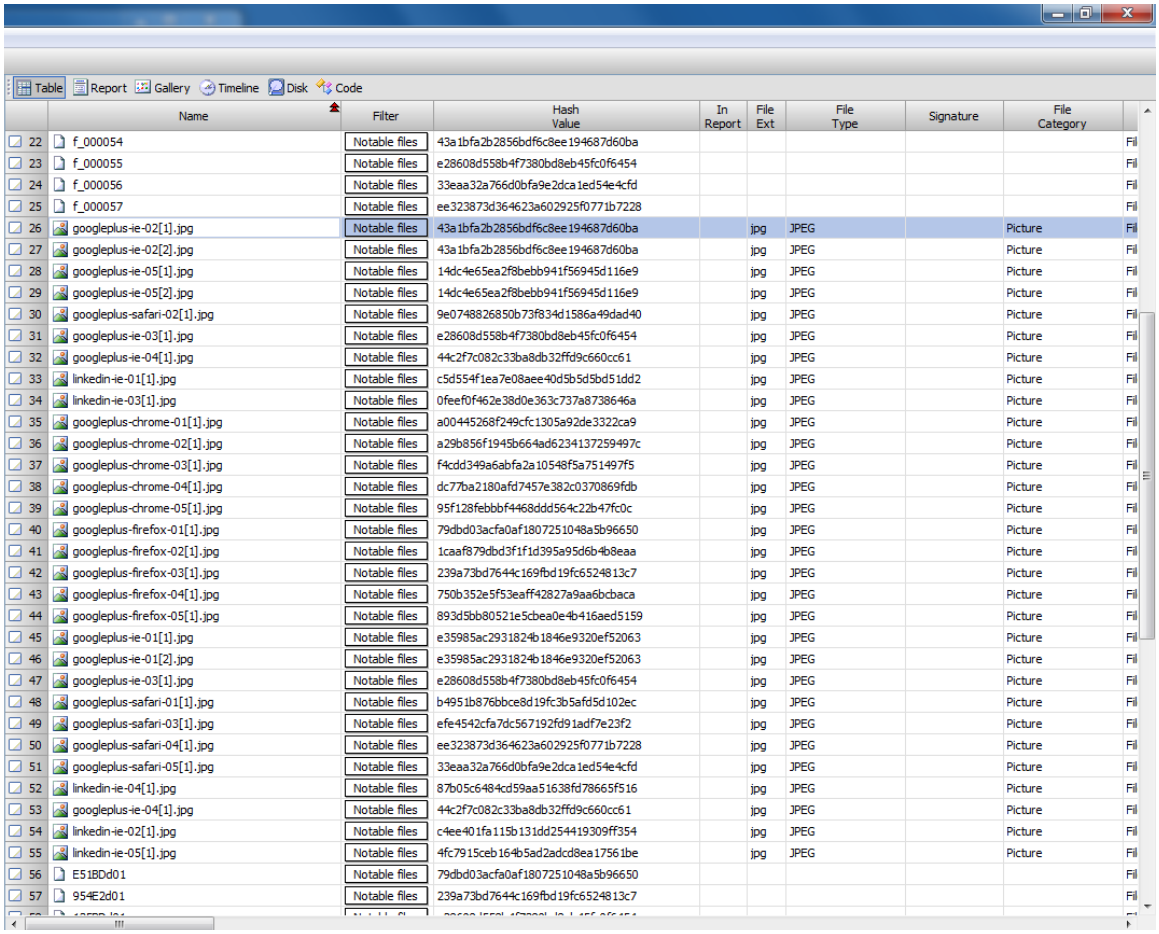



Number of Cache items found from EnCase

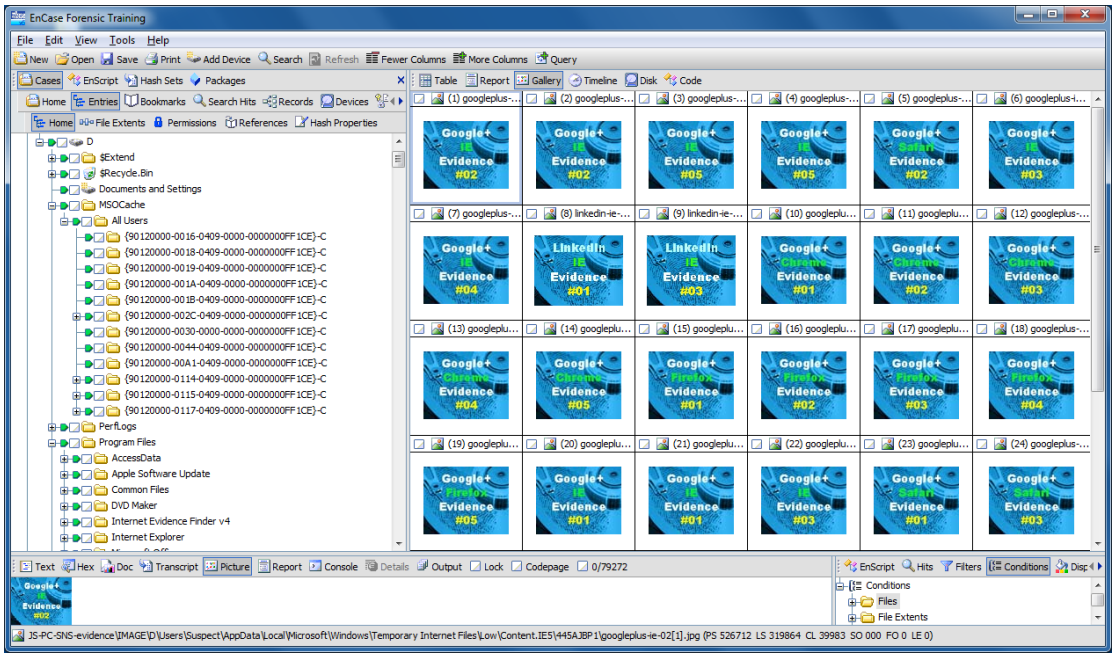
## IE cookie – Google plus



# Appendix C-10 Encase - Photo extraction (Notable only)



| | Name | Filter | Hash Value | In Report | File Ext | File Type | Signature | File Category | |
|---|---|---|---|---|---|---|---|---|---|
| 22 | f_000054 | Notable files | 43a1bfa2b2856bdf6c8ee194687d60ba | | | | | | Fil |
| 23 | f_000055 | Notable files | e28608d558b4f7380bd8eb45fc0f6454 | | | | | | Fil |
| 24 | f_000056 | Notable files | 33eaa32a766d0bfa9e2dca1ed54e4cfd | | | | | | Fil |
| 25 | f_000057 | Notable files | ee323873d364623a602925f0771b7228 | | | | | | Fil |
| 26 | googleplus-ie-02[1].jpg | Notable files | 43a1bfa2b2856bdf6c8ee194687d60ba | | jpg | JPEG | | Picture | Fil |
| 27 | googleplus-ie-02[2].jpg | Notable files | 43a1bfa2b2856bdf6c8ee194687d60ba | | jpg | JPEG | | Picture | Fil |
| 28 | googleplus-ie-05[1].jpg | Notable files | 14dc4e65ea2f8bebb941f56945d116e9 | | jpg | JPEG | | Picture | Fil |
| 29 | googleplus-ie-05[2].jpg | Notable files | 14dc4e65ea2f8bebb941f56945d116e9 | | jpg | JPEG | | Picture | Fil |
| 30 | googleplus-safari-02[1].jpg | Notable files | 9e0748826850b73f834d1586a49dad40 | | jpg | JPEG | | Picture | Fil |
| 31 | googleplus-ie-03[1].jpg | Notable files | e28608d558b4f7380bd8eb45fc0f6454 | | jpg | JPEG | | Picture | Fil |
| 32 | googleplus-ie-04[1].jpg | Notable files | 44c2f7c082c33ba8db32ffd9c660cc61 | | jpg | JPEG | | Picture | Fil |
| 33 | linkedin-ie-01[1].jpg | Notable files | c5d554f1ea7e08aee40d5b5d5bd51dd2 | | jpg | JPEG | | Picture | Fil |
| 34 | linkedin-ie-03[1].jpg | Notable files | 0feef0f462e38d0e363c737a8738646a | | jpg | JPEG | | Picture | Fil |
| 35 | googleplus-chrome-01[1].jpg | Notable files | a00445268f249cfc1305a92de3322ca9 | | jpg | JPEG | | Picture | Fil |
| 36 | googleplus-chrome-02[1].jpg | Notable files | a29b856f1945b664ad6234137259497c | | jpg | JPEG | | Picture | Fil |
| 37 | googleplus-chrome-03[1].jpg | Notable files | f4cdd349a6abfa2a10548f5a751497f5 | | jpg | JPEG | | Picture | Fil |
| 38 | googleplus-chrome-04[1].jpg | Notable files | dc77ba2180afd7457e382c0370869fdb | | jpg | JPEG | | Picture | Fil |
| 39 | googleplus-chrome-05[1].jpg | Notable files | 95f128febbbf4468ddd564c22b47fc0c | | jpg | JPEG | | Picture | Fil |
| 40 | googleplus-firefox-01[1].jpg | Notable files | 79dbd03acfa0af1807251048a5b96650 | | jpg | JPEG | | Picture | Fil |
| 41 | googleplus-firefox-02[1].jpg | Notable files | 1caaf879dbd3f1f1d395a95d6b4b8eaa | | jpg | JPEG | | Picture | Fil |
| 42 | googleplus-firefox-03[1].jpg | Notable files | 239a73bd7644c169fbd19fc6524813c7 | | jpg | JPEG | | Picture | Fil |
| 43 | googleplus-firefox-04[1].jpg | Notable files | 750b352e5f53eaff42827a9aa6bcbaca | | jpg | JPEG | | Picture | Fil |
| 44 | googleplus-firefox-05[1].jpg | Notable files | 893d5bb80521e5cbea0e4b416aed5159 | | jpg | JPEG | | Picture | Fil |
| 45 | googleplus-ie-01[1].jpg | Notable files | e35985ac2931824b1846e9320ef52063 | | jpg | JPEG | | Picture | Fil |
| 46 | googleplus-ie-01[2].jpg | Notable files | e35985ac2931824b1846e9320ef52063 | | jpg | JPEG | | Picture | Fil |
| 47 | googleplus-ie-03[1].jpg | Notable files | e28608d558b4f7380bd8eb45fc0f6454 | | jpg | JPEG | | Picture | Fil |
| 48 | googleplus-safari-01[1].jpg | Notable files | b4951b876bbce8d19fc3b5afd5d102ec | | jpg | JPEG | | Picture | Fil |
| 49 | googleplus-safari-03[1].jpg | Notable files | efe4542cfa7dc567192fd91adf7e23f2 | | jpg | JPEG | | Picture | Fil |
| 50 | googleplus-safari-04[1].jpg | Notable files | ee323873d364623a602925f0771b7228 | | jpg | JPEG | | Picture | Fil |
| 51 | googleplus-safari-05[1].jpg | Notable files | 33eaa32a766d0bfa9e2dca1ed54e4cfd | | jpg | JPEG | | Picture | Fil |
| 52 | linkedin-ie-04[1].jpg | Notable files | 87b05c6484cd59aa51638fd78665f516 | | jpg | JPEG | | Picture | Fil |
| 53 | googleplus-ie-04[1].jpg | Notable files | 44c2f7c082c33ba8db32ffd9c660cc61 | | jpg | JPEG | | Picture | Fil |
| 54 | linkedin-ie-02[1].jpg | Notable files | c4ee401fa115b131dd254419309ff354 | | jpg | JPEG | | Picture | Fil |
| 55 | linkedin-ie-05[1].jpg | Notable files | 4fc7915ceb164b5ad2adcd8ea17561be | | jpg | JPEG | | Picture | Fil |
| 56 | E51BDd01 | Notable files | 79dbd03acfa0af1807251048a5b96650 | | | | | | Fil |
| 57 | 954E2d01 | Notable files | 239a73bd7644c169fbd19fc6524813c7 | | | | | | Fil |



# Appendix C-11 Encase - Email extraction result

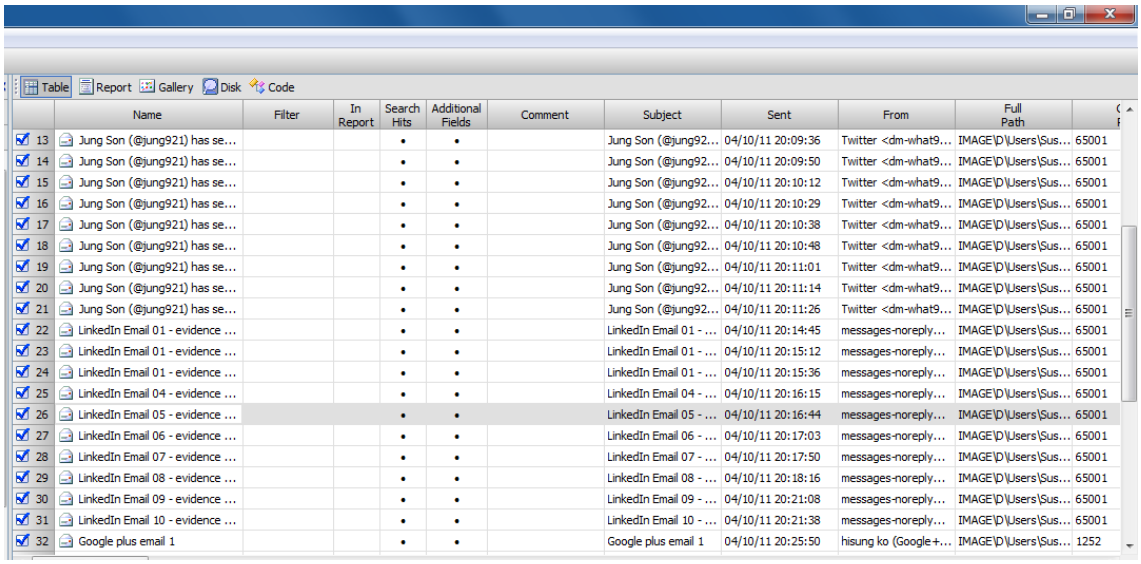


Table | Report | Gallery | Disk | Code

| | Name | Filter | In Report | Search Hits | Additional Fields | Comment | Subject | Sent | From | Full Path | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | Jung Son (@jung921) has se... | | | • | • | | Jung Son (@jung92... | 04/10/11 20:09:36 | Twitter <dm-what9... | IMAGE\D\Users\Sus... | 65001 |
| 14 | Jung Son (@jung921) has se... | | | • | • | | Jung Son (@jung92... | 04/10/11 20:09:50 | Twitter <dm-what9... | IMAGE\D\Users\Sus... | 65001 |
| 15 | Jung Son (@jung921) has se... | | | • | • | | Jung Son (@jung92... | 04/10/11 20:10:12 | Twitter <dm-what9... | IMAGE\D\Users\Sus... | 65001 |
| 16 | Jung Son (@jung921) has se... | | | • | • | | Jung Son (@jung92... | 04/10/11 20:10:29 | Twitter <dm-what9... | IMAGE\D\Users\Sus... | 65001 |
| 17 | Jung Son (@jung921) has se... | | | • | • | | Jung Son (@jung92... | 04/10/11 20:10:38 | Twitter <dm-what9... | IMAGE\D\Users\Sus... | 65001 |
| 18 | Jung Son (@jung921) has se... | | | • | • | | Jung Son (@jung92... | 04/10/11 20:10:48 | Twitter <dm-what9... | IMAGE\D\Users\Sus... | 65001 |
| 19 | Jung Son (@jung921) has se... | | | • | • | | Jung Son (@jung92... | 04/10/11 20:11:01 | Twitter <dm-what9... | IMAGE\D\Users\Sus... | 65001 |
| 20 | Jung Son (@jung921) has se... | | | • | • | | Jung Son (@jung92... | 04/10/11 20:11:14 | Twitter <dm-what9... | IMAGE\D\Users\Sus... | 65001 |
| 21 | Jung Son (@jung921) has se... | | | • | • | | Jung Son (@jung92... | 04/10/11 20:11:26 | Twitter <dm-what9... | IMAGE\D\Users\Sus... | 65001 |
| 22 | LinkedIn Email 01 - evidence ... | | | • | • | | LinkedIn Email 01 - ... | 04/10/11 20:14:45 | messages-noreply... | IMAGE\D\Users\Sus... | 65001 |
| 23 | LinkedIn Email 01 - evidence ... | | | • | • | | LinkedIn Email 01 - ... | 04/10/11 20:15:12 | messages-noreply... | IMAGE\D\Users\Sus... | 65001 |
| 24 | LinkedIn Email 01 - evidence ... | | | • | • | | LinkedIn Email 01 - ... | 04/10/11 20:15:36 | messages-noreply... | IMAGE\D\Users\Sus... | 65001 |
| 25 | LinkedIn Email 04 - evidence ... | | | • | • | | LinkedIn Email 04 - ... | 04/10/11 20:16:15 | messages-noreply... | IMAGE\D\Users\Sus... | 65001 |
| 26 | LinkedIn Email 05 - evidence ... | | | • | • | | LinkedIn Email 05 - ... | 04/10/11 20:16:44 | messages-noreply... | IMAGE\D\Users\Sus... | 65001 |
| 27 | LinkedIn Email 06 - evidence ... | | | • | • | | LinkedIn Email 06 - ... | 04/10/11 20:17:03 | messages-noreply... | IMAGE\D\Users\Sus... | 65001 |
| 28 | LinkedIn Email 07 - evidence ... | | | • | • | | LinkedIn Email 07 - ... | 04/10/11 20:17:50 | messages-noreply... | IMAGE\D\Users\Sus... | 65001 |
| 29 | LinkedIn Email 08 - evidence ... | | | • | • | | LinkedIn Email 08 - ... | 04/10/11 20:18:16 | messages-noreply... | IMAGE\D\Users\Sus... | 65001 |
| 30 | LinkedIn Email 09 - evidence ... | | | • | • | | LinkedIn Email 09 - ... | 04/10/11 20:21:08 | messages-noreply... | IMAGE\D\Users\Sus... | 65001 |
| 31 | LinkedIn Email 10 - evidence ... | | | • | • | | LinkedIn Email 10 - ... | 04/10/11 20:21:38 | messages-noreply... | IMAGE\D\Users\Sus... | 65001 |
| 32 | Google plus email 1 | | | • | • | | Google plus email 1 | 04/10/11 20:25:50 | hisung ko (Google+... | IMAGE\D\Users\Sus... | 1252 |

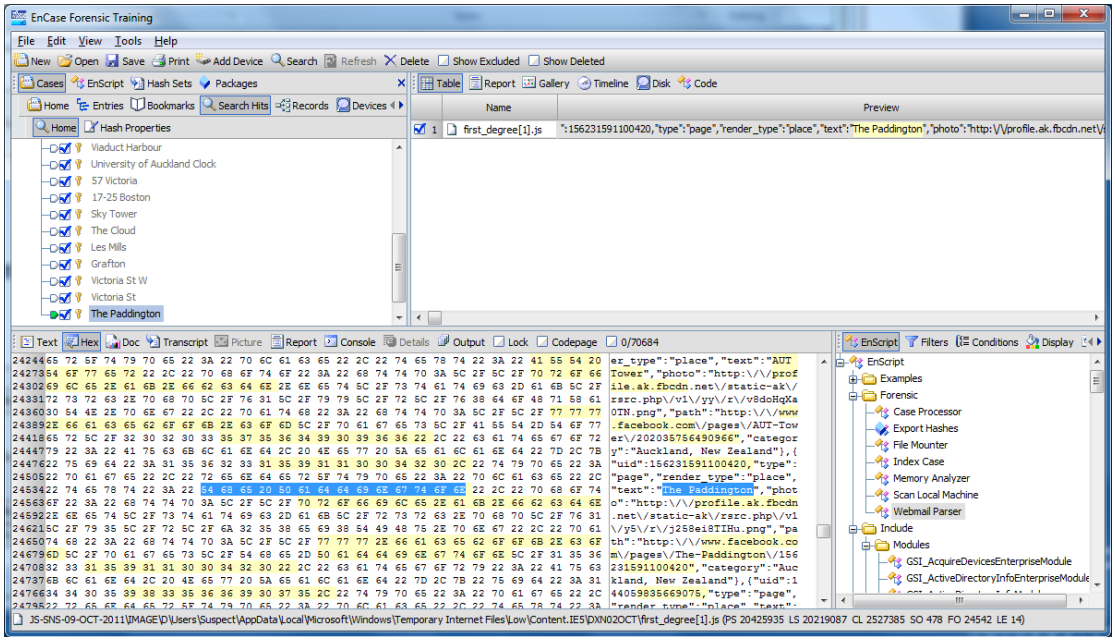
Text | Hex | Doc | Transcript | Picture | Report | Console | Details | Output | Lock | Codepage | 3344/70684

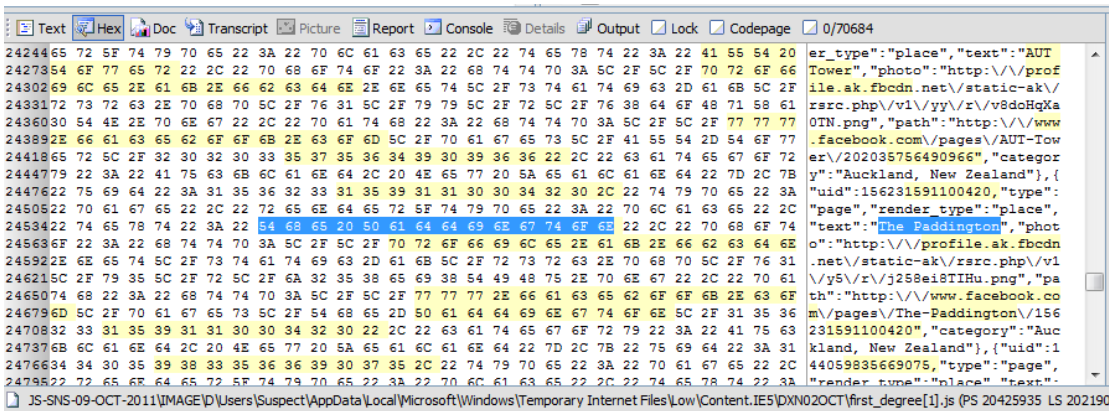
| | |
|---|---|
| Name | LinkedIn Email 05 - evidence email message from Linked In |
| Search Hits | • |
| Additional Fields | • |
| Subject | LinkedIn Email 05 - evidence email message from Linked In |
| Sent | 04/10/11 20:16:44 |
| Received | 04/10/11 20:16:46 |
| Message Size | 10168 |
| Created | 04/10/11 20:21:47 |
| Last Modification Time | 04/10/11 20:21:47 |
| To | Jung Son <jung921@gmail.com> |
| From | messages-noreply@bounce.linkedin.com <messages-noreply@bounce.linkedin.com> |
| Full Path | IMAGE\D\Users\Suspect\AppData\Local\Microsoft\Outlook\Outlook.pst\PST Volume\Root folder\Top of Personal Folders\Inbox\LinkedIn Email 05 - evidence email message from Linked In\PR_HTML |
| Code Page | 65001 |
| Email Type | Outlook (PST) |

---

LinkedIn Hi Sung Ko has sent you a message. Date: 10/04/2011 Subject: LinkedIn Email 05 - evidence email message from Linked In A man in south China's Hainan province braves strong winds and rain from typhoon Nesat. View/reply to this message [http://www.linkedin.com/e/-dhpm6z-gtck28ra-4x/-uZF7ZluwzVmVr...] Don't want to receive e-mail notifications? Adjust your message settings [http://www.linkedin.com/e/-dhpm6z-gtck28ra-4x/-uZF7ZluwzVmVr...] . ©2011, LinkedIn Corporation

# Appendix C-12 Encase - location extraction



# Appendix C-13 Encase – Wall post / Status update extraction

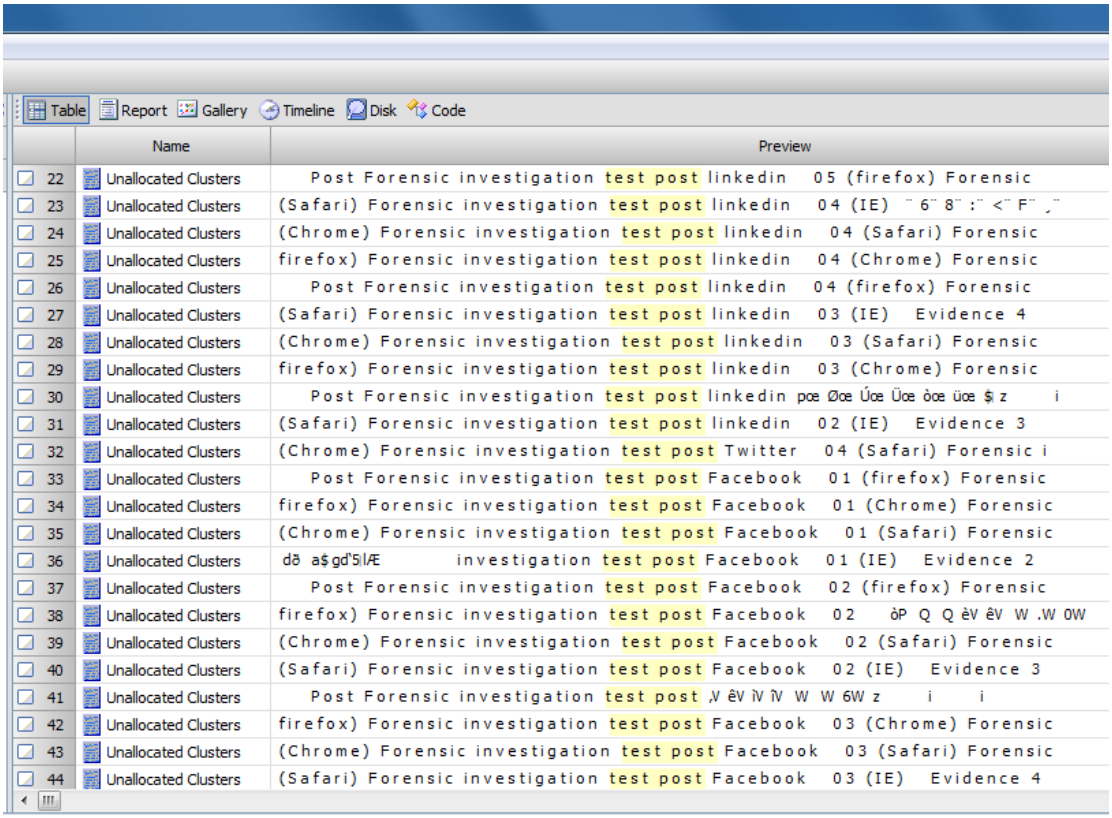
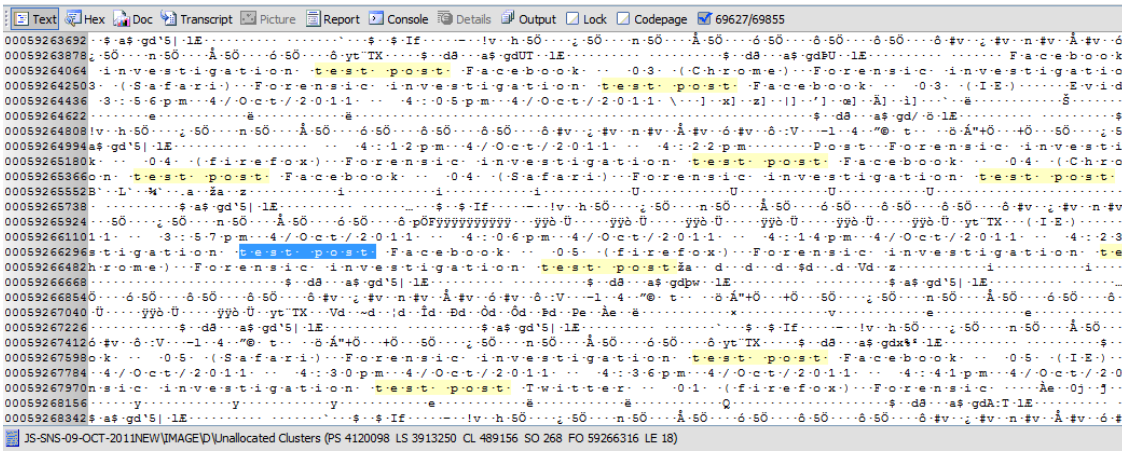


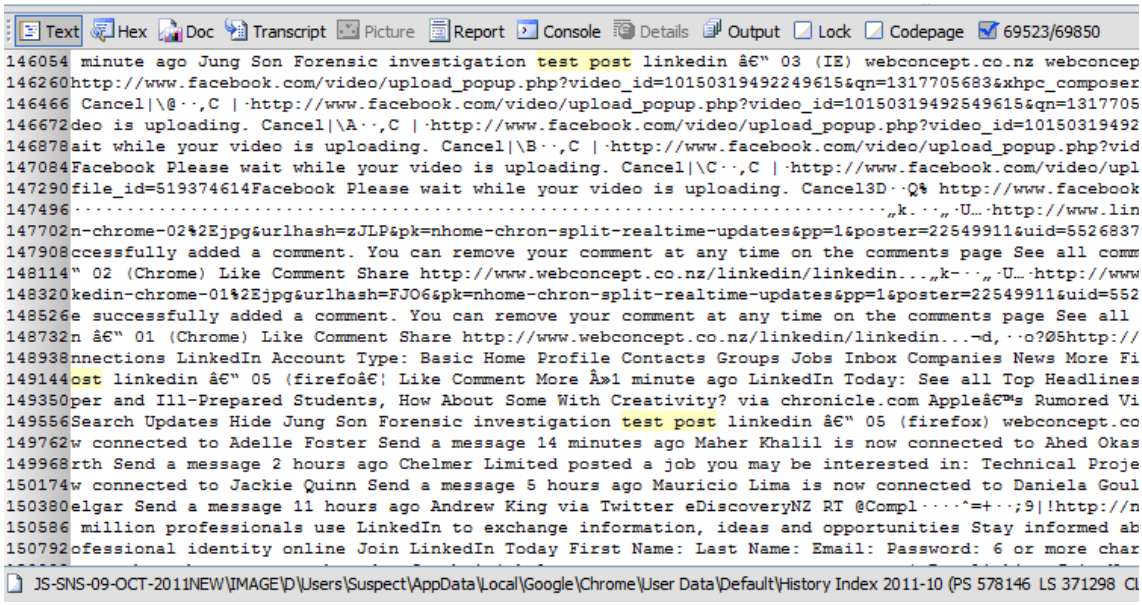
Table | Report | Gallery | Timeline | Disk | Code

| | Name | Preview |
|---|---|---|
| 22 | Unallocated Clusters | Post Forensic investigation test post linkedin 05 (firefox) Forensic |
| 23 | Unallocated Clusters | (Safari) Forensic investigation test post linkedin 04 (IE) ¨ 6¨ 8¨ :¨ <¨ F¨ ¸¨ |
| 24 | Unallocated Clusters | (Chrome) Forensic investigation test post linkedin 04 (Safari) Forensic |
| 25 | Unallocated Clusters | firefox) Forensic investigation test post linkedin 04 (Chrome) Forensic |
| 26 | Unallocated Clusters | Post Forensic investigation test post linkedin 04 (firefox) Forensic |
| 27 | Unallocated Clusters | (Safari) Forensic investigation test post linkedin 03 (IE) Evidence 4 |
| 28 | Unallocated Clusters | (Chrome) Forensic investigation test post linkedin 03 (Safari) Forensic |
| 29 | Unallocated Clusters | firefox) Forensic investigation test post linkedin 03 (Chrome) Forensic |
| 30 | Unallocated Clusters | Post Forensic investigation test post linkedin poe Øœ Úœ Üœ òœ üœ $ z i |
| 31 | Unallocated Clusters | (Safari) Forensic investigation test post linkedin 02 (IE) Evidence 3 |
| 32 | Unallocated Clusters | (Chrome) Forensic investigation test post Twitter 04 (Safari) Forensic i |
| 33 | Unallocated Clusters | Post Forensic investigation test post Facebook 01 (firefox) Forensic |
| 34 | Unallocated Clusters | firefox) Forensic investigation test post Facebook 01 (Chrome) Forensic |
| 35 | Unallocated Clusters | (Chrome) Forensic investigation test post Facebook 01 (Safari) Forensic |
| 36 | Unallocated Clusters | dð a$gd'5lÆ investigation test post Facebook 01 (IE) Evidence 2 |
| 37 | Unallocated Clusters | Post Forensic investigation test post Facebook 02 (firefox) Forensic |
| 38 | Unallocated Clusters | firefox) Forensic investigation test post Facebook 02 ðP Q Q èV êV W .W 0W |
| 39 | Unallocated Clusters | (Chrome) Forensic investigation test post Facebook 02 (Safari) Forensic |
| 40 | Unallocated Clusters | (Safari) Forensic investigation test post Facebook 02 (IE) Evidence 3 |
| 41 | Unallocated Clusters | Post Forensic investigation test post ,V êV ìV ÎV W W 6W z i i |
| 42 | Unallocated Clusters | firefox) Forensic investigation test post Facebook 03 (Chrome) Forensic |
| 43 | Unallocated Clusters | (Chrome) Forensic investigation test post Facebook 03 (Safari) Forensic |
| 44 | Unallocated Clusters | (Safari) Forensic investigation test post Facebook 03 (IE) Evidence 4 |



Text | Hex | Doc | Transcript | Picture | Report | Console | Details | Output | Lock | Codepage | 69627/69855

JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters (PS 4120098 LS 3913250 CL 489156 SO 268 FO 59266316 LE 18)


Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 69523/69850
146054 minute ago Jung Son Forensic investigation test post linkedin â€" 03 (IE) webconcept.co.nz webconcep
146260http://www.facebook.com/video/upload_popup.php?video_id=10150319492249615&qn=1317705683&xhpc_composer
146466 Cancel|\@··,C |·http://www.facebook.com/video/upload_popup.php?video_id=10150319492549615&qn=1317705
146672deo is uploading. Cancel|\A··,C |·http://www.facebook.com/video/upload_popup.php?video_id=10150319492
146878ait while your video is uploading. Cancel|\B··,C |·http://www.facebook.com/video/upload_popup.php?vid
147084Facebook Please wait while your video is uploading. Cancel|\C··,C |·http://www.facebook.com/video/upl
147290file_id=519374614Facebook Please wait while your video is uploading. Cancel3D··Q% http://www.facebook
147496·····„k.··„·U…·http://www.lin
147702n-chrome-02%2Ejpg&urlhash=zJLP&pk=nhome-chron-split-realtime-updates&pp=1&poster=22549911&uid=5526837
147908ccessfully added a comment. You can remove your comment at any time on the comments page See all comm
148114" 02 (Chrome) Like Comment Share http://www.webconcept.co.nz/linkedin/linkedin...„k-··„·U…·http://www
148320kedin-chrome-01%2Ejpg&urlhash=FJO6&pk=nhome-chron-split-realtime-updates&pp=1&poster=22549911&uid=552
148526e successfully added a comment. You can remove your comment at any time on the comments page See all
148732n â€" 01 (Chrome) Like Comment Share http://www.webconcept.co.nz/linkedin/linkedin...¬d,··o?Ø5http://
148938nnections LinkedIn Account Type: Basic Home Profile Contacts Groups Jobs Inbox Companies News More Fi
149144ost linkedin â€" 05 (firefoâ€¦ Like Comment More Â»1 minute ago LinkedIn Today: See all Top Headlines
149350per and Ill-Prepared Students, How About Some With Creativity? via chronicle.com Appleâ€™s Rumored Vi
149556Search Updates Hide Jung Son Forensic investigation test post linkedin â€" 05 (firefox) webconcept.co
149762w connected to Adelle Foster Send a message 14 minutes ago Maher Khalil is now connected to Ahed Okas
149968rth Send a message 2 hours ago Chelmer Limited posted a job you may be interested in: Technical Proje
150174w connected to Jackie Quinn Send a message 5 hours ago Mauricio Lima is now connected to Daniela Goul
150380elgar Send a message 11 hours ago Andrew King via Twitter eDiscoveryNZ RT @Compl····^=+··;9|!http://n
150586 million professionals use LinkedIn to exchange information, ideas and opportunities Stay informed ab
150792ofessional identity online Join LinkedIn Today First Name: Last Name: Email: Password: 6 or more char
JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Google\Chrome\User Data\Default\History Index 2011-10 (PS 578146 LS 371298 Cl

## Wall post found from Safari browser – EnCase

| Name | Preview | Full Path |
|---|---|---|
| Cache.db |  Forensic investigation test post linkedin – 03 (Safari)  | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| Cache.db |  Forensic investigation test post linkedin – 01 (Safari)  | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| Cache.db |  Forensic investigation test post linkedin – 04 (Safari)  | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| Cache.db | /span></a> Forensic investigation test post linkedin – 03 (Safari) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| Cache.db | /span></a> Forensic investigation test post linkedin – 05 (Safari) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| Cache.db |  Forensic investigation test post linkedin – 05 (Safari)  | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| Cache.db | /span></a> Forensic investigation test post linkedin – 04 (Safari) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| Cache.db | /span></a> Forensic investigation test post linkedin – 01 (Safari) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| Cache.db | /span></a> Forensic investigation test post linkedin – 02 (Safari) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| Cache.db |  Forensic investigation test post Twitter – 05 (Safari) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| Cache.db |  Forensic investigation test post Twitter – 04 (Safari) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| Cache.db |  Forensic investigation test post Twitter – 03 (Safari) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| Cache.db |  Forensic investigation test post linkedin – 02 (Safari)  | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\Cache.db |
| _11.cfs | Sign OutWelcome, Jung Son Jung Son Forensic investigation test post linkedin â€“ 03 (Safari) Like Comment Share http://www.webc | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\History_11.cfs |

| | | |
|---|---|---|
| _11.cfs | 0Te4 1 hour ago jung921 Jung Son Forensic investigation test post Twitter â€“ 05 (Safari) pic.twitter.com/wNdBHwoK 1 hour ago | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\History_11.cfs |
| _11.cfs | HwoK 1 hour ago jung921 Jung Son Forensic investigation test post Twitter â€“ 04 (Safari) pic.twitter.com/cGHAXPZP 1 hour ago | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\History_11.cfs |
| _11.cfs | XPZP 1 hour ago jung921 Jung Son Forensic investigation test post Twitter â€“ 03 (Safari) pic.twitter.com/oLICLkTk 1 hour ago | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\History_11.cfs |
| _11.cfs | LkTk 1 hour ago jung921 Jung Son Forensic investigation test post Twitter â€“ 02 (Safari) pic.twitter.com/WobnHxfk 1 hour ago | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\History_11.cfs |
| _11.cfs | efox - 05 2 minutes ago Jung Son Forensic investigation test post linkedin â€“ 05 (Safari) webconcept.co.nz webconcept.co.nz | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\History_11.cfs |
| _11.cfs | ) more updates from Jung Jung Son Forensic investigation test post linkedin â€“ 04 (Safari) webconcept.co.nz webconcept.co.nz | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\History_11.cfs |
| _11.cfs | hrome - 01 1 minute ago Jung Son Forensic investigation test post linkedin â€“ 03 (Safari) webconcept.co.nz webconcept.co.nz | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\History_11.cfs |
| _11.cfs | 02 55 seconds ago Hide Jung Son Forensic investigation test post linkedin â€“ 02 (Safari) webconcept.co.nz webconcept.co.nz | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\History_11.cfs |
| _11.cfs | ome - 03 50 seconds ago Jung Son Forensic investigation test post linkedin â€“ 01 (Safari) webconcept.co.nz webconcept.co.nz | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\AppData\Local\Apple Computer\Safari\History_11.cfs |

## Wall post found from Chrome browser - EnCase

| Name | Preview | Full Path |
|---|---|---|
| History Index 2011-10 | Sign OutWelcome, Jung Son Jung Son Forensic investigation test post linkedin â€“ 02 (Chrome) Like Comment Share http://www.webc | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\App Data\Local\Google\Chrome\User Data\Default\History Index 2011-10 |
| History Index 2011-10 | Sign OutWelcome, Jung Son Jung Son Forensic investigation test post linkedin â€“ 01 (Chrome) Like Comment Share http://www.webc | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\App Data\Local\Google\Chrome\User Data\Default\History Index 2011-10 |
| History Index 2011-10 | Sign OutWelcome, Jung Son Jung Son Forensic investigation test post linkedin â€“ 05 (Chrome) Like Comment Share http://www.webc | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\App Data\Local\Google\Chrome\User Data\Default\History Index 2011-10 |
| History Index 2011-10 | Sign OutWelcome, Jung Son Jung Son Forensic investigation test post linkedin â€“ 03 (Chrome) Like Comment Share http://www.webc | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\App Data\Local\Google\Chrome\User Data\Default\History Index 2011-10 |
| History Index 2011-10 | lhAzPo8 1 hour ago jung921 Jung Son Forensic investigation test post Twitter â€“ 05 (Chrome) pic.twitter.com/kqlxF0he 1 hour ago | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\App Data\Local\Google\Chrome\User Data\Default\History Index 2011-10 |
| History Index 2011-10 | qlxF0he 1 hour ago jung921 Jung Son Forensic investigation test post Twitter â€“ 04 (Chrome) pic.twitter.com/DqGKaiLq 1 hour ago | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\App Data\Local\Google\Chrome\User Data\Default\History Index 2011-10 |
| History Index 2011-10 | qGKaiLq 1 hour ago jung921 Jung Son Forensic investigation test post Twitter â€“ 03 (Chrome) pic.twitter.com/VQReTTL4 1 hour ago | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\App Data\Local\Google\Chrome\User Data\Default\History Index 2011-10 |
| History Index 2011-10 | QReTTL4 1 hour ago jung921 Jung Son Forensic investigation test post Twitter â€“ 02 (Chrome) pic.twitter.com/kPLNRkvW 1 hour ago | JS-SNS-09-OCT-2011NEW\IMAGE\D\Users\Suspect\App Data\Local\Google\Chrome\User Data\Default\History Index 2011-10 |

## Wall post found from System Volume Information - EnCase

| Name | Preview | Full Path |
|---|---|---|
| {9cec5430-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} | ass="snippet"> ... STORIES Jung Son Forensic investigation test post Facebook â€“ 02 (Chrome) â€” at AUT Tower. Wall Phot | JS-SNS-09-OCT-2011NEW\IMAGE\D\System Volume Information\{9cec5430-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} |
| {9cec5430-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} | ass="snippet"> ... STORIES Jung Son Forensic investigation test post Facebook â€“ 02 (Chrome) â€” at AUT Tower. Wall Phot | JS-SNS-09-OCT-2011NEW\IMAGE\D\System Volume Information\{9cec5430-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} |
| {9cec5430-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} | Like Â· ... ... nds ago Jung Son Forensic investigation test post Facebook â€“ 01 (Chrome) â€” at AUT Tower. Wall Phot | JS-SNS-09-OCT-2011NEW\IMAGE\D\System Volume Information\{9cec5430-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} |
| {9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} | ass="snippet"> ... ung Son Jung Son Forensic investigation test post linkedin â€“ 02 (Chrome) Like Comment Share http://w | JS-SNS-09-OCT-2011NEW\IMAGE\D\System Volume Information\{9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} |
| {9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} | ass="snippet"> ... ung Son Jung Son Forensic investigation test post linkedin â€“ 03 (Chrome) Like Comment Share http://w | JS-SNS-09-OCT-2011NEW\IMAGE\D\System Volume Information\{9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} |
| {9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} | ass="snippet"> ... ung Son Jung Son Forensic investigation test post linkedin â€“ 04 (Chrome) Like Comment Share http://w | JS-SNS-09-OCT-2011NEW\IMAGE\D\System Volume Information\{9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} |
| {9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} | s Groups ... ... ed Attach a link Forensic investigation test post linkedin â€“ 05 (firefoâ€¦ Like Comment More Â»1 min | JS-SNS-09-OCT-2011NEW\IMAGE\D\System Volume Information\{9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} |
| {9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} | iv class="snippet">jung921 Jung Son Forensic investigation test post Twitter â€“ 01 (Chrome) pic.twitter.com/JBryc | JS-SNS-09-OCT-2011NEW\IMAGE\D\System Volume Information\{9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} |
| {9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} | iv class="snippet">jung921 Jung Son Forensic investigation test post Twitter â€“ 03 (Chrome) pic.twitter.com/APEhe | JS-SNS-09-OCT-2011NEW\IMAGE\D\System Volume Information\{9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} |

| | | |
|---|---|---|
| {9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} | iv class="snippet">jung921 Jung Son Forensic investigation test post Twitter â€“ 04 (Chrome) pic.twitter.com/7G1cY | JS-SNS-09-OCT-2011NEW\IMAGE\D\System Volume Information\{9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} |
| {9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} | Tweet jun ... ... jung921 Jung Son Forensic investigation test post Twitter â€“ 05 (firefox) pic.twitter.com/l3uQ | JS-SNS-09-OCT-2011NEW\IMAGE\D\System Volume Information\{9cec5434-ee2c-11e0-90f6-001143a4c194}{3808876b-c176-4e48-b7ae-04046e6cc752} |

## Wall post found from Unallocated Clusters - EnCase

| Name | Preview | Full Path |
|---|---|---|
| Unallocated Clusters | ost Forensic investigati on test post Facebook 01 (firefox) For | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigati on test post Facebook 01 (Chrome) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigati on test post Facebook 01 (Safari) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | gd‘5□ lÆ investigati on test post Facebook 01 (IE) Eviden | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigati on test post Facebook 02 (firefox) For | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigati on test post Facebook 02 òP Q Q èV êV | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigati on test post Facebook 02 (Safari) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigatio n test post Facebook 0 2 (IE) Eviden | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigati on test post ,V êV ìV îV W W 6W z i | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigati on test post Facebook 03 (Chrome) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigati on test post Facebook 03 (Safari) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigatio n test post Facebook 0 3 (IE) Eviden | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigati on test post Facebook 04 (firefox) For | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigati on test post Facebook 04 (Chrome) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigati on test post Facebook 04 (Safari) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigatio n test post Facebook 0 4 ` <` >` @` B` L | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigati on test post Facebook 05 (firefox) For | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |

| | | |
|---|---|---|
| Unallocated Clusters | ox) Forensic investigati on test post Facebook 05 (Chrome) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigati on test postža d d d $d .d Vd z i i | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigatio n test post Facebook 0 5 (IE) Twitter | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigati on test post Twitter 01 (firefox) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ÿÿò Ü ÿÿò Ü yt¨TX investig ation test post Twitter 01 (Chrome) Foren | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigati on test post Twitter 01 (Safari) Foren | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigatio n test post Twitter 01 ( IE) Evidenc | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigati on test post Twitter 02 (firefox) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigati on test post Twitter 02 (Chrome) Foren | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigati on test post Twitter 02 (Safari) Foren | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigatio n test post Twitter 02 ( IE9) Eviden | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigati on test post Twitter 03 (firefox) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigati on test post Twitter 03 (Chrome) Foren | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigati on test post Twitter 03 (Safari) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigati on test post Google Plus 02 (firefox) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigati on test post Google Plus 02 (Chrome) F | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigati on test post Google Plus 02 (Safari) F | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigatio n test post Google Plus 02 (IE) Evi | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |

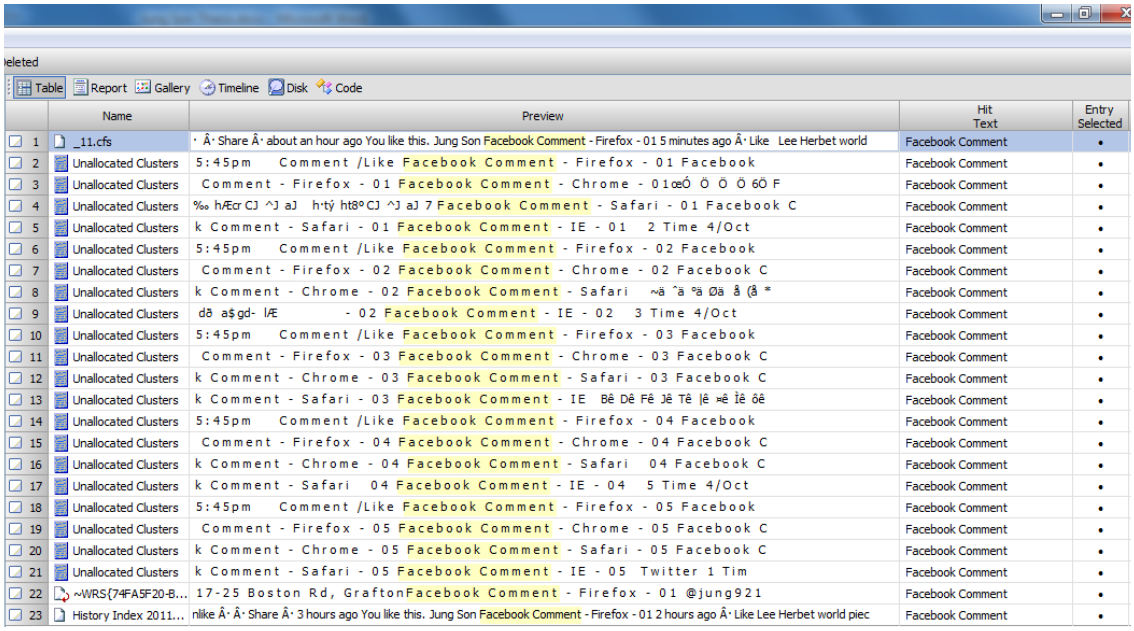
| | | |
|---|---|---|
| Unallocated Clusters | ost Forensic investigation test post Google Plus 03 (firefox) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigation test post Google Plus 03 (Chrome) F | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ÿÿò Ü ÿÿò Ü ÿÿò Ü ÿÿò Ü ÿÿò Ü yt¨TX test post Google Plus 03 (Safari) F | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigation test post Google Plus 03 (IE) Evi | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigation test post Google Plus 04 (firefox)H | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | Forensic investigation test post Google Plus 04 (Chrome) F | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigation test post Google Plus 04 (Safari) F | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigation test post Google Plus 04 (IE) Evi | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigation test post Google Plus 05 (firefox) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigation test post Google Plus 05 (Chrome) F | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigation test post Google Plus 05 (Safari) F | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigation test post Google Plus 05 øÏ (Ò *Ò ,Ò .Ò | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | F E KForensic investigation test post Twitter 03 (IE9) Eviden | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigation test post Twitter 04 (firefox) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigation test post Twitter â} h€ j€ l€ ,€ Œ€ ´€ z | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigation test post Twitter 04 (Safari) Foren | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigation test post Twitter 04 ( IE9) Eviden | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigation test post Twitter 05 (Chrome) Foren | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |

| | | |
|---|---|---|
| Unallocated Clusters | me) Forensic investigation test post Twitter 05 (Safari) Foren | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigation test post Twitter 05 (IE9) LinkedI | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigation test post linkedin 01 (firefox) For | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigation test post linkedin 01 (Chrome) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigation test post linkedin 01 (Safari) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigation test post linkedin 01 (IE) Eviden | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigation test post linkedin 02 (firefox) For | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigation test post linkedin 02 (Chrome) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | yt¨TX Forensic investigation test post linkedin 02 (Safari) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigation test post linkedin 02 (IE) Eviden | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigation test post linkedin pœ Øœ Úœ Üœ òœ üœ $□ z | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigation test post linkedin 03 (Chrome) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigation test post linkedin 03 (Safari) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigation test post linkedin 03 (IE) Eviden | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigation test post linkedin 04 (firefox) For | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigation test post linkedin 04 (Chrome) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigation test post linkedin 04 (Safari) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigation test post linkedin 04 (IE) ¨ 6¨ 8¨ :¨ | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |

| | | |
|---|---|---|
| Unallocated Clusters | ost Forensic investigation test post linkedin 05 (firefox) For | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ox) Forensic investigation test post linkedin 05 (Chrome) Fore | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigation test post L® t® œ® Ä® Æ® È® Ê® Ô® F¯ ¶¯ .² ë | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigation test post linkedin 05 (IE) Google | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ost Forensic investigation test post Google Plus 01 (firefox) | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ^J aJ 8Forensic investigation test post Google Plus 01 (Chrome) F | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | me) Forensic investigation test post Google Plus 01 (Safari) F | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |
| Unallocated Clusters | ri) Forensic investigation test post Google Plus 01 (IE) Evi | JS-SNS-09-OCT-2011NEW\IMAGE\D\Unallocated Clusters |

# Appendix C-14 Encase – Comment/Reply extraction

## Facebook comments

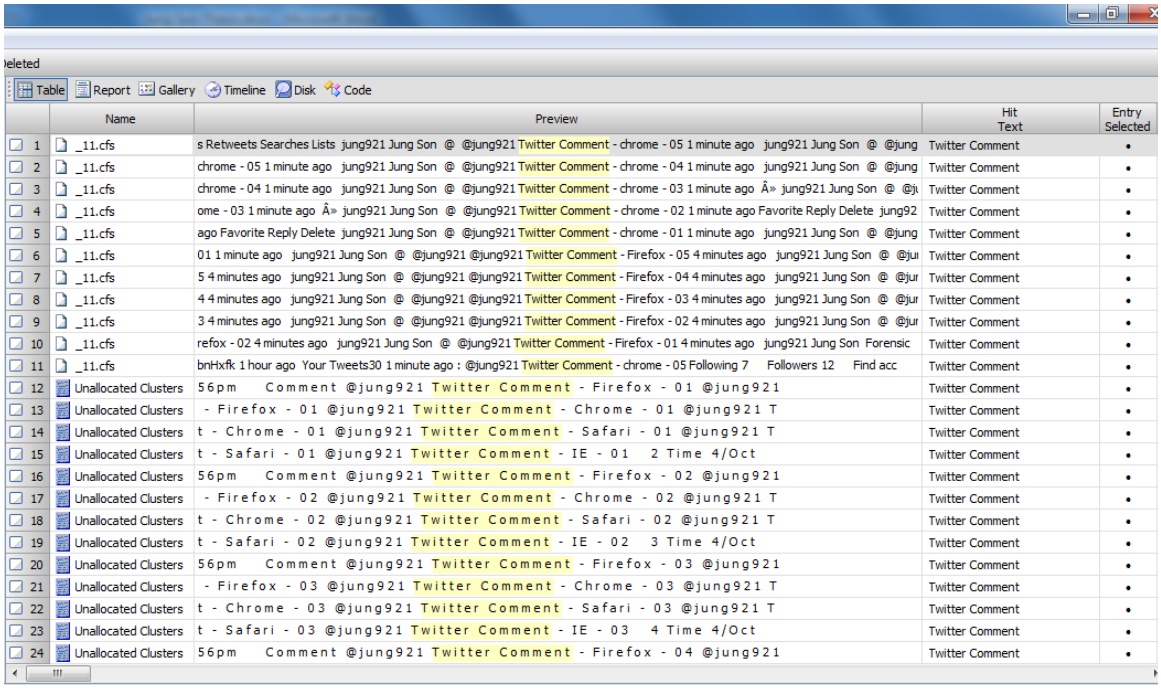


eleted

Table | Report | Gallery | Timeline | Disk | Code

| | Name | Preview | Hit Text | Entry Selected |
|---|---|---|---|---|
| 1 | _11.cfs | · Â· Share Â· about an hour ago You like this. Jung Son Facebook Comment - Firefox - 01 5 minutes ago Â· Like Lee Herbet world | Facebook Comment | • |
| 2 | Unallocated Clusters | 5:45pm Comment /Like Facebook Comment - Firefox - 01 Facebook | Facebook Comment | • |
| 3 | Unallocated Clusters | Comment - Firefox - 01 Facebook Comment - Chrome - 01œÓ Ö Ö Ö 6Ö F | Facebook Comment | • |
| 4 | Unallocated Clusters | ‰ hÆcr CJ ^J aJ h·tý ht8ºCJ ^J aJ 7 Facebook Comment - Safari - 01 Facebook C | Facebook Comment | • |
| 5 | Unallocated Clusters | k Comment - Safari - 01 Facebook Comment - IE - 01 2 Time 4/Oct | Facebook Comment | • |
| 6 | Unallocated Clusters | 5:45pm Comment /Like Facebook Comment - Firefox - 02 Facebook | Facebook Comment | • |
| 7 | Unallocated Clusters | Comment - Firefox - 02 Facebook Comment - Chrome - 02 Facebook C | Facebook Comment | • |
| 8 | Unallocated Clusters | k Comment - Chrome - 02 Facebook Comment - Safari ~ä ^ä °ä Øä å (å * | Facebook Comment | • |
| 9 | Unallocated Clusters | dð a$gd- lÆ - 02 Facebook Comment - IE - 02 3 Time 4/Oct | Facebook Comment | • |
| 10 | Unallocated Clusters | 5:45pm Comment /Like Facebook Comment - Firefox - 03 Facebook | Facebook Comment | • |
| 11 | Unallocated Clusters | Comment - Firefox - 03 Facebook Comment - Chrome - 03 Facebook C | Facebook Comment | • |
| 12 | Unallocated Clusters | k Comment - Chrome - 03 Facebook Comment - Safari - 03 Facebook C | Facebook Comment | • |
| 13 | Unallocated Clusters | k Comment - Safari - 03 Facebook Comment - IE Bê Dê Fê Jê Tê Ìê »ê Ìê ôê | Facebook Comment | • |
| 14 | Unallocated Clusters | 5:45pm Comment /Like Facebook Comment - Firefox - 04 Facebook | Facebook Comment | • |
| 15 | Unallocated Clusters | Comment - Firefox - 04 Facebook Comment - Chrome - 04 Facebook C | Facebook Comment | • |
| 16 | Unallocated Clusters | k Comment - Chrome - 04 Facebook Comment - Safari 04 Facebook C | Facebook Comment | • |
| 17 | Unallocated Clusters | k Comment - Safari 04 Facebook Comment - IE - 04 5 Time 4/Oct | Facebook Comment | • |
| 18 | Unallocated Clusters | 5:45pm Comment /Like Facebook Comment - Firefox - 05 Facebook | Facebook Comment | • |
| 19 | Unallocated Clusters | Comment - Firefox - 05 Facebook Comment - Chrome - 05 Facebook C | Facebook Comment | • |
| 20 | Unallocated Clusters | k Comment - Chrome - 05 Facebook Comment - Safari - 05 Facebook C | Facebook Comment | • |
| 21 | Unallocated Clusters | k Comment - Safari - 05 Facebook Comment - IE - 05 Twitter 1 Tim | Facebook Comment | • |
| 22 | ~WRS{74FA5F20-B... | 17-25 Boston Rd, GraftonFacebook Comment - Firefox - 01 @jung921 | Facebook Comment | • |
| 23 | History Index 2011... | nlike Â· Â· Share Â· 3 hours ago You like this. Jung Son Facebook Comment - Firefox - 01 2 hours ago Â· Like Lee Herbet world piec | Facebook Comment | • |

## Twitter comments

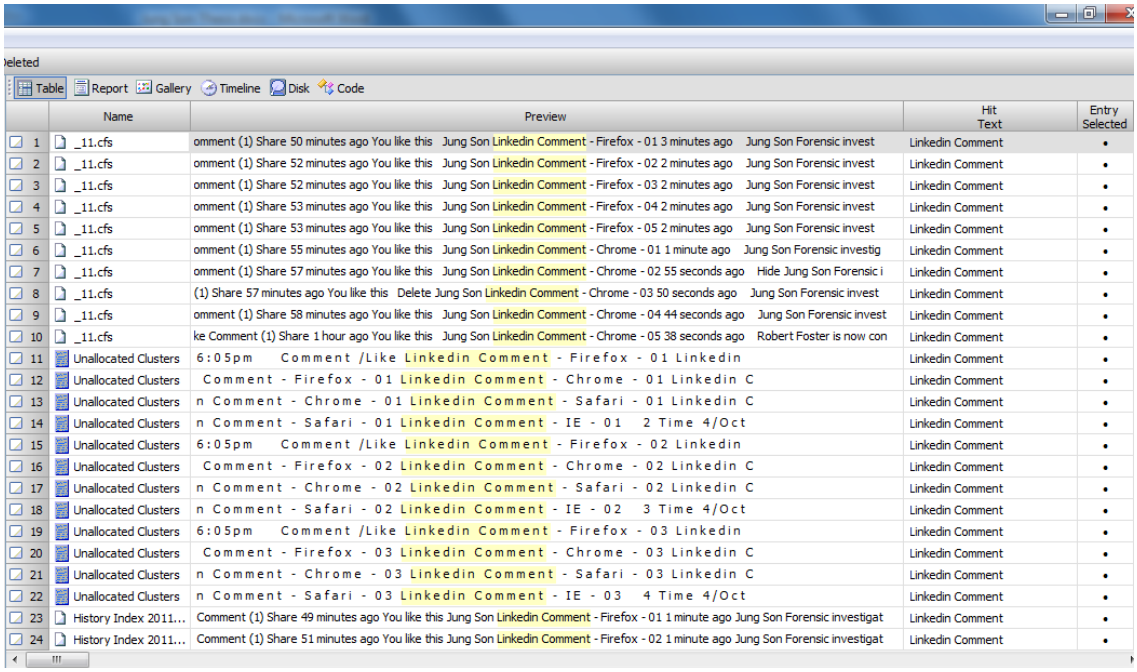


eleted

Table | Report | Gallery | Timeline | Disk | Code

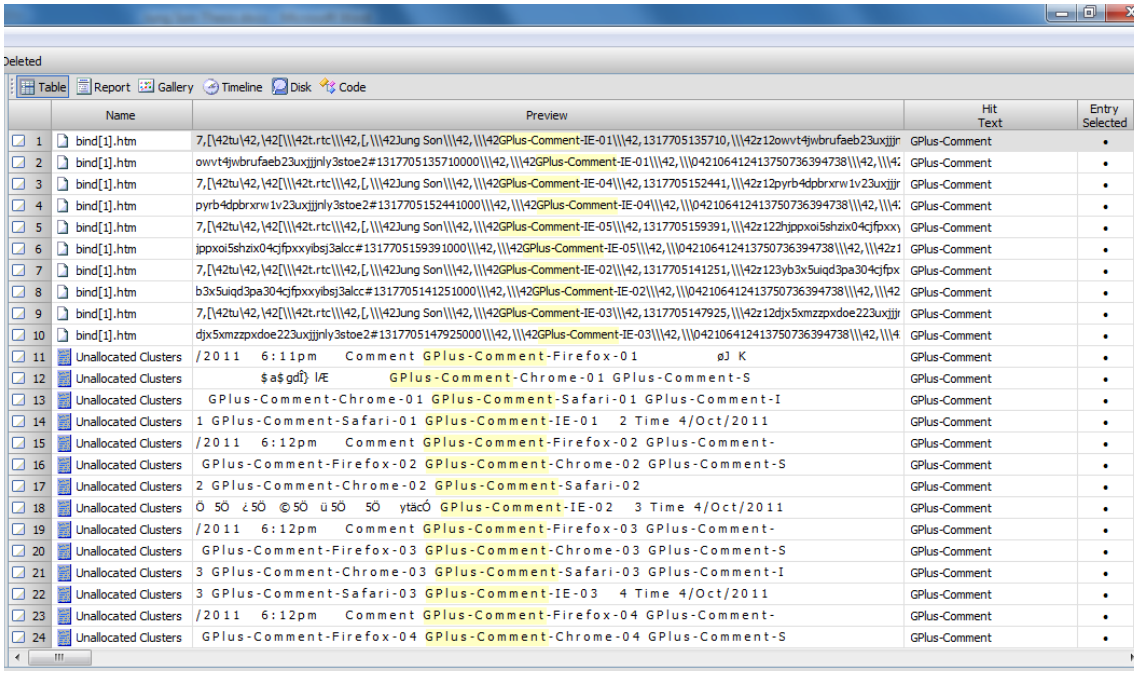
| | Name | Preview | Hit Text | Entry Selected |
|---|---|---|---|---|
| 1 | _11.cfs | s Retweets Searches Lists jung921 Jung Son @ @jung921 Twitter Comment - chrome - 05 1 minute ago jung921 Jung Son @ @jung | Twitter Comment | • |
| 2 | _11.cfs | chrome - 05 1 minute ago jung921 Jung Son @ @jung921 Twitter Comment - chrome - 04 1 minute ago jung921 Jung Son @ @jung | Twitter Comment | • |
| 3 | _11.cfs | chrome - 04 1 minute ago jung921 Jung Son @ @jung921 Twitter Comment - chrome - 03 1 minute ago Â» jung921 Jung Son @ @j | Twitter Comment | • |
| 4 | _11.cfs | ome - 03 1 minute ago Â» jung921 Jung Son @ @jung921 Twitter Comment - chrome - 02 1 minute ago Favorite Reply Delete jung92 | Twitter Comment | • |
| 5 | _11.cfs | ago Favorite Reply Delete jung921 Jung Son @ @jung921 Twitter Comment - chrome - 01 1 minute ago jung921 Jung Son @ @jung | Twitter Comment | • |
| 6 | _11.cfs | 01 1 minute ago jung921 Jung Son @ @jung921 @jung921 Twitter Comment - Firefox - 05 4 minutes ago jung921 Jung Son @ @ju | Twitter Comment | • |
| 7 | _11.cfs | 5 4 minutes ago jung921 Jung Son @ @jung921 @jung921 Twitter Comment - Firefox - 04 4 minutes ago jung921 Jung Son @ @ju | Twitter Comment | • |
| 8 | _11.cfs | 4 4 minutes ago jung921 Jung Son @ @jung921 @jung921 Twitter Comment - Firefox - 03 4 minutes ago jung921 Jung Son @ @ju | Twitter Comment | • |
| 9 | _11.cfs | 3 4 minutes ago jung921 Jung Son @ @jung921 @jung921 Twitter Comment - Firefox - 02 4 minutes ago jung921 Jung Son @ @ju | Twitter Comment | • |
| 10 | _11.cfs | refox - 02 4 minutes ago jung921 Jung Son @ @jung921 Twitter Comment - Firefox - 01 4 minutes ago jung921 Jung Son Forensic | Twitter Comment | • |
| 11 | _11.cfs | bnHxfk 1 hour ago Your Tweets30 1 minute ago : @jung921 Twitter Comment - chrome - 05 Following 7 Followers 12 Find acc | Twitter Comment | • |
| 12 | Unallocated Clusters | 56pm Comment @jung921 Twitter Comment - Firefox - 01 @jung921 | Twitter Comment | • |
| 13 | Unallocated Clusters | - Firefox - 01 @jung921 Twitter Comment - Chrome - 01 @jung921 T | Twitter Comment | • |
| 14 | Unallocated Clusters | t - Chrome - 01 @jung921 Twitter Comment - Safari - 01 @jung921 T | Twitter Comment | • |
| 15 | Unallocated Clusters | t - Safari - 01 @jung921 Twitter Comment - IE - 01 2 Time 4/Oct | Twitter Comment | • |
| 16 | Unallocated Clusters | 56pm Comment @jung921 Twitter Comment - Firefox - 02 @jung921 | Twitter Comment | • |
| 17 | Unallocated Clusters | - Firefox - 02 @jung921 Twitter Comment - Chrome - 02 @jung921 T | Twitter Comment | • |
| 18 | Unallocated Clusters | t - Chrome - 02 @jung921 Twitter Comment - Safari - 02 @jung921 T | Twitter Comment | • |
| 19 | Unallocated Clusters | t - Safari - 02 @jung921 Twitter Comment - IE - 02 3 Time 4/Oct | Twitter Comment | • |
| 20 | Unallocated Clusters | 56pm Comment @jung921 Twitter Comment - Firefox - 03 @jung921 | Twitter Comment | • |
| 21 | Unallocated Clusters | - Firefox - 03 @jung921 Twitter Comment - Chrome - 03 @jung921 T | Twitter Comment | • |
| 22 | Unallocated Clusters | t - Chrome - 03 @jung921 Twitter Comment - Safari - 03 @jung921 T | Twitter Comment | • |
| 23 | Unallocated Clusters | t - Safari - 03 @jung921 Twitter Comment - IE - 03 4 Time 4/Oct | Twitter Comment | • |
| 24 | Unallocated Clusters | 56pm Comment @jung921 Twitter Comment - Firefox - 04 @jung921 | Twitter Comment | • |

## LinkedIn comments



| | Name | Preview | Hit Text | Entry Selected |
|---|---|---|---|---|
| 1 | _11.cfs | omment (1) Share 50 minutes ago You like this Jung Son Linkedin Comment - Firefox - 01 3 minutes ago Jung Son Forensic invest | Linkedin Comment | • |
| 2 | _11.cfs | omment (1) Share 52 minutes ago You like this Jung Son Linkedin Comment - Firefox - 02 2 minutes ago Jung Son Forensic invest | Linkedin Comment | • |
| 3 | _11.cfs | omment (1) Share 52 minutes ago You like this Jung Son Linkedin Comment - Firefox - 03 2 minutes ago Jung Son Forensic invest | Linkedin Comment | • |
| 4 | _11.cfs | omment (1) Share 53 minutes ago You like this Jung Son Linkedin Comment - Firefox - 04 2 minutes ago Jung Son Forensic invest | Linkedin Comment | • |
| 5 | _11.cfs | omment (1) Share 53 minutes ago You like this Jung Son Linkedin Comment - Firefox - 05 2 minutes ago Jung Son Forensic invest | Linkedin Comment | • |
| 6 | _11.cfs | omment (1) Share 55 minutes ago You like this Jung Son Linkedin Comment - Chrome - 01 1 minute ago Jung Son Forensic investig | Linkedin Comment | • |
| 7 | _11.cfs | omment (1) Share 57 minutes ago You like this Jung Son Linkedin Comment - Chrome - 02 55 seconds ago Hide Jung Son Forensic i | Linkedin Comment | • |
| 8 | _11.cfs | (1) Share 57 minutes ago You like this Delete Jung Son Linkedin Comment - Chrome - 03 50 seconds ago Jung Son Forensic invest | Linkedin Comment | • |
| 9 | _11.cfs | omment (1) Share 58 minutes ago You like this Jung Son Linkedin Comment - Chrome - 04 44 seconds ago Jung Son Forensic invest | Linkedin Comment | • |
| 10 | _11.cfs | ke Comment (1) Share 1 hour ago You like this Jung Son Linkedin Comment - Chrome - 05 38 seconds ago Robert Foster is now con | Linkedin Comment | • |
| 11 | Unallocated Clusters | 6:05pm Comment /Like Linkedin Comment - Firefox - 01 Linkedin | Linkedin Comment | • |
| 12 | Unallocated Clusters | Comment - Firefox - 01 Linkedin Comment - Chrome - 01 Linkedin C | Linkedin Comment | • |
| 13 | Unallocated Clusters | n Comment - Chrome - 01 Linkedin Comment - Safari - 01 Linkedin C | Linkedin Comment | • |
| 14 | Unallocated Clusters | n Comment - Safari - 01 Linkedin Comment - IE - 01 2 Time 4/Oct | Linkedin Comment | • |
| 15 | Unallocated Clusters | 6:05pm Comment /Like Linkedin Comment - Firefox - 02 Linkedin | Linkedin Comment | • |
| 16 | Unallocated Clusters | Comment - Firefox - 02 Linkedin Comment - Chrome - 02 Linkedin C | Linkedin Comment | • |
| 17 | Unallocated Clusters | n Comment - Chrome - 02 Linkedin Comment - Safari - 02 Linkedin C | Linkedin Comment | • |
| 18 | Unallocated Clusters | n Comment - Safari - 02 Linkedin Comment - IE - 02 3 Time 4/Oct | Linkedin Comment | • |
| 19 | Unallocated Clusters | 6:05pm Comment /Like Linkedin Comment - Firefox - 03 Linkedin | Linkedin Comment | • |
| 20 | Unallocated Clusters | Comment - Firefox - 03 Linkedin Comment - Chrome - 03 Linkedin C | Linkedin Comment | • |
| 21 | Unallocated Clusters | n Comment - Chrome - 03 Linkedin Comment - Safari - 03 Linkedin C | Linkedin Comment | • |
| 22 | Unallocated Clusters | n Comment - Safari - 03 Linkedin Comment - IE - 03 4 Time 4/Oct | Linkedin Comment | • |
| 23 | History Index 2011... | Comment (1) Share 49 minutes ago You like this Jung Son Linkedin Comment - Firefox - 01 1 minute ago Jung Son Forensic investigat | Linkedin Comment | • |
| 24 | History Index 2011... | Comment (1) Share 51 minutes ago You like this Jung Son Linkedin Comment - Firefox - 02 1 minute ago Jung Son Forensic investigat | Linkedin Comment | • |

## Google Plus comments



| | Name | Preview | Hit Text | Entry Selected |
|---|---|---|---|---|
| 1 | bind[1].htm | 7,[\42tu\42,\42[\\\42t.rtc\\\42,[,\\\42Jung Son\\\42,\\\42GPlus-Comment-IE-01\\\42,1317705135710,\\\42z12owvt4jwbrufaeb23uxjjjr | GPlus-Comment | • |
| 2 | bind[1].htm | owvt4jwbrufaeb23uxjjjnly3stoe2#1317705135710000\\\42,\\\42GPlus-Comment-IE-01\\\42,\\\042106412413750736394738\\\42,\\\42 | GPlus-Comment | • |
| 3 | bind[1].htm | 7,[\42tu\42,\42[\\\42t.rtc\\\42,[,\\\42Jung Son\\\42,\\\42GPlus-Comment-IE-04\\\42,1317705152441,\\\42z12pyrb4dpbrxrw1v23uxjjjr | GPlus-Comment | • |
| 4 | bind[1].htm | pyrb4dpbrxrw1v23uxjjjnly3stoe2#1317705152441000\\\42,\\\42GPlus-Comment-IE-04\\\42,\\\042106412413750736394738\\\42,\\\42 | GPlus-Comment | • |
| 5 | bind[1].htm | 7,[\42tu\42,\42[\\\42t.rtc\\\42,[,\\\42Jung Son\\\42,\\\42GPlus-Comment-IE-05\\\42,1317705159391,\\\42z122hjppxoi5shzix04cjfpxxy | GPlus-Comment | • |
| 6 | bind[1].htm | jppxoi5shzix04cjfpxxyibsj3alcc#1317705159391000\\\42,\\\42GPlus-Comment-IE-05\\\42,\\\042106412413750736394738\\\42,\\\42z1 | GPlus-Comment | • |
| 7 | bind[1].htm | 7,[\42tu\42,\42[\\\42t.rtc\\\42,[,\\\42Jung Son\\\42,\\\42GPlus-Comment-IE-02\\\42,1317705141251,\\\42z123yb3x5uiqd3pa304cjfpx | GPlus-Comment | • |
| 8 | bind[1].htm | b3x5uiqd3pa304cjfpxxyibsj3alcc#1317705141251000\\\42,\\\42GPlus-Comment-IE-02\\\42,\\\042106412413750736394738\\\42,\\\42 | GPlus-Comment | • |
| 9 | bind[1].htm | 7,[\42tu\42,\42[\\\42t.rtc\\\42,[,\\\42Jung Son\\\42,\\\42GPlus-Comment-IE-03\\\42,1317705147925,\\\42z12djx5xmzzpxdoe223uxjjjr | GPlus-Comment | • |
| 10 | bind[1].htm | djx5xmzzpxdoe223uxjjjnly3stoe2#1317705147925000\\\42,\\\42GPlus-Comment-IE-03\\\42,\\\042106412413750736394738\\\42,\\\42 | GPlus-Comment | • |
| 11 | Unallocated Clusters | /2011 6:11pm Comment GPlus-Comment-Firefox-01 øJ K | GPlus-Comment | • |
| 12 | Unallocated Clusters | $a$ gdÎ} lÆ GPlus-Comment-Chrome-01 GPlus-Comment-S | GPlus-Comment | • |
| 13 | Unallocated Clusters | GPlus-Comment-Chrome-01 GPlus-Comment-Safari-01 GPlus-Comment-I | GPlus-Comment | • |
| 14 | Unallocated Clusters | 1 GPlus-Comment-Safari-01 GPlus-Comment-IE-01 2 Time 4/Oct/2011 | GPlus-Comment | • |
| 15 | Unallocated Clusters | /2011 6:12pm Comment GPlus-Comment-Firefox-02 GPlus-Comment- | GPlus-Comment | • |
| 16 | Unallocated Clusters | GPlus-Comment-Firefox-02 GPlus-Comment-Chrome-02 GPlus-Comment-S | GPlus-Comment | • |
| 17 | Unallocated Clusters | 2 GPlus-Comment-Chrome-02 GPlus-Comment-Safari-02 | GPlus-Comment | • |
| 18 | Unallocated Clusters | Ö 5Ö ¿5Ö ©5Ö ü5Ö 5Ö ytäcÓ GPlus-Comment-IE-02 3 Time 4/Oct/2011 | GPlus-Comment | • |
| 19 | Unallocated Clusters | /2011 6:12pm Comment GPlus-Comment-Firefox-03 GPlus-Comment- | GPlus-Comment | • |
| 20 | Unallocated Clusters | GPlus-Comment-Firefox-03 GPlus-Comment-Chrome-03 GPlus-Comment-S | GPlus-Comment | • |
| 21 | Unallocated Clusters | 3 GPlus-Comment-Chrome-03 GPlus-Comment-Safari-03 GPlus-Comment-I | GPlus-Comment | • |
| 22 | Unallocated Clusters | 3 GPlus-Comment-Safari-03 GPlus-Comment-IE-03 4 Time 4/Oct/2011 | GPlus-Comment | • |
| 23 | Unallocated Clusters | /2011 6:12pm Comment GPlus-Comment-Firefox-04 GPlus-Comment- | GPlus-Comment | • |
| 24 | Unallocated Clusters | GPlus-Comment-Firefox-04 GPlus-Comment-Chrome-04 GPlus-Comment-S | GPlus-Comment | • |

# Appendix C-15 Facebook Chatting raw file

facebook-text.txt


```
["chat-msg-event\"]=JSCC.get('i4e8c1ebd16f85549187029116');templates[\"chat-sheet-notice\"]=JSCC.get
('i4e8c1ebd16f85549187029117');window.chatDisplay = new ChatDisplayInterim({\"750190551\":[{\"from\":519374614,\"to\":750190551,\"time\":
1317801980085,\"msgId\":\"1317801977539:2166487281\",\"msg\":{\"text\":\"dlTekrk so wkwl Qkfdkwnj! TkfEoRkwl!!\",\"messageId\":\"id.
227090730682701\"},\"type\":\"msg\"},{\"from\":750190551,\"to\":519374614,\"time\":1317802040175,\"msgId\":null,\"msg\":{\"text\":\"Wat?\",
\"messageId\":\"id.265134373526413\"},\"type\":\"msg\"},{\"from\":750190551,\"to\":519374614,\"time\":1317802051610,\"msgId\":null,\"msg\":
{\"text\":\"Ok. \",\"messageId\":\"id.243970542321851\"},\"type\":\"msg\"},{\"from\":750190551,\"to\":519374614,\"time\":
1317802062747,\"msgId\":null,\"msg\":{\"text\":\"Wat kinda business?\",\"messageId\":\"id.299151090100506\"},\"type\":\"msg\"},{\"from\":
519374614,\"to\":750190551,\"time\":1317802093193,\"msgId\":\"1317802090704:2711686307\",\"msg\":{\"text\":\"de ddql bang business\",
\"messageId\":\"id.256526721058996\"},\"type\":\"msg\"},{\"from\":519374614,\"to\":750190551,\"time\":1317802175583,\"msgId\":
\"1317802173182:912047377\",\"msg\":{\"text\":\"What are you doing now? I mean before you chat with me?\",\"messageId\":\"id.
131618556940330\"},\"type\":\"msg\"},{\"from\":750190551,\"to\":519374614,\"time\":1317802248017,\"msgId\":null,\"msg\":{\"text\":\"I will
cut ur \",\"messageId\":\"id.269263323108266\"},\"type\":\"msg\"},{\"from\":750190551,\"to\":519374614,\"time\":1317802268441,\"msgId
\":null,\"msg\":{\"text\":\"U will never have \",\"messageId\":\"id.178316382248060\"},\"type\":\"msg\"},{\"from\":750190551,\"to\":
519374614,\"time\":1317802288371,\"msgId\":null,\"msg\":{\"text\":\"U happy with dat?\",\"messageId\":\"id.209327855801148\"},\"type\":
\"msg\"},{\"from\":750190551,\"to\":519374614,\"time\":1317802299905,\"msgId\":null,\"msg\":{\"text\":\"Internet too slow \",\"messageId\":
\"id.117945178312411\"},\"type\":\"msg\"},{\"from\":750190551,\"to\":519374614,\"time\":1317802308215,\"msgId\":null,\"msg\":{\"text\":\"Or
this Facebook slow\",\"messageId\":\"id.222409561156775\"},\"type\":\"msg\"},{\"from\":519374614,\"to\":750190551,\"time\":
1317802380861,\"msgId\":\"1317802378430:889699444\",\"msg\":{\"text\":\"OMG!!! did you know that I am doing this for my research? and to
publish?\",\"messageId\":\"id.142193105879078\"},\"type\":\"msg\"},{\"from\":750190551,\"to\":519374614,\"time\":1317802397610,\"msgId
\":null,\"msg\":{\"text\":\"Haha\",\"messageId\":\"id.297776603571539\"},\"type\":\"msg\"},{\"from\":519374614,\"to\":750190551,\"time\":
1317802401753,\"msgId\":\"1317802399301:3970685313\",\"msg\":{\"text\":\"do you think I can use this as evidence? OMG! I have to do the
whole thing again! Thanks!!\",\"messageId\":\"id.211134408952628\"},\"type\":\"msg\"},{\"from\":750190551,\"to\":519374614,\"time\":
1317802404260,\"msgId\":null,\"msg\":{\"text\":\"Cool wife\",\"messageId\":\"id.123882477714520\"},\"type\":\"msg\"},{\"from\":
750190551,\"to\":519374614,\"time\":1317802422545,\"msgId\":null,\"msg\":{\"text\":\"I know I'm a great help\",\"messageId\":\"id.
203594386378094\"},\"type\":\"msg\"}
```


| | | |
|---|---|---|
| 309371218 | 35 31 39 33 37 34 36 31 34 2C 5C 22 74 6F 5C 22 3A 37 35 30 31 39 30 35 35 31 | 519374614,\"to\":750190551 |
| 309371244 | 2C 5C 22 74 69 6D 65 5C 22 3A 31 33 31 37 38 30 31 39 38 30 30 38 35 2C 5C 22 | ,\"time\":1317801980085,\" |
| 309371270 | 6D 73 67 49 64 5C 22 3A 5C 22 31 33 31 37 38 30 31 39 37 37 35 33 39 3A 32 31 | msgId\":\"1317801977539:21 |
| 309371296 | 36 36 34 38 37 32 38 31 5C 22 2C 5C 22 6D 73 67 5C 22 3A 7B 5C 22 74 65 78 74 | 66487281\",\"msg\":{\"text |
| 309371322 | 5C 22 3A 5C 22 64 6C 54 65 6B 72 6B 20 73 6F 20 77 6B 77 6C 20 51 6B 66 64 6B | \":\"dlTekrk so wkwl Qkfdk |
| 309371348 | 77 6E 6A 21 20 54 6B 66 45 6F 52 6B 77 6C 21 21 5C 22 2C 5C 22 6D 65 73 73 61 | wnj! TkfEoRkwl!!\",\"messa |
| 309371374 | 67 65 49 64 5C 22 3A 5C 22 69 64 2E 32 32 37 30 39 30 37 33 30 36 38 32 37 30 | geId\":\"id.22709073068270 |
| 309371400 | 31 5C 22 7D 2C 5C 22 74 79 70 65 5C 22 3A 5C 22 6D 73 67 5C 22 7D 2C 7B 5C 22 | 1\"},\"type\":\"msg\"},{\" |
| 309371426 | 66 72 6F 6D 5C 22 3A 37 35 30 31 39 30 35 35 31 2C 5C 22 74 6F 5C 22 3A 35 31 | from\":750190551,\"to\":51 |
| 309371452 | 39 33 37 34 36 31 34 2C 5C 22 74 69 6D 65 5C 22 3A 31 33 31 37 38 30 32 30 34 | 9374614,\"time\":131780204 |
| 309371478 | 30 31 37 35 2C 5C 22 6D 73 67 49 64 5C 22 3A 6E 75 6C 6C 2C 5C 22 6D 73 67 5C | 0175,\"msgId\":null,\"msg\ |
| 309371504 | 22 3A 7B 5C 22 74 65 78 74 5C 22 3A 5C 22 57 61 74 3F 5C 22 2C 5C 22 6D 65 73 | ":{\"text\":\"Wat?\",\"mes |
| 309371530 | 73 61 67 65 49 64 5C 22 3A 5C 22 69 64 2E 32 36 35 31 33 34 33 37 33 35 32 36 | sageId\":\"id.265134373526 |
| 309371556 | 34 31 33 5C 22 7D 2C 5C 22 74 79 70 65 5C 22 3A 5C 22 6D 73 67 5C 22 7D 2C 7B | 413\"},\"type\":\"msg\"},{ |
| 309371582 | 5C 22 66 72 6F 6D 5C 22 3A 37 35 30 31 39 30 35 35 31 2C 5C 22 74 6F 5C 22 3A | \"from\":750190551,\"to\": |
| 309371608 | 35 31 39 33 37 34 36 31 34 2C 5C 22 74 69 6D 65 5C 22 3A 31 33 31 37 38 30 32 | 519374614,\"time\":1317802 |
| 309371634 | 30 35 31 36 31 30 2C 5C 22 6D 73 67 49 64 5C 22 3A 6E 75 6C 6C 2C 5C 22 6D 73 | 051610,\"msgId\":null,\"ms |

Sel start = 309371325, len = 198; clus = 5356298; log sec = 42850384; phy sec = 43057232