

Forensics Analysis of Residual Artefacts Acquired During Normal and Private Web Browsing Sessions

NORAH ABDULRAHMAN ALOMIRAH

A thesis submitted to the Faculty of Design and Creative Technologies
Auckland University of Technology
In partial fulfilment of the requirements for the degree of
Master of Information Security and Digital Forensics


School of Engineering, Computer and Mathematical Sciences

Auckland, New Zealand

2016

Declaration

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

A handwritten signature in black ink, appearing to read 'Norah', is centered above a horizontal dotted line that spans the width of the signature.

NORAH ABDULRAHMAN ALOMIRAH

(17-September-2016)

Acknowledgements

The thesis was completed at the Faculty of Design and Creative Technologies in the School of Engineering, Computer and Mathematical Sciences at Auckland University of Technology, New Zealand. First and foremost, I thank Allah the Most Gracious and the Most Merciful who gave me the opportunity and supplied me with courage, strengths and blessing in completing this thesis.

I would like to express my deepest gratitude to everyone who has supported me through the past years of my studies in New Zealand. I would like to thank my parents, sisters and brothers for their limitless support from the beginning to the end of writing this thesis.

I would like to thank my thesis supervisor, Dr. Alastair Nisbet, who was supportive since the first day of my thesis. He has provided me with valuable guidance to accomplish the thesis, without him, I would not have been able to achieve this much. Thanks to all my course mates, for all the guidance and assistance when needed during the past two years.

I would like to thank the software vendors for providing the free trial version of Belkasoft and Magnet Internet Evidence Finder. Also I would like to thank the Saudi Arabian Government, the Ministry of Education in Saudi Arabia, and the Saudi Cultural Mission in New Zealand for providing me with the scholarship and their continuous support.

Last but not least, I would like to thank my best friend Mashael Aljohani that was there supporting me from the beginning of this degree sharing brilliant ideas, continually guiding and helping whenever I was lost and stressed out.

Abstract

Privacy as a social and legal issue is a concern for many people. Internet users are concerned about the browsing information that is left on the storage areas such as the hard disk. Web browser vendors have developed a feature to partially address this concern. The private browsing mode is a specialised mode widely supported by major commodity web browsers which aims to protect users' browsing activity when browsing the Internet. The feature does not store private browsing data, such as browsing history, cookies, cache and passwords, on the local hard disk. The private browsing mode is a standard feature among the major browsers, but the implementation of the feature is inconsistent between web browsers. Private browsing mode is often updated by web browser vendors to achieve what it claims which creates a new challenge for digital forensic professionals, especially in the field of web browser forensics. The purpose of this research is to examine the private browsing mode on different operating systems and from different web browser vendors to test the web vendors' claims that private browsing activities are not stored or recorded on the local hard drive of the digital device.

The research experiments were conducted in a laboratory environment following the empirical approach. Windows 10, OS X El Capitan, and Ubuntu 16.04 operating systems were used to install web browsers to carry out the research testing. There was one unique browser on each operating system; for instance, Windows 10 had Internet Explorer as a unique web browser for that operating system (OS), while Firefox and Chrome were used on all three operating systems to test their reliability in leaving no information on private browsing activities. The experimental scenario followed a single scenario on all three devices and then involved examining the local hard disks.

The findings of the research showed that the private browsing feature in Internet Explorer does not offer what it claims, as all the private browsing activity conducted was able to be recovered using Encase forensic software. Opera on Ubuntu had not stored any data related to the private browsing session. Google Chrome and Mozilla Firefox had different results based on the operating system used, as in Windows 10 some of the browsing session was left in the hibernation file, while in Ubuntu 16.04 there were no records of the private browsing activities. The results show that private browsing mode does provide some

privacy to users, especially when using the feature provided by Mozilla Firefox. During the research experiment, it was discovered that there was a lack of effective digital forensic tools in detecting the private browsing artefacts, which raises challenges for digital forensic experts. Therefore, there is an opportunity for future research and development in the area of web browser forensics.

Table of Contents

DECLARATION	III
ACKNOWLEDGEMENTS	IV
ABSTRACT.....	V
TABLE OF CONTENTS.....	VII
LIST OF TABLES.....	X
LIST OF FIGURES	XI
LIST OF ABBREVIATIONS.....	XIII
 CHAPTER 1: INTRODUCTION	 1
1.0. BACKGROUND	1
1.1. MOTIVATIONS	4
1.2. THE RESEARCH APPROACH AND FINDINGS.....	5
1.3. STRUCTURE OF THESIS	7
 CHAPTER 2: RESEARCH LITERATURE REVIEW	 9
2.0 INTRODUCTION	9
2.1 PRIVACY	9
2.2 INTERNET ORIGINS	19
2.3 PRIVATE BROWSING	25
2.4 PRIVATE BROWSING IMPLICATIONS.....	29
2.4.1 BROWSING STORAGE AREAS	30
2.5 DIGITAL FORENSICS	37
2.5.1. DIGITAL FORENSICS MODELS	39
2.5.1.1. COMPUTER FORENSICS INVESTIGATIVE PROCESS (1995)	41
2.5.1.2. DFRWS INVESTIGATIVE MODEL	41
2.6 CONCLUSION	44
 CHAPTER 3: RESEARCH METHODOLOGY	 45
3.0. INTRODUCTION	45
3.1. REVIEW OF SIMILAR RESEARCH.....	45
3.2. RESEARCH DESIGN	49
3.2.1. RESEARCH QUESTION	51
3.2.2. RESEARCH PHASES	52
3.3. DATA REQUIREMENTS	53
3.3.1 TESTING PROCESS.....	53
3.3.2 TESTING SCENARIO.....	55
3.3.3 DATA COLLECTION.....	56
3.4. WEB BROWSING ENVIRONMENT SETUP & TESTING SCENARIO	56
3.5. CONCLUSION	57

CHAPTER 4: RESEARCH FINDINGS AND ANALYSIS	58
4.0. INTRODUCTION	58
4.1. VARIATION ENCOUNTERED	58
4.1.1. TESTING PROCESS	59
4.1.2. TESTING SCENARIO & DATA COLLECTION	59
4.2. FORENSICS INVESTIGATION ENVIROMENT SETUP	60
4.3. DIGITAL FORENSICS	61
4.3.1. EVALUATION AND ASSESSMENT	61
4.3.2. ACQUISITION OF DIGITAL EVIDENCE	61
4.3.3. SURVEY OF THE DIGITAL SCENE	63
4.3.4. DIGITAL EVIDENCE EXAMINATION	64
4.3.5. LOCATING WINDOWS 10 BROWSER ARTEFACTS.....	64
4.3.6. RESULTS OF ANALYSING THE WINDOWS 10 OPERATING SYSTEM	66
4.3.7. COMPARISON OF COMMON WEB BROWSERS IN TWO MODES ON WINDOWS OS	73
4.3.8. LOCATING MAC OS BROWSER ARTEFACTS	74
4.3.9. RESULTS OF ANALYSING THE MAC OS OPERATING SYSTEM.....	76
4.3.10. COMPARISON OF COMMON WEB BROWSERS IN TWO MODES ON MAC OS X	80
4.3.11. LOCATING UBUNTU 16 OPERATING SYSTEM BROWSER ARTEFACTS	81
4.3.12. RESULTS OF ANALYSING THE UBUNTU 16 OPERATING SYSTEM	82
4.3.13. COMPARISON OF COMMON WEB BROWSERS IN TWO MODES ON UBUNTU 16 OS	85
4.4. CONCLUSION	86
 CHAPTER 5: RESEARCH DISCUSSION	 87
5.0. INTRODUCTION	87
5.1. ANSWERING THE RESEARCH QUESTIONS	87
5.1.1. ANSWERS TO SUB-QUESTIONS	87
5.1.1. THE RESEARCH QUESTION.....	89
5.2. DISCUSSION	90
5.2.1. DISCUSSION OF THE CASE SCENARIO ENVIRONMENT	90
5.2.2. DISCUSSION ON DATA ACQUISITION AND ANALYSIS	92
5.3. RECOMMENDATION FOR WEB BROWSER FORENSICS.....	93
5.4. CONCLUSION	94
 CHAPTER 6: RESEARCH CONCLUSION	 96
6.0. INTRODUCTION	96
6.1. SUMMARY OF RESEARCH.....	96
6.2. LIMITATIONS OF RESEARCH.....	98
6.3. FUTURE RESEARCH	99
 REFERENCES.....	 101
APPENDICES	106

APPENDIX 1 – NORMAL BROWSING MODE TESTING SCENARIO ON THREE OPERATING SYSTEMS.....	106
APPENDIX 2 – PRIVATE BROWSING MODE TESTING SCENARIO ON THREE OPERATING SYSTEMS.....	111
APPENDIX 3 – HASHES OF THE FORENSICS IMAGES.....	116
APPENDIX 4 – ENCASE GENERATED FORENSIC REPORT.....	117

List of Tables

Table 2. 1: Stored data during InPrivate browsing (Smulikowski, 2009)	30
Table 2. 2: Digital forensics investigation frameworks	40
Table 3. 1: Summary of the Six Research Studies	50
Table 3. 2: Testing Scenario	55
Table 3. 3: Experiment URL and keywords	56
Table 4. 1: Hardware and Software Specifications	60
Table 4. 2: Default locations of the three common web browsers in Windows 10	65
Table 4. 3: Internet Explorer Privacy Mode Evidence	69
Table 4. 4: Mozilla Firefox Privacy Mode Evidence	71
Table 4. 5: Google Chrome Privacy Mode Evidence	73
Table 4. 6: Default locations of the three common web browsers in Mac OS X	75
Table 4. 7: Default locations of the three common web browsers in Ubuntu 16	81
Table 5. 1: Sub-Question 1 and Answer	88
Table 5. 2: Sub-Question 2 and Answer	88
Table 5. 3: Sub-Question 3 and Answer	89

List of Figures

Figure 2. 1: Consumers' Concern over Privacy (TRUSTe).....	15
Figure 2. 2: The Internet Sketch Plan, 1969 (Schneider et.al, p.7).....	20
Figure 2. 3: Number of Websites by Year Since 2000 (Internet Live Stats, 2014).....	24
Figure 2. 4: Indications of the Private Browsing Mode.....	29
Figure 2. 5: Web Browser Cache Functionality (Parsons, 2015)	32
Figure 2. 6: Firefox Browsing History Table.....	33
Figure 2. 7: Hibernation File viewed in Encase Software (hyberfil.sys) (Bunting & Wei, 2006, p.381)	35
Figure 2. 8: Viewing Partitions on the Hard Disk (Vacca & Rudolph, 2010).....	36
Figure 2. 9: Brief History of Computer Forensics (Hayes, 2014)	38
Figure 2. 10: Earliest Forensics Examination Framework.....	41
Figure 2. 11: Digital Forensics Research Working Group (DFRWS) Model (Yusoff et al, 2011)	42
Figure 2. 12: Validating Data (Daniel, 2011)	43
Figure 3. 1: Research Phases	53
Figure 3. 2: Research Testing Process	54
Figure 3. 3: Lab Environment Web Browsing Process.....	57
Figure 4. 1: Encase Acquisition	61
Figure 4. 2: Encase Acquisition Options	62
Figure 4. 3: Acquisition & Verification Process of Seized Hard Disk	62
Figure 4. 4: Evidence Extracted using Encase Forensic Tool	64
Figure 4. 5: WebCacheV01.dat Database analysis	67
Figure 4. 6: Google Chrome Cache Extracted from Encase Software	68
Figure 4. 7: Email Sent by Suspect Recovered in Encase Software.....	70
Figure 4. 8: Email Recovered Viewed in Encase	72
Figure 4. 9: Texts from the Email Sent by the Suspect Viewed in Encase Software	72
Figure 4. 10: Comparison of Web Browsers Artefacts on Windows 10 OS	74
Figure 4. 11: Safari Cache Viewed in Encase Software	77
Figure 4. 12: Mozilla Firefox Cookies.sqlite Database File Viewed in SqliteBrowser..	78
Figure 4. 13: Mozilla Firefox Cached Image Viewed in IrfanView	78

Figure 4. 14: Suspect's Email Viewed in Encase Software.....	79
Figure 4. 15: Comparison of Web Browsers Artefacts on Mac OS X.....	81
Figure 4. 16: Opera History Database Viewed in SQL Viewer.....	83
Figure 4. 17: Opera Cookies Database Viewed in SQL Viewer.....	84
Figure 4. 18: Comparison of Web Browsers Artefacts on Ubuntu OS.....	86

List of Abbreviations

• ACR	Automatic Crash Restore
• ARPNET	Advanced Research Projects Agency Network
• BBN	Bolt, Beranek, and Newman
• CBK	Common Body of Language
• DARPA	Defence Advanced Research Projects Agency
• DFRWS	Digital Forensic Research Workshop
• DNS	Domain Name System
• DOM	Document Object Model Storage
• ESD	Electrostatic Discharge
• ESE	Extensible Storage Engine
• FAT	File Allocation Tables
• FBI	Federal Bureau of Investigation
• FTC	Federal Trade Commission
• GIF	Graphic Interchange Format
• HCI	Human-Computer Interaction
• HTML	Hypertext Markup Language
• HTTP	Hypertext Transfer Protocol
• IE	Internet Explorer
• IEF	Magnet Internet Evidence Finder forensic tool
• IMP	Interface Message Processors
• IP	Internet Protocol Address
• MD5	Message Digest 5
• NIST	National Institute of Standards and Technology
• NSCA	National Center for Supercomputing Applications
• OS	Operating System
• P2P	Peer-to-peer
• RAM	Random Access Memory
• SHA-1	Secure Hash Algorithm version 1
• SRI	Stanford Research Institute

- UCLA University of California, Los Angeles
- UCSB University of California, Santa Barbara
- UIUC University of Illinois in Urbana-Champaign
- URLs Universal Resource Locators
- USB Universal Serial Bus
- VM Virtual Machine
- WWW World Wide Web

Chapter 1: Introduction

1.0. BACKGROUND

The Internet is a necessary tool for everyday tasks involved in human life, as it is being used to connect others from different destinations for communicating, sharing information and many other activities. Web browsers are programs that are installed on operating systems to allow users around the globe to access, view, and communicate with websites, other users and other files stored on web servers. In addition, they are able to record and retain the browsing activity of users' sessions. The information includes storing files, storing images, URLs visited, search terms, emails, cookies and other types of information. The information related to users' browsing activities is stored on the local hard disk of the computer and can be accessed and retrieved easily by any user who has access to the same machine (Said, Mutawa, Awadhi, & Guimaraes, 2011).

As users are becoming more concerned about their browsing activity while surfing the Internet, web browser companies have developed a feature that aims to leave no traces of the browsing activity relating to the private browsing session (Satvat, Forshaw, Hao, & Toreini, 2014). The feature is known as private browsing on common web browsers, which enables end consumers to have better control over their privacy. The feature has two main goals to achieve. The first and foremost goal is to leave no trace of the browsing session on the user's device. When a user visits a website there should not be any information related to that website in the browser's history, cache, or cookies on the local computer. More precisely, it aims to secure the private browsing session against a local attacker that takes control of the digital device at a specific time, as there should not be any information related to the private browsing session prior to that time. Secondly, it aims to secure against web attackers, which allows end consumers to hide their identity when visiting some websites (Aggarwal, Bursztein, Jackson, & Boneh, 2010).

The feature was firstly introduced in 2005, in Safari browsers, and was then added to other Internet browsers such as Internet Explorer, Google Chrome, and Mozilla Firefox. Not all web browsers providing the private browsing feature are consistent in the

type of privacy provided, as some browsers protect the user against local attackers only and others against web attackers, while yet another browser protects against both. For instance, Google Chrome and Mozilla Firefox provide privacy against a local attacker and some protection against a web attacker, whereas Safari provides privacy against local attackers only. Furthermore, there are inconsistencies within a single browser.

A survey conducted by Aggarwal et al. (2010) showed that 19% of Internet users located in the United State of America (USA) are using the private browsing feature to search for information, online shopping, browsing adult sites, looking up people and other information not specified. Another recent survey was conducted by Gao, Yang, Fu, Lindqvist and Wang (2014) on 200 participants across the USA. 136 participants in the survey knew about the private browsing feature and their purpose of using the feature was to leave no traces of the browsing session such as the history and cookies. In addition, the participants have used the private browsing feature to protect their personal information, browsing porn or dating sites, online shopping, entertainment online while being on work devices, for curiosity and other reasons that have not been identified.

Technologically-minded offenders use the technology illegally to profit by using users' personal information or data for their own purposes. Offenders currently are using the technology in various ways and becoming more sophisticated and rigorous in avoiding being detected to achieve their crime (Zainudin, Merabti, & Llwellyn-Jones, 2011). As the private browsing feature is being more recognised and used among consumers, there might be higher chance of misuse of the feature, which creates a new issue for digital forensic professionals, as users are able to hide their data when using the private browsing feature.

Private browsing mode is often updated by web browser vendors to achieve what it claims which creates a new challenge for digital forensic professionals, especially in the field of web browser forensics. In addition, the feature is being added to different digital devices such as smartphones and tablets, and digital forensic examiners do not routinely search for the private browsing artefacts. Thus, digital forensic examiners may miss potential evidence that might bring value to a digital forensics case. To assist forensic examiners in avoiding this scenario, this research aims to provide guidance to digital forensic examiners to be able to identify the private browsing artefacts. Therefore, the proposed main research question in regard to the topic is:

Does privacy mode allow users to browse the Internet without leaving any evidence behind?

1.1. MOTIVATIONS

The background of this is briefly discussed in section 1.0 in order to understand the importance of the chosen research area. This section discusses the motivation to start investigating the private browsing feature on different operating systems and web browsers. The research has been motivated after reading previous articles and research published in the area of private browsing.

Digital forensic investigators need to have knowledge of where the browsers store the different artefacts, how long they are kept on the storage medium, and the proper way to examine and extract them in a digital forensics manner. There are an increasing number of criminal and civil cases involving the use of web browsers and Internet activity. Web browsers on different operating systems are often updated and there might be some difference in the area where the browsing artefacts are stored between versions of the same browser or different browsers. The ability to investigate Internet users' activity is often critical, whether involved in high-profile criminal cases or minor cases, as it could reveal evidence that could be presented in law enforcement cases. The information related to a user's browsing activity could reveal offenses ranging from violation of an organisation's policy performed by employees to more serious offences such as child pornography or hacking systems. Thus, retrieving any of the browsing activity such as the browser history, cookies, cache, downloaded files and search terms might assist the forensic investigators to learn what the suspect's attention to a crime to reveal potential evidence.

The other motivation to start the research was to investigate if information specifically related to users' private browsing sessions would be left on the local hard disk of the target machine. The researchers Said et al. (2011) have found many of the private browsing activities conducted on Windows XP operating system with Internet Explorer, Mozilla Firefox, Google Chrome web browsers installed. The information related to the session was recovered from different locations on the local hard drive and the physical memory. Several research studies have been conducted to test the private browsing mode, although the testing was performed on old versions of the operating system and web browsers. The results of these are presented and reviewed in section 3.1.

In summary, the motivation of this research is to be able to test the private browsing feature across multiple operating systems and web browsers in order to assist

digital forensic professionals to understand the level of secrecy provided by each web browser.

1.2. THE RESEARCH APPROACH AND FINDINGS

In order to answer the research's main question proposed for this thesis, it is necessary to ensure that the experimental scenario is accomplished following appropriate and effective methodology, as presented in Chapter 3. The selected approach was chosen after reviewing similar research in the area of private browsing. Associated with the main research question, there were three sub-questions developed that were relevant to the research experiment and problem area.

The proposed research was designed based on an empirical approach, which consists of five research phases. Phase 1 of the research was conducted by preparing and setting up the devices and identifying their features, hardware and software characteristics. After preparing the workstations, phase 2 begins with performing the testing scenario, which consists of a single scenario to be followed. The testing scenario depicts as closely as possible a real world event. In phase 3, using the computer forensics guidance model, an acquisition of the seized digital device will be applied. Phase 4 examines and extracts the relevant information generated in phase 2. The outcomes of phase 3 and phase 4 are reflected in phase 5 as a recommendation of the best practices in process or procedure to be followed in web browser forensics.

The research has proved that there are private browsing artefacts found on the local hard disk depending on the web browser and operating system utilised. The experimental research found that private browsing activity performed on three web browsers on the Windows operating system are kept in different location on the local hard disk of the target machine. The majority of recovered artefacts were found in unallocated space on the local hard disk, hibernation files or other deleted files.

Mac OS X had some of the information related to the private browsing activity conducted by the users, such as emails. The Ubuntu operating system had no information related to the private browsing activity conducted on Opera, Google Chrome, and Mozilla Firefox.

It was discovered from the experimental scenario that private browsing artefacts on local hard disks are not always recoverable. In addition, there were not many digital forensics tools that were capable of recovering the artefacts left on the local hard disk.

The only tool that was able to recover the private browsing artefacts was Encase Forensic Software, developed by Guidance Software.

1.3. STRUCTURE OF THESIS

The structure of this thesis is organised into six chapters. They are: Chapter 1, Introduction; Chapter 2, Research Literature Review; Chapter 3, Research Methodology; Chapter 4, Research Findings and Analysis; Chapter 5, Research Discussion; and Chapter 6, Research Conclusion.

Chapter 1 is an introductory section where it presents the background area of the research, the importance of the research topic, the motivation for this research, the approaches followed in conducting the research and a summary of the findings of the experiment.

Chapter 2 presents the literature review of this research to gain the knowledge of private browsing and recent studies in the area of web browser forensics. The areas reviewed in Chapter 2 include: privacy and value of it among Internet users, the history of Internet, private browsing, the implications of private browsing, the browsing storage areas, and digital forensics.

Chapter 3 establishes the research methodology that will be followed for the thesis project. Six similar approaches to the chosen research area were studied and reviewed in order to form a research method that is appropriate for the proposed project. The chapter identifies the main research question, sub-question, and data requirements.

Chapter 4 reports the research findings for each phase of the research. Any changes made to the testing phase are acknowledged and explained in the beginning of Chapter 4. The second section to Chapter 4 is specifying the digital forensics workstation and tools used to examine the results. The findings, examination and analysis of the data collection, along with a comparative analysis between the browsers are presented in the third section.

Chapter 5 is the research discussion, which presents the key finding results from Chapter 4. This chapter answers the main research question and sub-question based on the findings provided in Chapter 4. The chapter delivers a critical reflection on the thesis discussing the strength, weakness and limitations. The chapter concludes with recommendations related to web browser forensics.

Chapter 6 is the conclusion based on the entire research. It summarises the research findings and the approach being followed for the experiment scenario. The chapter presents the limitations of the proposed research approach. The chapter is

concluded with a discussion of the possible further research opportunities to develop in the area of web browser forensics.

The appendices are provided at the end of the thesis as supplementary information. The research appendices include the controlled data, forensics image acquisitions and verifications, generated forensic reports from Encase, and additional findings from the conducted experiments.

Chapter 2: Research Literature Review

2.0 INTRODUCTION

The Internet is used by many people on a daily basis utilising web browsers to perform online activities such as global communication, shopping, social networking, exchanging emails and conducting business. The browser activities conducted by users' are logged and stored by web browsers which include caching files, URL's visited, search terms and cookies. The Internet activities are valuable for digital forensic investigators when conducting an examination on a user's local disk. This is especially true, in cases where questionable websites are visited or criminal acts were performed through the Internet. There are two main area of focus in the literature review, the first is privacy, which includes a discussion of the value and importance to individuals and specifically Internet privacy. The second area of focus is the digital forensics investigation processes related to this subject. The objective of this chapter is to discuss the Internet browsing activities in public and private browsing modes in common web browsers. With a brief introduction to the Internet's history from its academic and military invention to its present widespread use among users.

The review consists of six sections. Section 2.1 discusses the definition of privacy, individuals' concern towards privacy and how they value their privacy when browsing on the Internet. The following, section 2.2 introduces the Internet with a brief history of its launch and how Internet users are sharing personal information on different websites and applications. Section 2.3 and section 2.4 introduces private browsing mode which is a feature on major web browsers which aims to prevent users' activities from being locally stored on the computer. In addition to the areas where browsing activities are maintained on the digital device. The final section reviews the digital forensics history, process, and the challenges that forensic experts face during an investigation.

2.1 PRIVACY

Technological developments are increasingly being involved in societies, assisting people in performing a variety of human activities, such as working, shopping and accessing information. Today, right across the globe, an everyday aspect for many

people's lives is human-computer interaction (HCI). Digital devices have provided a positive effect on humans' lives, yet the advantage of digital devices has raised a social and legal issue for many individuals and organisations (Acquisti, Gritzalis, Lambrinoudakis, & Vimercati, 2007). Privacy as a social and legal issue is a concern for many people while some people remain unconcerned about their privacy as they may feel that they have nothing to be hidden from others (Gunnarsson & Ekberg, 2003; Solove, 2011; Friedewald & Pohoryles, 2016). However, hiding information from others is not what privacy is always concerned with. The concept of privacy is to give people the right to decide what personal information is public and what is private.

Since the 19th century, concerns regarding protecting individuals' privacy against the technological advances is not a new concern (Poole, 2005). It has been discussed many times from a broad range of perspectives such as lawyers, ethicists, sociologists, communication professionals, computer scientists and more. Privacy's definition, value, and approach differ across nations, cultures, religions, communities and individuals (Gellman & Dixon, 2011; Allmer, 2015). When privacy is discussed, frequently there are disagreements on its definition, purpose, and best practices. Thus there is no single standard or globally agreed definition of privacy (Trepte & Reinecke, 2011).

The earliest, simplest and classic definition of privacy for many was coined by Warren & Brandies (1980); who stated that individuals have the right to be let alone, which means that each individual has the right of being free from others' observation or distribution. Anderson (2008) defines the concept of privacy as follows: "Privacy is the ability and/or right to protect your personal secrets; it extends the ability and/or right to prevent invasions of your personal space" (p. 13-14). Several scholars consider privacy as the degree to which clients can manage their own private information (Bennett, 1967; Jourard 1966, Westin 1967; Trepte & Reinecke, 2011). While others view the notion of privacy as the case of accessing someone's mind and body (Altman, 1975; Leino-Kilpi et al. 2001). On the other hand Burgoon, 1982; Parrot et al 1989; Trepte & Reinecke, (2011) defined privacy as the involvement of three aspects which consider physical, psychological, social, and information aspects. A further privacy definition by Maw (2015) states that "privacy secures information from all individuals except those who are authorised to view it".

Regardless of the diverse conceptualisations, there are two common approaches to the discussion and definition of privacy. The first approach of defining privacy is from the legal and normative perspectives. The approach's concern is mainly on answering questions such as "What is the nature of privacy?" and "How much privacy should a user have?" (Trepte & Reinecke 2011). The other discussion has considered privacy as a social and behavioural conception. The latter approach was concentrated on the way individual users and/or groups of individual users perceive, preserve, and transfer their personal information in the different social environments.

As stated by Trepte & Reinecke (2011), there are two forms of privacy protection for each individual client that are either passive or active. The former protection comprises dependence on external components such as the government or other independent users. Generally the passive protection is beyond the management of one individual user or organisation. Two requirements are required in the passive protection which are collective actions and institutional support. Cultural and socio-political norms are highly sensitive in this type of protection. In addition, a significant challenge is posed to the passive protection by the online communication environment.

On the other hand Trepte & Reinecke (2011) explained active protection which depends on individual users actively implementing the different protection schemes. For instance in the physical world, an individual could use walls to enforce soundproofing; a door to prevent any strangers entering the individual private space or even a sign that displays the desire of privacy. Concerning the digital and virtual world, there are various protective strategies that users can implement to secure their online privacy activities. The strategies could be by installing firewalls, virus protection software, and importantly using encryption when transmitting sensitive data. The process of securing individuals' privacy could be primarily considered as boundary management over diverse controlling schemes to individuals' personal space and information. Individuals themselves are required to detect the threats that could expose their own personal privacy over the network and then evaluate the threat weights alongside their confidentiality preferences and select and adopt the protection strategy that is most suitable.

However, other authors stated that personal information has to be identified in order for privacy to be defined (Frackman, Martin & Ray, 2002). Personally identifiable information (PII), which is shortened to personal information, is not tied to a single

definition (Frackman, Martin & Ray, 2002). The Federal Trade Commission (FTC) defines the PII as information that could be linked to specific individuals that includes but is not limited to information such as the individual's name, post address, contact number, fingerprint, passport number, email address and so on. Data linked from digital devices that could identify an individual or a digital device via a unique identifier could be considered as PII, depending on a person's view. Frackman, Martin & Ray (2002) have stated that the information obtained from the Internet is not directly identified as personal information as in the last years organisations are specialising in collecting and mining clickstream data.

Clickstream data is information about a digital device, not the user. The data shows the path taken from when the computer enters the network until it arrives at its destination or site along with further details such as the amount of time the user spent at a particular website and when the user left the website. However, clickstream data does not insure that the data collected is from a specific individual using the digital device, as multiple users might have used the same digital device. Therefore, clickstream data is not able to distinguish between users (Frackman, Martin & Ray, 2002).

Companies and stores often store information about their clients on their systems for a variety of reasons, most commonly for marketing and sales purposes to market clients directly or to indicate users' preferences to the product they often purchase. Corporations that clients have business with are constantly gathering a considerable amount of clients' data on a regular basis (Cherry, 2013). Businesses collect personal information or even purchase people's information from third parties to enhance their business and meet customers' needs (Ontario Government, 2015). According to Cherry (2013), companies can collect as much information about their customers as they like, and there are no laws or regulations that can prevent this. As a result, this creates the risk of personal information being stolen by other users.

In spite of this, personal information of users is not only exposed by companies. Users by themselves share their information online on different social media platforms such as Facebook and Twitter. Information that is posted on social media networks may not only be viewed by the user's family and friends. Social media networks are generally publicly open by default, which means that anyone that opens a particular social media platform could view any user's posts. Therefore, attackers and identity thieves are finding

it easier to collect information in order to break into users' accounts and to gather their entire identity (Cherry, 2013).

Privacy has been a concern for human beings from time long before the Internet existed. However, in the digital era, societies are also concerned about digital privacy and the protection of their personal information as information is transmitted and stored by digital devices. According to Harrah & McGregor (2001), a principal concern of the information age is digital privacy. One of the key factors to any system architecture is privacy, and it is a vital requirement for personalisation systems that are mainly focused on storing users' profiles. Data holders are responsible for ensuring the privacy and confidentiality of the data when it is released (Sadhya & Verma, 2015). Accessible information on the Internet enhances the ability of organisations and cybercriminals that may later compromise citizens' personal security. Users are concerned with the amount of personal information that they have to share with others over the network. In addition to the risks associated with sharing too much personal information which raise questions of how to protect their personal information (Cherry, 2013).

In the digital era, information that users transmit over the network are destined to be stored on digital devices even if the user does not know that his/her information is being stored, such as when a user visits a website over a public or private network. When a user uses a local library's Internet with a desktop or laptop computer or even a cell phone, information about the user's session is stored in some form or another (Cherry, 2013).

Digital devices are becoming more and more pervasive in this manner, and it is critical to understand how privacy can be compromised for the sake of advancement (Gunnarsson & Ekberg, 2003). The huge amounts of data that are used by enhanced technologies are becoming exposed to different types of threats and attacks from opponents and dangerous entities. This is particularly true of data that includes individuals' personal information which is being attacked by different types of threats. This is a problem because a failure in security mechanisms of the system could lead to critical problems for each individual in that system, such as identity theft (Gunnarsson & Ekberg, 2003). Privacy is not a factor that affects a person by themselves; it affects everyone, and each user has the right to share his/her opinion on what is acceptable or not acceptable (Gellman & Dixon, 2011). One of the biggest threats to customers is

identity theft, as the information of customers' credit cards or even their entire identity details could be stored on the company's database (Miller & Cross, 2012).

The issue of privacy on the Internet is a major concern not only for privacy advocates, who are individuals or groups from society with an aim of limiting the reach of surveillance on individuals and who view the privacy of users over the network as a moral concern, but also for individual users on the Internet. It is also a concern and a prime issue for any organisation that requires the use of the Internet for their business to function. Currently, this means that every organisation is affected to some extent (Frackman, Martin & Ray, 2002).

Information can be collected either with the permission of the individual or without his/her permission, as in the clickstream data collection (Frackman, Martin & Ray, 2002). Information on the Internet is collected in a variety of ways. One of the methods of gathering data is when a user enters a website and registers his/her information. The other method is to passively obtain information about the user via the digital device or the browser he/she is using. Clickstream data is information gathered by monitoring IP addresses of digital devices connected over the network. Each device connected to the Internet is identified with a unique identifier referred to as the Internet Protocol (IP) address. The aim of the IP address is to uniquely identify a single computer or any digital device such as routers that contains a network adapter to communicate with other devices connected to the Internet. The third method to obtain information is by Web bugs, which are a form of Graphic Interchange Format (GIFs) and referred to as clear GIFs or invisible GIFs. In addition, cookies that reside on the user's hard drive gather and store information about the user's browser information such as the IP address, type of browser being used, and the operating system of the digital device (Frackman, Martin & Ray, 2002). Cookies and Web bugs are data that is obtained through monitoring the IP addresses of digital devices and is also known as clickstream. An increasingly common method of collecting information of individuals is through the use of a tracking software. Several companies provide free or low-cost software made to assist users with their browsing activities. Some tracking software may track the user's movements over the Internet and send the information back to the company that issued the program (Frackman, Martin & Ray, 2002).

Several studies from the 20th century have revealed that personal privacy was one of the main barriers to Internet users especially when making purchases. A recent survey on data privacy by The TRUSTe 2015 Consumer Confidence Privacy Index concluded that 92% of American consumers on the Internet are concerned about their Internet privacy to some extent. Figure 2.1 illustrates the respondents' concerns regarding privacy over the network.

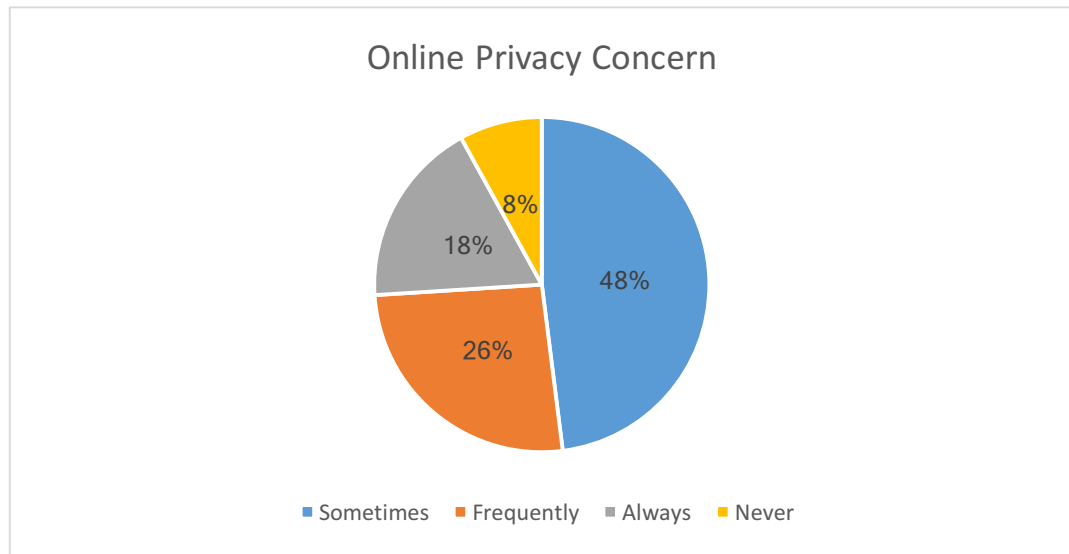


Figure 2. 1: Consumers' Concern over Privacy (TRUSTe, 2015)

This result was the same as in their previous survey in January 2014, while in January 2013, 89% were concerned. An older survey conducted in 2000 by Forrester Research reported that nearly two-thirds of the respondents stated that they were concerned about their privacy over the network while 12% of consumers would pay third companies to improve the protection of their online activities. Odyssey, a company based in San Francisco conducted a survey on online privacy and identified that 92% of Internet users do not trust organisations for their information to be preserved and to remain confidential to others (Frackman, Martin & Ray, 2002). There is a remarkable consistency with other surveys in the conclusions with privacy being a concern for consumers. There is common agreement that the Internet is a significant technology for both individuals' and organisations' online activities. However, online privacy is a vital matter, as users both individuals and businesses are involved more and more in sharing their personal information over the Internet (Frackman, Martin & Ray, 2002).

Online consumers often believe and expect that each consumer has online privacy when posting to or conversing with initiatives, and has, to some extent, legal protection of the information that users' share. Cyberspace crimes regarding privacy are generally similar to the crimes committed in physical life, which means illegal acts such as trespassing and solicitation are considered crimes whether online or offline. However, prosecution in cyberspace is considered complicated due to the different legislation in each country. As Trepte & Reinecke (2011) state, the beliefs of consumers concerning online privacy is in agreement with certain entities, domains and forms under the US law, yet Internet privacy advocates have stated that the legal restrictions are narrowed to specific domains.

Laws differ from one country to another. For instance the European Union and countries such as New Zealand and Canada have defined the privacy rights in their law more than the United States has defined privacy rights (Payton & Claypoole, 2014). On the other hand, Gunnarsson & Ekberg (2003) state that other nations have fewer protections regarding privacy. Furthermore, sorting which law or regulation to apply when privacy is breached has been an issue for legislators and courts. The court system is not able to control the breaches on a global network and to have a system that will operate on the global network will take a decade to develop (Gunnarsson & Ekberg, 2003). Thus, consumers need to be educated about the dangers of their online activities and, rather than relying on the law itself, they need to be notified that their online activities are leaving electronic footprints, and so act accordingly (Trepte & Reinecke, 2011).

For consumers, personal information can be transmitted or stored on a server in a different country from the individual who has provided it. Individuals should understand that electronic footprints are left on any digital device they use over a network (Gunnarsson & Ekberg, 2003). Personal information includes not the only data that individuals should secure but other information such as metadata, which is defined as data about data. Metadata information includes the time and date on which the data was created, or even the location where the data was created, or who was the author of that data. Hackers and illegal users can use metadata information in order to identify a specific individual in order to perform illegal activities such as identity theft or stalking (Cox, Mulder & Tadic, 2006).

Further efforts need to be made in order to assist online consumers to be more aware of their personal privacy over the Internet and to help them remain anonymous in certain circumstances. Online users are often able to protect and safeguard their information during their online activities with technical measures. For instance, users are able to disable cookies on web browsers to prevent cookies from gathering information and enable cookies on websites that a user trusts in order to maintain data privacy. In addition, individuals can install programs developed to remove spyware software from the computer's hard drive. Peer-to-peer (P2P) networks and anonymous Web surfing are two options that allow users to connect online to another user directly without reaching centralised servers (Gunnarsson & Ekberg, 2003).

There have been debates on the concept of whether users on the Internet should be anonymous or not with strong points of view from both sides. There are two anonymity types; complete anonymity and pseudonymity (Gunnarsson & Ekberg, 2003). Complete anonymity is when a post is submitted online and it is impossible to identify the user who wrote it. Pseudonymity is when a user takes a nickname or a pseudonym that defines him as an online user, but this nickname does not link the user to a specific individual.

However, being anonymous in cyberspace is complicated; consumers online can be easily identified through different methods such as by the Ethernet network cards or the microprocessors, all of which have unique serial numbers. Internet users could be traced through cookies, and an email address could be linked to a specific individual. SafeWeb, a software company, has developed software that aims to give users complete online privacy while surfing the Web. Yet, the software reportedly does not grant the privacy it promises, and instead has apparently revealed users' confidential information (Gunnarsson & Ekberg, 2003). Thus, privacy does not always mean that an individual is granted anonymity, which means that individuals should be cautious when sharing their personal information during their online activities. As McNealy, the founder of Sun Microsystems, stated, the privacy of consumers has been a red herring issue, and there is in fact zero privacy for any individual (Cady & McGregor, 2001).

Privacy violation occurs when an individual's sensitive information is disclosed to an adversary. Violations towards privacy are divided into two fundamental types, namely targeted attacks and data harvesting. Targeted attacks occur when an offender searches for information about another online user in order to learn more about them.

This is referred to as stalking. If the same situation happened concerning a company's data instead of an individual person's, then this is referred to as industrial espionage. Finally, if the data concerns an entire country, it is called spying. The alternatives to stalking, industrial espionage and spying are illegal acts for which offenders can be sent to prison. Users are able to prevent these breaches from occurring by applying security measures on their computers. However, attackers are often able to bypass a system if it did not apply and update its security measures if the attacker has the necessary resources and to skirt around security measures (Schneier, 2011).

Data harvesting is an attack that involves cross-correlation of data, which consists of searching for an individual or a group of particular characteristics. For instance, the offender might search for individuals who subscribe to a specific magazine in a certain geographic area and who are participants in a particular political party. The data harvesting technique of finding information about a specific individual by cross-correlating is not a new technique, but computerised information has provided an automated process of searching for a specific target. However, data harvesting is valuable because it can be computerised but if the computerised data was protected, an offender may not even know where to look for information. However, having computerised data that is completely protected is simply impossible (Schneier, 2011).

One of the fastest-growing online crimes in the United States and other countries such as New Zealand is identity theft (Acquisti et al, 2007). Identity theft occurs when someone pretends to be someone they are not by using another individual's identity such as the individual's name, bank account details or even the individual's credit card in order to commit crimes. As a consequence, if the identity theft performed is a criminal act in the name of the legitimate user this may damage the individual's name and reputation. In the United States alone, there are approximately 750,000 cases each year involving identity theft. There are various ways to steal someone's identity, but it often occurs by inside sources stealing the data and then selling it (Gunnarsson & Ekberg, 2003; Miller & Cross, 2012; Salinger, 2013).

This constant threat in cyberspace not only consists of identity theft, but also involves other electronic crimes. Electronic crimes, shortened as (e-crimes), are diverse and involve, but are not limited to, the following: breaches, hacking into systems, installing malicious software, cyber stalking, pornography, online frauds, scams, unsolicited bulk

emails, denial of service attacks and other illegal acts. The New Zealand Police consider ‘electronic crimes’ to involve all crimes where information and technology is either used as a tool, storage, or the target of an offence (New Zealand Police, 2015). The Internet as a medium has provided advantages to society but criminals in particular could raise a threat specifically towards individuals’ privacy with information technology being involved in various areas of economic and social life. The threats that occur over the Internet, known as cyber threats, are in many respects similar to the threats occurring in the offline world. Cybercrime, which many computer crimes fall under, is defined as any illegal activity that occurs through the use of a digital device connected to the virtual society of the Internet (New Zealand Government, 2015). For instance, cyber stalking, which is similar to offline stalking, is an international threat that emerged a decade ago and is a continually growing threat across nations, which aims to threaten and harass individuals, groups or even organisations through the use of communication technologies in cyberspace (New Zealand Government, 2015).

2.2 INTERNET ORIGINS

The Internet as a worldwide network did not generally emerge as it is today, nor did it establish automatically through early communications. The history and the origins of the Internet are difficult to place to a specific point (Schwartz & Kleinrock, 2010), since the roots of the Internet can be placed back to the era of the most primitive communication technologies. In primitive terms, an internetwork can be traced to early stages of logic and mathematics or yet to the occurrence of language. The Internet consists of components that form this substantial infrastructure which are technical and social forerunner factors that occurred from history to the present.

Robert (2011) states that the beginnings of the Internet could be dated back to “Sputnik”, the satellite that was for the first time launched into space by the Soviet Union in October, 1957. The invention of Sputnik occurred during a strained Cold War between the United States of America and the Soviet Union (Oppedisano, 2011). The United States were eager to invent, develop, attain, and maintain a scientific technology that would overcome the Soviet Union invention. In the late 1950s and early 1960s, the United States Department of Defence Advanced Research Projects Agency (DARPA) initiated the networks that were the forerunner to the Internet (Horner, 1997). Their aim was to

implement an efficient computer network that was able to resist tragedy such as a nuclear attack.

The first time users began referring to this network as ‘Internet’ was in 1982 (Selfe & Hawisher, 2004; Liska, 2014). The word ‘Internet’ originates from the phrase “internetworking”. The Internet, often known as “the Net” is a global system of digital devices on a network of numerous independent networks which allows users with the proper permission to send and receive information from any computer (Shah, 2009). The Internet in the early days was very small compared to what it is now (Oppedisano, 2011; Liska, 2014).

In 1969, the University of California, Los Angeles (UCLA) enabled the use of packet switching on their computer devices to communicate with other computers at a variety of university sites, for example the University of Utah and other universities in California. The communication established between these computers were the initial nodes which then expanded to connect other networks of academic organisations and government authorities in the Advanced Research Projects Agency Network (ARPNET) (Schneider, Evans & Pinard, 2009; Oppedisano, 2011, p. 3). Figure 2.2 shows a hand drawn plan of the Internet network that was created in 1969.

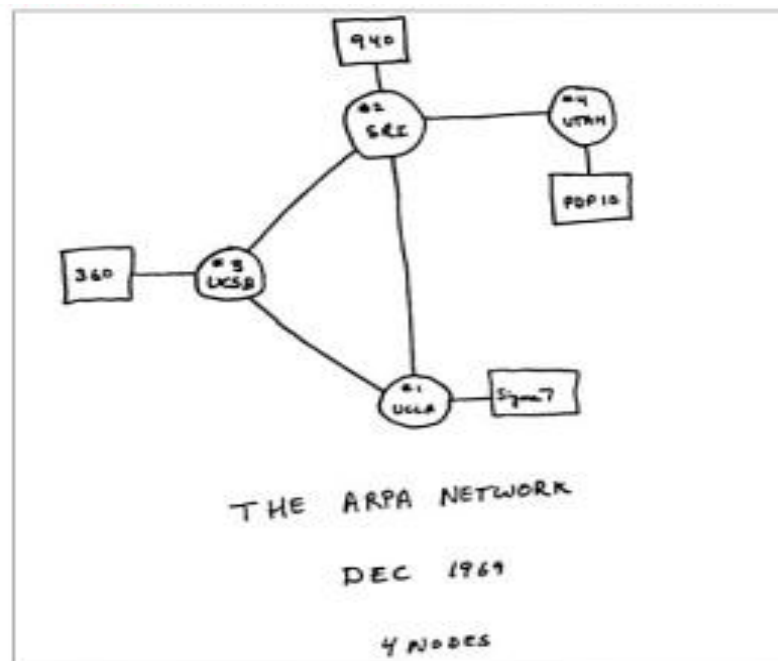


Figure 2. 2: The Internet Sketch Plan, 1969 (Schneider et.al, p.7)

ARPNET was rapidly growing in the United States from coast to coast, connecting the technologies of Bolt, Beranek, and Newman (BBN) to the network. The ARPNET was granted to the BBN Technologies organisation, which was located in Cambridge, Massachusetts. The organisation's role began with the first stages of the Internet in 1969 when they were granted a contract with DARPA to establish and implement a network that was committed to connecting four interface message processors (IMPs). The designed network had to automatically manage the packets by routing and sending them to their destination while concurrently updating the network a few times each second. The design of the network by the BBN Corporation was configured and sent to UCLA for testing. The team at UCLA connected the cables to the first IMP and ran it. The network was kept running for a few weeks without breaking down, which led them to test another IMP. An IMP arrived on October 29 at the Stanford Research Institute (SRI) to further test the network, which resulted in the first transmitted characters over the innovative network and the birth of ARPNET. Later, the third and fourth IMPs were configured at the University of California, Santa Barbara (UCSB) and the University of Utah. By April 1972, the network was increasing with a connection of 23 sites (Oppedisano, 2011).

In the 1980s the Internet was mainly used for connecting universities, research institutions and other computer science organisations to send and receive information through protected systems. Throughout the 1980s, the Internet continued to expand to connect computers located in buildings, cities, and countries across the globe in order to facilitate faster and more widespread communication (Anderson, 2011).

The Internet has vastly evolved since then. It is one of the most significant innovations in technology. Today, it is the foundation for some of the largest communication systems and technologies in the world. However, this network was not generally used until the early 1990s, when two important inventions emerged. One of these significant inventions was the World Wide Web (www) commonly known as the web. People often mistakenly use the terms 'web' and 'the Internet' as synonyms for each other. However, the web is in fact a public service operating over the Internet (Yeager, McGrath, 1996; Anderson, 2011).

The World Wide Web (www) is a worldwide networked environment of interlinked records, documents, information and data that are accessed through the Internet. It is also

defined as a connection of computers on a network that utilises the Internet to be able to interchange data, images, videos or any sort of multimedia following the standard protocols. The transforming point for the web was when the first web browser was introduced in 1993. It was a well-known Netscape web browser called Mosaic which was a graphical browser that was invented by cofounder Marc Andreessen and a group of computer scientists at the National Center for Supercomputing Applications (NSCA) at the University of Illinois in Urbana-Champaign (UIUC). The Mosaic web browser made the Internet more productive and simple to use as users were able to point the mouse and click on icons and hyperlinked words. Internet Services were announced in 1995 by major carriers such as British Telecom, France Telecom, Deutsche Telekom, Swedish Telecom, Norwegian Telecom, and Finnish Telecom. The Internet established itself in the mid-1990s as the main point for information, communication and business (McPherson, 2009).

The web is not only formed on the invention of the Internet and network services, it involves preceding information systems, hypermedia and digital representation of data. The World Wide Web is formed by three significant technologies, which are:

- Universal Resource Locators (URLs)
- Hypertext Transfer Protocol (HTTP)
- Hypertext Markup Language (HTML)

These three important technologies are open, public web protocols that are available for use by any client. The URL is an address system that allows nearly any type of stored data to be retrieved from practically anywhere over the Internet. The aim of a URL is to provide the stored file with a unique address regardless of the procedure it is following. URLs are used within web browsers to retrieve the web pages of a specific stored file from the host computer. Then the web pages of the specific stored file are downloaded to the client's device and presented on the screen of that same device. The Domain Name System (DNS) is used to translate the URLs into numeric addresses. This is a global system of connected servers that collects and saves the location of any type of website. The numeric address system is referred to as the Internet Protocol Address (IP). The IP replaces the numeric strings which raised issues of how users use them with the alphanumeric addresses. The web browser is able to contact the web server after the DNS

translation of the URL of the specified file the client has requested. URLs do not often look simple and short as shown in the following URL example on the New Zealand Government's website <https://www.govt.nz/browse/immigration-and-visas/>. As the web has developed, URLs are becoming more and more complex (Shah, 2009). This URL represents an address hosted in domains located in New Zealand. The structure of the above URL consists of the following factors:

1. Protocol: **http**
2. Host computer name: **www**
3. Second-level domain name: **govt**
4. Top-level domain name: **nz**
5. Directory name: **browse**
6. File name: **immigration-and-visas**

HTTP is a language or a lingua franca between two components of the web architecture system, which are the web browser and the web server that allow a variety of software programs to function and operate together to exchange data. HTTP is a clear set of rules that are aimed to be proper for the use of hypermedia systems allocated over networks. Furthermore, HTTP is the fundamental protocol employed for the World Wide Web. Each web browser is required to interpret the HTML language (Shah, 2009).

HTML allows programmers to generate multimedia hypertext that can be used by any type of web browser. It also allows programmers to assign more specific details on how a document should be displayed on the client's web browser. For instance, a pointer to other documents, often known as anchors, could be utilised by the programmer. An anchor fetches the next document from the server when it is clicked by the client (Shah, 2009).

The second significant invention was the Web browser, which was invented by Tim Berners-Lee. The invention of the Web browser was essential as the World Wide Web required it in order to access and surf for information (Anderson, 2011). It was written and developed one year after the invention of the World Wide Web. A Web browser is "a software program that allows users to access and navigate the World Wide Web" (Shah, 2009, p. 14). There is a variety of software browsers that are able to process the

computer application on different operating systems. These browsers include Internet Explorer, Google Chrome, Mozilla Firefox, Safari and Opera among other less common browsers. The World Wide Web has allowed users across the globe to access and contribute to its wealth of information. The Internet comprises numerous amounts of data on nearly every topic. The web has dramatically changed the way people around the world communicate, work, and learn. As users add new Web pages frequently, the influence of the World Wide Web will continue to expand (Mcpherson, 2009; Shah, 2009; Cohen-Almagor, 2011). Figure 2.3 illustrates the growing number of websites between the year 2000 and the year 2014.

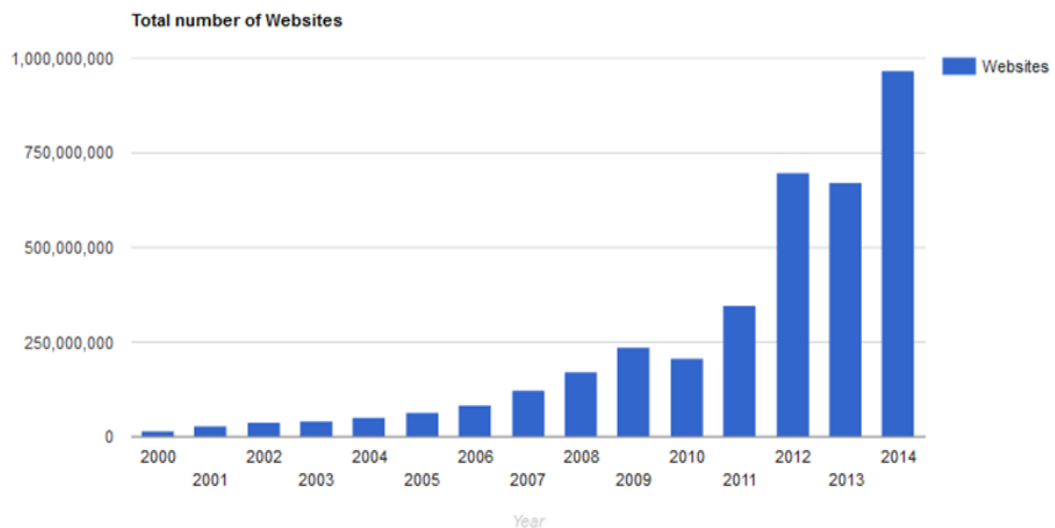


Figure 2. 3: Number of Websites by Year Since 2000 (Internet Live Stats, 2014)

Users around the world were then able to create their own personal web pages. People globally were getting more and more interested in the Internet as a source to search for information, business, commerce, entertainment, and nearly anything else. The Internet was increasingly used by users and one of the main clients' concern was the need and value of privacy when surfing the web. Users are sharing and producing their own personal information on the Internet because of the developments and changes in information and communication technologies. For instance, users' personal information was allowed to be recorded on software developed for writing purposes such as Notepad, TextEdit and other basic editors. In addition, the development of printing technology has simplified the process of producing private information and distributing it to the public which resulted in maximum efficiency of electronic communications and rapid

movement of information sharing. Furthermore, the invention of digital technologies and the increasing proliferation of social media in the last two decades has exposed challenges in the way users view privacy and privacy protection (Shah, 2009; Cohen-Almagor, 2011).

Computerised data has raised the need for privacy in most societies to protect individuals' and organisations personal information from invaders. Individuals' and businesses' personal data are and will continue to be a valuable asset (Hoven & Weckert, 2008). Invasion of privacy is an issue whether it is online or offline. As sharing one's private information online becomes more commonplace, it becomes even more vital to take actions in protecting users' personal information and privacy that they do not wish to share openly. In the digital sphere, more users are involved in business transactions compared with the non-digital world, and this involves personal information such as names, email addresses, credit card information, and other sensitive data. This could lead to the threat of an offender secretly eavesdropping on confidential data being shared between parties, which is an increasing threat in the digital world compared to the physical world (Flegel, 2007). One risk with online transactions is the possibility of fraud. There are different creative ways for an offender to commit fraud online by the use of email, phone or website (Miller & Jentz, 2011). The Nigerian letter fraud scam is one of the longest-running frauds that involved the loss of hundreds of millions of dollars and continues to this day (Miller & Cross, 2012).

With the variety of threats occurring over the digital network, the concern of users online has raised the need to secure their privacy. There are many ways to secure information with regards to browsing activities, and among these is, disabling cookies which could prevent websites from tracking individuals' information (Miller & Jentz, 2011).

2.3 PRIVATE BROWSING

As the concern of privacy is rising, companies have developed some tools to prevent tracking and accessing individuals' information. Many web browser vendors have added a new feature that is built into their browsers which is designed to secure individuals' information while browsing online. In addition, this feature is able to avoid websites or prevent offenders from tracking individuals while surfing the web or even storing the

browser cache and history list on the individual's computer hard disk. The feature is useful to some extent as it should prevent the browsing activities from being stored on the user's device but it not completely private from third-party tracking software that is embedded in some sites or servers (Lerner, Elberty, Poole, & Krishnamurthi, 2013).

In 2005, the private browsing mode feature was initially introduced in Apple Safari 2.0. Private browsing was informally known as "porn mode", as some users did not want their wives or others to know about their adult browsing history (Cherry, 2013). Three years after the introduction of the private browsing feature by Apple, Google Chrome 1.0 was developed as Google's version, which was called "Incognito". Subsequently, Mozilla Firefox 3.5 and Internet Explorer 8 presented versions of this feature, known respectively as Private Browsing and InPrivate (Said et. al, 2011). Zalewski (2012) states that private browsing "creates a non-persistent browsing sandbox, isolated from the main browser session, which is completely discarded as soon as the last private browsing window is closed" (p. 249). Another definition by Parsons (2015) states that private browsing is a service offered by most common browsers which aims to delete the browser cache and the history list from being stored on the digital device.

The private browsing mode is thus now included under different names in all common browsers, with the main objective being to delete and remove all the information that could lead to others gaining knowledge of the user's private browsing activity. The browser wipes the cache information, cache, history, cookies and other data stored in local storage spaces when the private browsing session is closed (Jacobson & Idziorek, 2012; Laud, 2012). Several browser vendors claim that private mode browsing protects the user's browsed information from being stored locally on the user's machine. In the event that these claims are valid, users will have greater protection when browsing the web because they will not need to worry about others finding out about their browsing activities (Lerner et al, 2013).

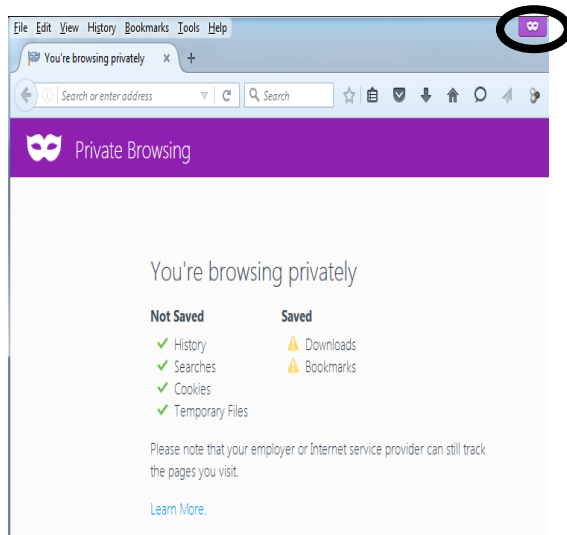
The private browsing mode is often defined as the feature that does not remember any data about an individual's current session. The aim of this mode is to prohibit any data being written to the disk. The initial plan when developing the private browsing feature in Firefox was to have a bullet-proof solution that will not write anything to the disk (Lerner et al., 2013). If what Firefox claims is accurate, individuals who wish to browser privately on the Internet will have more confidence while browsing. Google

Chrome in incognito mode has claimed that there will not be any cookies or other information related to the session remaining on the hard disk after the browser is closed, as all details including the records of the files being downloaded will be deleted after the session is ended on the user's device. Google Chrome has noted that information of the user's browsing activity when using the incognito mode could be viewed by the internet service provider, the network administrator if using a public computer, or the website being visited (Google, 2016). Meanwhile, Internet Explorer (IE) ensures that data relating to the browser history, temporary Internet files, form data, cookies, and user names and passwords are prevented from being preserved (Internet Explorer, 2016). Safari has provided more details than other vendors on what private browsing offers to users. As claimed by Safari, webpages, AutoFill information, and downloads are not retained by the browser. In addition, each private tab is isolated from other tabs, which prevents other websites from tracking users' browsing activities. Furthermore, private browsing activities are not stored in iCloud (a feature developed by Apple to connect between Apple devices and share information, which includes webpages). Opera claims, as other web browser vendors have claimed, that browsing activities will not be retained by the browser. The data that will be deleted after a private session has ended are browsing history, items in cache, cookies and logins (Harvell, 2013; Safari, 2015). Internet Explorer's behaviour in normal browsing mode saves all the browsing activities, while in private browsing mode information related to that session would be discarded. The changes to Internet Explorer's behaviour in private browsing mode are as followed:

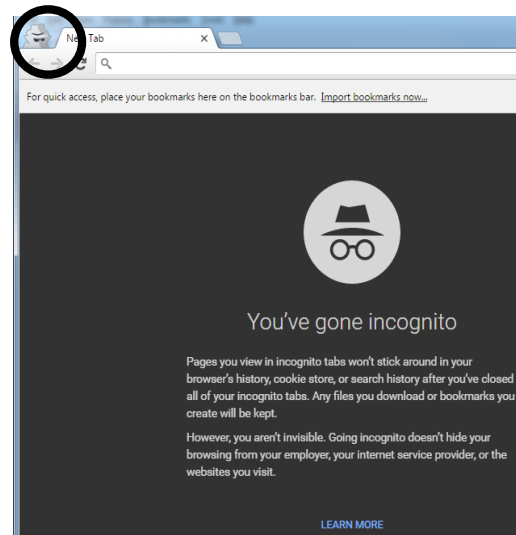
- New cookies are not stored
 - All new cookies become "session" cookies
 - Existing cookies can still be read
 - The new Document Object Model (DOM) storage feature behaves the same way
- New history entries will not be recorded
- New temporary Internet files will be deleted after the Private Browsing window is closed
- Form data is not stored
- Passwords are not stored
- Addresses typed into the address bar are not stored
- Queries entered into the search box are not stored

- Visited links will not be stored

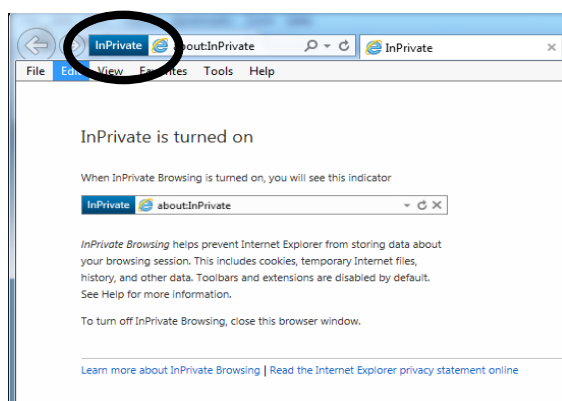
Users using shared digital devices in public or at home could take advantage of the private browsing mode to browse the web without leaving any traces of their browsing activities on the shared device. For instance, a user who wants to search for an engagement ring on a shared device, but who wants to keep this search hidden, will benefit from the private browsing feature as this will delete any history files relating to the engagement ring as soon as the user exits the browser window (Jacobson & Idziorek, 2012). Figure 2.4 presents the user interfaces associated with the private browsing modes in four common browsers, which are Firefox 45.0, Google Chrome 50.0, Internet Explorer 11, and Safari 8. Google Chrome and Internet Explorer have clear indicators that browsing is being conducted in private mode, while the indicators on Firefox 3.6 are more subtle. Safari 8's indicators in private browsing mode currently display a dark address in the address bar of the Safari browser.



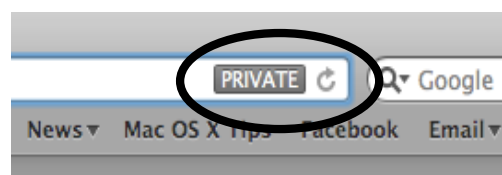
(a) Firefox 45.0



(b) Google Chrome 50.0



(c) Internet Explorer 11



(d) Safari 8

Figure 2. 4: Indications of the Private Browsing Mode

2.4 PRIVATE BROWSING IMPLICATIONS

The privacy browsing mode could be a beneficial feature for users who wish to browse privately without leaving any traces to the user's browsing activity. However there may be web browsers that do not actually do what they have claimed or what users expect them to do. The private browsing mode could leave information behind about what users have been doing during their private browsing session. As pointed out previously in section 2.3, history entries are the only entity that is not recorded in Internet Explorer InPrivate browsing, while other types of information are recorded and later deleted after the session ends, such as the browser's cache (Smulikowski, 2009). This means that there may be a possibility for forensic experts to recover the deleted files to search for relevant information using specialist data recovery tools. The information entities that are affected,

for instance by Internet Explorer InPrivate browsing, are shown in table 2.1. There are different areas where information of browsing activities could be stored on local devices, such as cache, cookies and other areas that will be discussed in the following section.

Table 2. 1: Stored data during InPrivate browsing (Smulikowski, 2009)

Information	How it is affected by InPrivate Browsing
Cookies	Kept in memory so pages work correctly, but cleared when the browser is closed.
Temporary Internet files	Stored on disk so pages work correctly, but deleted when the browser is closed.
Webpage history	This information is not stored
Form data and passwords	This information is not stored
Anti-phishing cache	Temporary information is encrypted and stored so pages work correctly
Address bar and search AutoComplete	This information is not stored
Automatic Crash Restore (ACR)	ACR can restore when a tab crashes in a session, but if the whole window crashes, data is deleted and the window cannot be restored
Document Object Model (DOM) storage	The DOM storage is a kind of “super cookie” that web developers can use to retain information. Like regular cookies, they are not kept after the window is closed

2.4.1 Browsing Storage Areas

Every time a digital device accesses the Internet, the device’s operating system records information regarding the websites that have been visited. The information related to each session is stored with the belief that the user will possibly want to revisit the website, and so this information will make the access to the website in the future much quicker (Girard, 2013). There are different areas where information related to web browsing is stored in digital devices which depends on the browser and operating system utilised; for instance Internet Explorer leaves browsing artefacts in a file called index.dat. Web browsing activities can lead computer forensic experts to potential evidence that could be useful to present in a civil or criminal investigation. Digital forensic investigators are more likely to find valuable and relevant data such as the URL of the last visited website, the date and

time it has been visited, and the number of times the website was has been visited by the user, in the following areas; browser cache, browser cookies, browsing history, Random Access Memory (RAM), paging files, Hibernation File, download history, saved passwords, saved forms and unallocated space (EC-Council, 2009; Gogolin, 2012).

2.4.1.1 Web Browser Cache

The cache is an area which indicates which websites have been visited by a user, and as such this could be an important area to investigate. Frequently visited websites are accessed faster when there is a cache on the user's device (Girard, 2013). The cache is defined as "an area of RAM or disk storage used to store frequently accessed information for speedy retrieval" (Stanger & Grayson, 2006). The cache contains a collection of web page copies that are stored on the device's hard disk or in its volatile memory as a result of an individual's web browsing activity. Most web browser vendors have provided the ability for the cache to be cleared manually by the user; yet expert digital investigators could use tools to reconstruct the cache in order to view the files and find traces of important information (EC-Council, 2009). When users are browsing, the web browser fetches pages and graphics to form the web page and then stores the web page's temporary files, HTML documents, images and other web page elements to the browser cache of users' local devices in order that downloading the same content later will be much easier. This is shown in figure 2.5 (Parsons, 2015). Browsers check and load the images or files when visiting a website from the cache rather than downloading them again from the web if they exist in the cache (Sklar, 2014). Cache files could include the URL of the website visited by the user, file names, and file extensions such as .gif. The cache contents could remain on the user's local device for days, months, or until the user's storage space is filled up with other data, which is specified in the user settings under preferences. The cache location differs from one operating system to another and from one web browser to another (Altheide & Carvey, 2011).

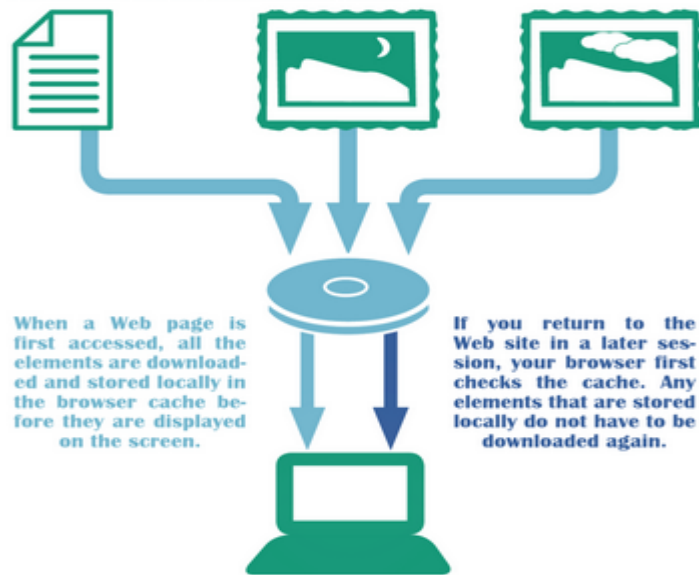


Figure 2. 5: Web Browser Cache Functionality (Parsons, 2015)

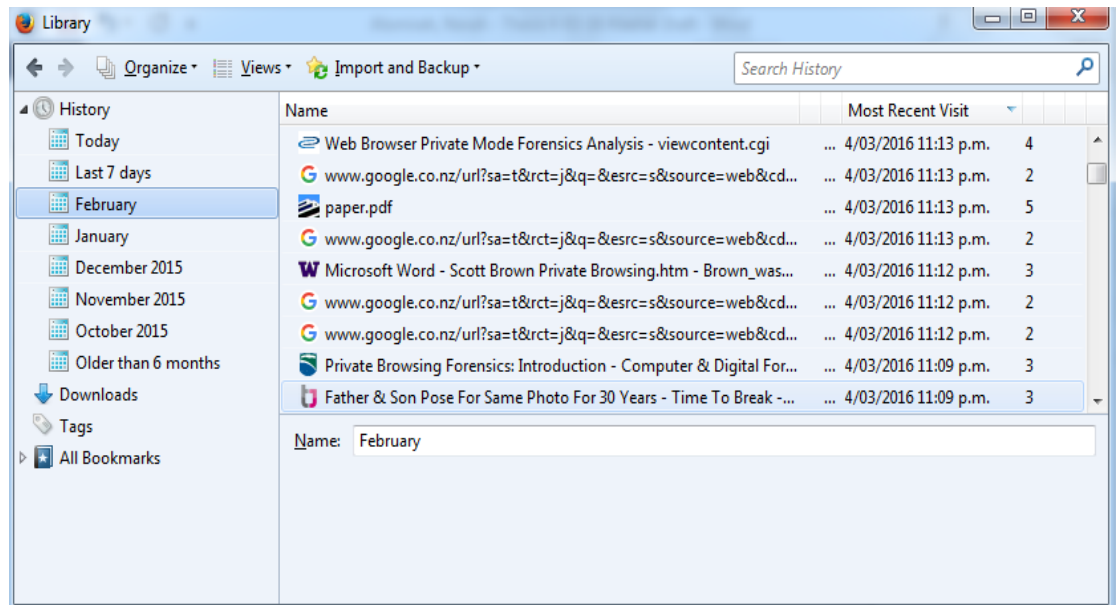
2.4.1.2 Web Browser Cookies

Cookies are similar to the web browser cache as they determine the websites that have been visited by individuals. Cookies could be useful during an investigation as they are able to remember the personal information of a user such as their username and password being typed into a website. Cookies are text files of information that reside on a user's system often located in the memory of the individual's device by a visited website (Girard, 2013). Cookies currently are used by many websites to store data about users and the mode they are using the website with on their local devices. Some information about the users such as usernames and passwords is maintained by cookies to track each user interaction (Cherry, 2013). 'Persistent' and 'session' are two types of cookies. The differentiation between the two types is their lifetime. The former remains on the user's hard disk for a particular period of time after the user has visited a website. The time of expiration of the persistent cookie is set by the website, and the cookie will remain on the user's hard disk until the time of expiration has been reached. The aim of the persistent cookie is to record when the user revisits the website (Danesh, Lau, & Mehrassa, 2002).

Conversely, the session cookie expires after an individual logs out of the website or closes the browser. Session cookies can be found on shopping websites as they are utilised to keep track of the user's item in the virtual shopping cart. There are different locations on an individual's computer where cookies are stored which depends, on the browser being utilised. There is a variety of tools on which to view the contents of cookies, including simple text editors such as Notepad (Danesh, Lau, & Mehrassa, 2002).

2.4.1.3 Web Browsing History

The website that has been visited by users is automatically recorded by web browsers. For instance, Internet Explorer records the user's browsing activity in details such as the universal resource locator (URL), and the time and date for each website visited in a file named index.dat (Girard, 2013). Figure 2.6 presents a web history of the browsing activities using Firefox, which includes the URL, the date and time, the most recent visit, and the number of times a particular website has been visited.



The screenshot shows the Firefox Library window with the 'History' tab selected. The left sidebar shows a calendar view for February. The main pane displays a table of browsing history entries. The table has columns for 'Name', 'Most Recent Visit', and a count of visits. The entries include various Google search results, a PDF file, and a Microsoft Word document. The search bar at the top of the main pane is set to 'February'.

Name	Most Recent Visit	Visits
Web Browser Private Mode Forensics Analysis - viewcontent.cgi	4/03/2016 11:13 p.m.	4
www.google.co.nz/url?sa=t&rct=j&q=&esrc=s&source=web&cd...	4/03/2016 11:13 p.m.	2
paper.pdf	4/03/2016 11:13 p.m.	5
www.google.co.nz/url?sa=t&rct=j&q=&esrc=s&source=web&cd...	4/03/2016 11:13 p.m.	2
Microsoft Word - Scott Brown Private Browsing.htm - Brown_was...	4/03/2016 11:12 p.m.	3
www.google.co.nz/url?sa=t&rct=j&q=&esrc=s&source=web&cd...	4/03/2016 11:12 p.m.	2
www.google.co.nz/url?sa=t&rct=j&q=&esrc=s&source=web&cd...	4/03/2016 11:12 p.m.	2
Private Browsing Forensics: Introduction - Computer & Digital For...	4/03/2016 11:09 p.m.	3
Father & Son Pose For Same Photo For 30 Years - Time To Break - ...	4/03/2016 11:09 p.m.	3

Figure 2. 6: Firefox Browsing History Table

2.4.1.4 RAM

Random Access Memory or RAM is the main memory for digital devices to store temporary data, codes, settings and so forth. RAM is a volatile memory, which means that data stored in memory will be lost after the digital device is powered off. Information that is stored in RAM before powering off the device is often written to the hard disk in files called paging files. Information related to RAM can also be found in unallocated clusters, file slack and the hibernation file. Furthermore, digital forensic experts might be able to find relevant information in RAM using the appropriate data recovery tools. Therefore the contents of RAM may be able to be retrieved from the device's local disk.

2.4.1.5 Paging Files

Paging files, referred to as swap files, are duplicates of the physical memory which are designed to increase the amount of memory available to the programs running on the digital device. The paging file is the most vital form of ambient data, which is information that is recorded in files and not usually accessible by users (Vacca & Rudolph, 2010). Most users using digital devices are not aware of the existence of paging files. These files are considered as virtual memory extension of the physical memory. Paging files can be temporary or permanent; this depends on the version of the operating system installed and the user settings.

Permanent paging files are preferable from the forensic perspective as they hold larger amounts of data for a long period of time. However, temporary paging files are more common. When a temporary paging files reduces its size too close to zero, it occasionally transfers the file's content to unallocated (free) space, which could be forensically examined to retrieve potential evidence (Vacca & Rudolph, 2010).

The size of these files is frequently large, usually ranging from 40MB to more than 400MB and named pagefile.sys (Bunting & Wel, 2006). In addition, swap files semi-permanently duplicate general transient information from the memory. Paging files are regularly overwritten with new data and can be wiped by the operating system when the digital device is powered off or on. Furthermore, the swap file could contain fragments of deleted data. The contents of the paging file may consist of Internet browsing activity, remnants of word processing, database entries and any other operations that have occurred in previous sessions on the operating system. Forensic experts face a challenge when analysing the swap file, but it may be possible to find relevant evidence if the offender was believed to have been engaged in some sort of illegal activity, such as acquiring or transferring child pornography shortly before his/her digital device was seized (Steel, 2014).

2.4.1.6 Hibernation File

Many operating systems such as Windows and Mac OS allow the digital device to sleep, hibernate, and shut down. Hibernation and sleep are two major states that allow digital devices to store temporary data to quickly retrieve them in a matter of seconds. Each of these options has its own way of functioning to temporarily store data and then terminate the power. The purpose of the hibernation option is to save the device's power by switching to hibernation mode while it is not being used. The user's activity and the

physical memory (RAM) is written to a file to allow return to the precise point where the device went into hibernation (Bunting & Wei 2006). The size of the hibernation files is the same size as the system's RAM memory size. The contents are captured and automatically written to the hibernation file by the operating system, which is named hiberfil.sys in Windows and sleepimage on Mac devices (Hayes, 2014). The location of the hibernation file is in the root of the system drive as shown in figure 2.7.

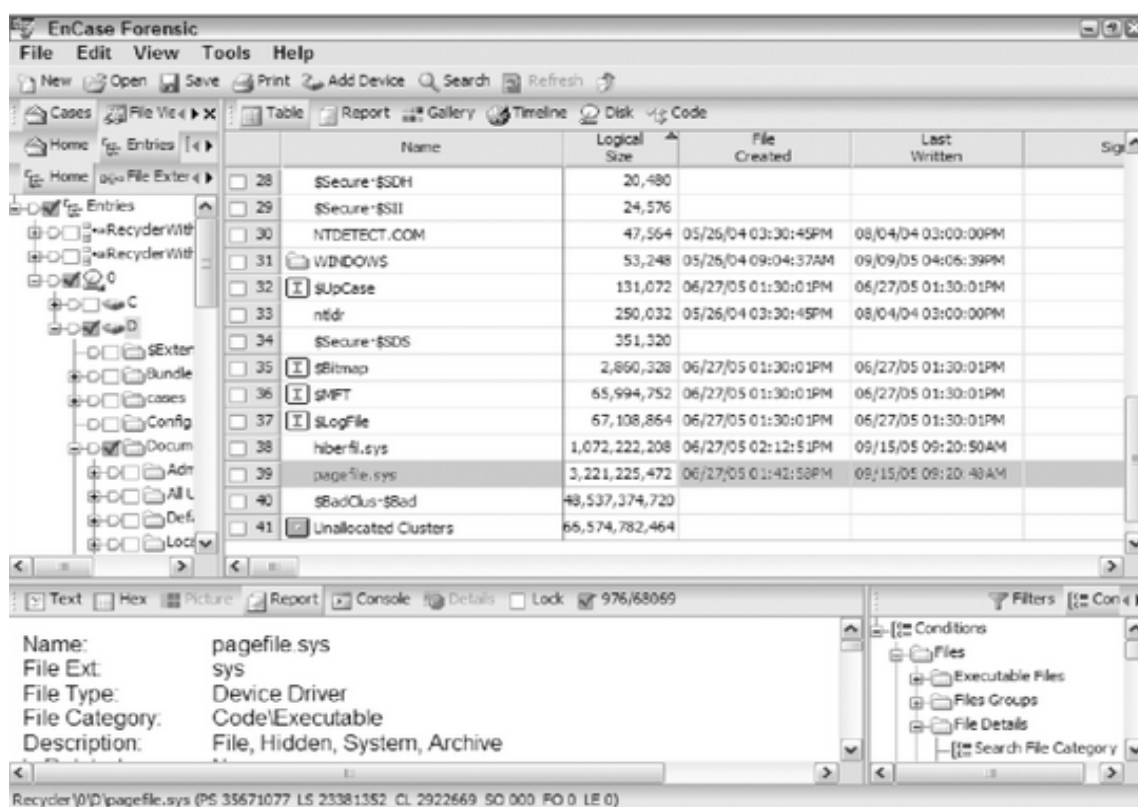


Figure 2. 7: Hibernation File viewed in Encase Software (hyberfil.sys) (Bunting & Wei, 2006, p.381)

The hibernation file and paging files are similar to each other in terms of their potential contents. However, the hibernation file captures and records the entire contents of the physical memory and is intentionally stored when a digital device is shut down (Steel, 2014). The data that has been recorded using the hibernation file is restored when the digital device is awakened. The hibernation file could assist digital forensic experts in learning what was happening to the system at its last point of operation, as the file is not securely deleted after the computer is turned on. The capacity of the hibernation file could be quite large depending on the size of RAM available on the computer, so plenty of time might be needed to analyse it (Bidgoli, 2006).

2.4.1.7 Unallocated Space

When files are deleted via traditional methods, such as dragging or placing files into the recycle bin of a computer and then emptying the bin, the contents of those files are not actually removed from the hard drive. Individuals may think that deleting files means that it is impossible to recover the file but in fact the majority of deleted data remains on the drive at least in the short term. Files are stored using a “directory” on most file systems which maps filenames and other metadata to locate the file contents on the disk. The contents of the file are kept in its location until the operating system overwrites the deleted file area with new information. Therefore, when files are deleted following the traditional methods, they are deleted or labelled as deleted in the directory and the area where they are stored is made available to be overwritten with new data.

The area is referred to as unallocated space by the operating system, or free space, or slack space, which is defined as the hard drive area where file storage has never been allocated for the area of deleted file content (Vacca & Rudolph, 2010). However, slack space is different from unallocated space. Slack space is the unused area between the end of the actual saved file and the end of the cluster. The type of information that is held by unallocated space could consist of intact files, fragments of files and subdirectories, and temporary files that were created and deleted by computer programs or the operating system. In addition, files that were recently sent to a printer, or users attempting to repartition or reformat a hard disk, or files which were open when the system crashed could be forensically found in unallocated space (Vacca & Rudolph, 2010). Figure 2.8 shows an example of three hard disk partitions and two DVD-ROM disks.

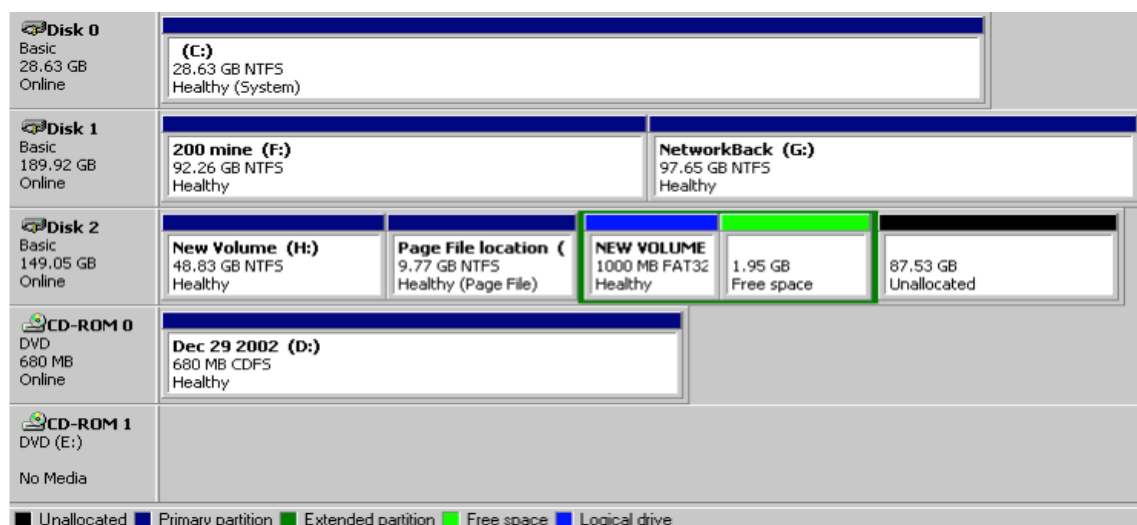


Figure 2. 8: Viewing Partitions on the Hard Disk (Vacca & Rudolph, 2010)

The fragments of old files in unallocated space can be found anywhere on the drive, even on different partitions, though they are usually found on the next partition headers, file allocation tables (FAT), and the last sectors of a cluster. A file allocation table (FAT) in Windows-based operating systems is a table that is responsible for storing the association between files and the clusters that are assigned to them. Clusters are defined as “a fixed-length block of data on a computer that is used to store files” (Maras, 2015, p.36). There are a range of sizes of clusters operating on Microsoft Operating System and these depend on the size of the hard drive and the file system.

2.5 DIGITAL FORENSICS

From the 1960s to the early 1980s corporations, universities, research centers, and government agencies primarily owned and operated computers as industrial systems developed to support data processing functions. System administrators were responsible for securing the system and computers with routine audits to ensure the efficiency and accuracy of the data processing functions. The computer during that time of period became an area of interest to the information security, legal and law enforcement communities. Small ad hoc groups of individuals have been created by several government agencies to gather data from computer systems that could be used as evidence in civil or criminal cases (Sachowski, 2016)

Computers then started to become available for personal use for many users which raised threats to companies and individuals. Prior to the 1980s, many crimes involving the use of computers were dealt with using existing laws. Furthermore, forensic investigations were performed by investigators that had basic training, were disorganised, lacked computer forensics equipment and tools and did not follow standard procedures. However, law enforcement agencies began creating additional laws in response to the increasing number of computer crimes. Government agencies began to establish a common body of language (CBK) of principles, methodologies and techniques that digital forensic investigators could apply to standardise and implement a formal structure to computer forensics investigations.

According to Sachowski (2016) computer forensics took a major step forward in becoming more formal through the 1990s to 2000s. Additionally the Internet became quickly available for use in corporates and homes that introduced consumers' accessibility to electronic mail and web browsing. The growth of crime into computer systems for that period was known with different terms which were computer forensics, forensics computer analysis, or forensics computing. According to Daniel, Daniel, &

Spielman (2012) computer forensics is defined as “the collection, preservation, analysis, and presentation of electronic evidence for use in a legal matter using forensically sound and generally accepted processes, tools, and practices” (p. 3).

Digital forensics is a scientific discipline that uses digital data to solve a crime with a close adherence to the law. Digital forensics was known as computer forensics at first, as it mostly dealt with computer crimes; but as other technological developments were developed, the discipline extended to involve all digital technologies. Digital forensics involves more specific areas such as mobile forensics, Internet forensics, web forensics, network forensics, and recently new areas of interest: cloud forensics and social network forensics. Figure 2.9 presents a brief historical perspective of digital forensics.

Year	Event
1981	IBM introduced the 5150 PC.
1984	The FBI established the Magnetic Media Program, later known as CART.
1984	The National Center for Missing and Exploited Children (NCMEC) was founded.
1985	HTCIA was founded in CA.
1986	The USSS established the Electronic Crimes Task Force (ECTF).
1986	Congress passed the Computer Fraud and Abuse Act.
1993	The first International Conference on Computer Evidence took place.
1994	Congress passed the Crime Bill, and the USSS began working on crimes against children.
1994	Mosaic Netscape, the first graphical web browser, was released.
1995	The International Organization on Computer Evidence (IOCE) was formed.
1996	USSS founded the New York Electronic Crimes Task Force (ECTF).
1999	The First Regional Computer Forensics Laboratory (RCFL) was established in San Diego.
2000	The IRS Criminal Investigation Division (IRS-CID) began using ILook.
2001	The USA PATRIOT Act and USSS were directed to establish ECTFs nationwide.
2001	INTERPOL developed a database of exploited children (ICAID).
2002	The Department of Homeland Security (DHS) was formed.
2003	The PROTECT Act was passed to fight against child exploitation.
2003	Fusion centers were established.
2007	The National Computer Forensics Institute (NCFI) was established.
2008	The formation of an INTERPOL Computer Forensics Analysis Unit was approved.
2009	The first European ECTF was formed (Italy).
2010	The second European ECTF was formed (United Kingdom).

Figure 2. 9: Brief History of Computer Forensics (Hayes, 2014)

Digital forensics evidence involves any electronic media that stores or transmits data in various forms. There are different types of digital evidence that could be seized in a criminal case such as hard disks, images, documents, Universal Serial Bus (USB) drives, laptops, and smartphones. The data from the digital evidence seized and examined can be relevant as it assists law enforcement representatives to convict the individuals they may arrest. The digital evidence collected should be carefully acquired in a proper approach by the digital forensic investigator to preserve the evidence from being altered as it can be easily modified or destroyed if mishandled.

Digital forensics has been involved in many investigations, ranging from criminal to civil investigations. Seized digital evidence is maintained and preserved by forensic examiners in law enforcement investigations to ensure that the data obtained for evidence is examined following the correct legal procedures and legislative standards within and the rules of evidence (Nelson, Phillips, & Steuart, 2010). A variety of hardware and software tools are used by forensic investigators to extract and analyse data. Evidence in a digital forensics investigation could include emails, images, videos, websites visited, and Internet searches (Hayes, 2014). The definition of digital forensics was first stated at the Digital Forensic Research Workshop (DFRWS) in 2001:

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

2.5.1. Digital Forensics Models

There have been many digital forensics investigation processes throughout the years that have been proposed and established with one distinct objective in common: to ensure that the investigation process follows an appropriate guideline that allows the investigation outcomes to be presented in a court (Carrier, 2009). In the early 1980s, the FBI Laboratory and other law enforcement agencies started to develop new programs to examine computer artifacts. The procedure conducted by digital forensic examiners in an investigation has a direct influence on the results of an investigation (Yusoff, Ismail & Hassan, 2011). Thus, it is essential to have scientific processes that follow the legal procedures when conducting a forensic investigation in order to have a successful prosecution (Kohn, Eloff, & Olivier, 2006).

Inappropriate steps performed by forensic experts, such as bypassing a step or switching any of the steps, may lead to inconclusive results which may give rise to invalid conclusions. Therefore, it is indeed crucial for the digital forensic examiners to handle digital evidence in the proper manner, as all actions taken will be later subjected to scrutiny by the judiciary. The existence of an accepted structured model offers a proper mechanism to follow by the digital forensics examiner. Table 2.2 presents the history of

the digital forensics models at their earliest to their present with a brief discussion of some of the frameworks in the next section.

Table 2. 2: Digital Forensics Investigation Frameworks

Model Number	Year	Name
M01	1995	Computer Forensic Investigative Process
M02	2001	DFRWS Investigative Model
M03	2001	Scientific Crime Scene Investigation Model
M04	2002	Abstract Digital Forensic Model
M05	2003	Integrated Digital Investigation Process
M06	2003	End to End Digital Investigation
M07	2004	Enhance Digital Investigation Process
M08	2004	Extended Model of Cybercrime Investigation
M09	2004	A Hierarchical, Objective-Based Framework for the Digital Investigation
M10	2006	Computer Forensic Field Triage Process Model
M11	2006	Framework for a Digital Forensic Investigation
M12	2007	Dual Data Analysis Process
M13	2007	Common Process Model for Incident and Computer Forensics
M14	2009	Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)
M15	2010	Network Forensic Generic Process Model

Over the years, some of the proposed frameworks have been relevant to a very specific investigation scenario while other models have been applicable to a wider scope. In addition, some of the processes tend to be more detailed whereas others tend to be more general.

The different types of digital forensics frameworks proposed by many authors' leads challenges for digital forensic investigators when selecting the appropriate digital forensics framework as there is not a standard model that should be followed. Digital forensic investigators that have only a very basic knowledge might be unsure as to what type of framework to apply for each investigation (Kalbande & Jain, 2013).

2.5.1.1. Computer Forensics Investigative Process (1995)

The earliest digital forensics framework was proposed in 1995 by Mark Pollitt, a special agent at the Federal Bureau of Investigation (FBI). He proposed a procedure for the way digital evidence should be handled so that the results of the forensics examination will be technically reliable and legally acceptable. Pollitt's computer forensics model consisted of four distinct phases, as shown in figure 2.10 (Yusoff et al. 2011).

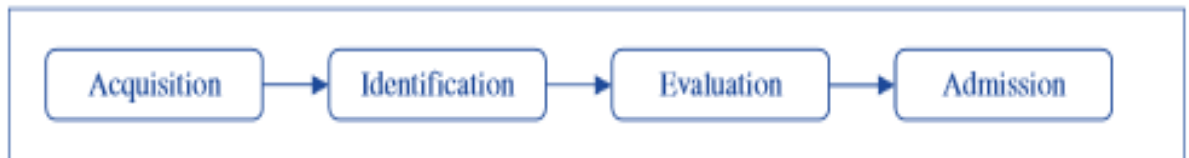


Figure 2. 10: Earliest Forensics Examination Framework

The initial phase is to ensure that the digital evidence is acquired in the proper manner including acceptable legal authority to acquire the device. The next phase, which is identification, is to examine the digital evidence to find relevant data. The evaluation phase determines if the examined device is in fact important to the case being investigated and can be considered as legitimate evidence. The last phase accounts for presenting the acquired and extracted evidence to the court.

2.5.1.2. DFRWS Investigative Model

In 2001, the Digital Forensics Research Workshop (DFRWS) proposed and recommended a digital forensics investigation process that consists of 6 steps, which are as follows in figure 2.11:

- Identification – involves profile detection, system monitoring, audit analysis
- Preservation – critical phase that involves setting an appropriate case management and ensuring a proper chain of custody to ensure that the evidence is free from contamination
- Collection – involves collecting the evidence in a proper manner
- Examination – critical phase that involves examining the digital evidence of hidden or encrypted data
- Analysis – critical phase that involves analysing the evidence such as data mining
- Presentation – involves documenting all phases and export testimony

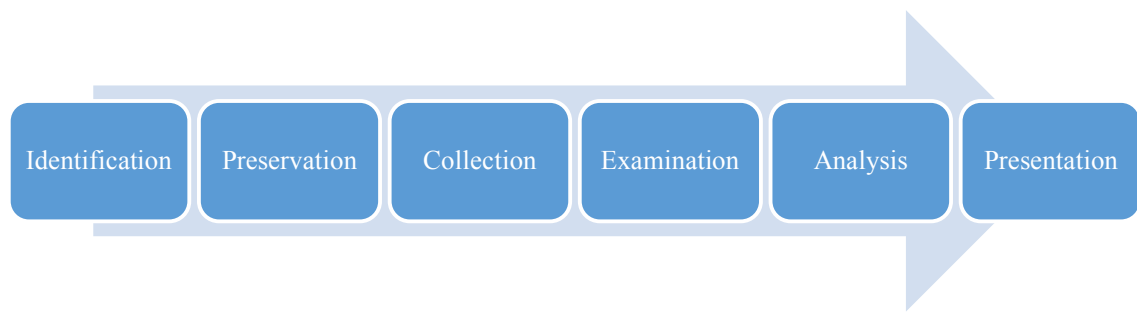


Figure 2. 11: Digital Forensics Research Working Group (DFRWS) Model (Yusoff et al, 2011)

Other models such as the National Institute of Standards and Technology (NIST) have recommended that the digital forensics investigation should follow the four basic phases, which are collection, examination, analysis and reporting (Kent, Chevalier, Grance, & Dang, 2006). Yusoff et al. (2011) in their research compiled all the phases used in digital forensics investigations and found that there are 46 different phases that are duplicates or which overlap each other. Other research conducted by Alharbi, Weber-Jahnke and Traore (2011) has also compiled all phases and found that most of the stages covered five distinct phases: identification, preservation, collection, analysis, and reporting.

Phase one, which is identification, involves tasks that are performed to locate each digital piece of evidence while being aware of how and where the digital evidence is stored and justifying the tools and techniques used to acquire and examine it (McKemmish, 1999). Digital evidence is located on storage mediums that store electronic data or transmit data through the network. Digital evidence can be easily tampered with, therefore digital forensic examiners should handle the seized evidence in the proper manner and with care. During a digital forensics investigation, if there has been any mishandling of the evidence, this will invalidate the evidence seized, which means that it will likely not be acceptable in court. This is important when collecting evidence, as the acquisition of evidence should not result in any changes to the original evidence. Preserving the evidence from being tampered with and altered is the forensic examiner's main goal when collecting digital evidence. When examining computer hard drives forensic specialists, recommend using forensics bridges, either hardware or software based, before processing the acquisition of the suspect's hard disk. Forensics bridges are used to prevent the workstation operating system writing data to the hard disk, thus maintaining the integrity of the data.

Validating the image by comparing the hash value of the suspect's disk with the image taken is the following critical step when the acquisition of the image is finalised as shown in figure 2.12. The hash value ensures that the data imaged has not been changed

by creating a unique hexadecimal identifier for each file. There are different methods to create hash values for data validation, the Message Digest 5 (MD5) and Secure Hash Algorithm version 1 (SHA-1) are the most common hash algorithm used in a forensics investigation. Digital forensic examiners can then start the next phase of examining and analysing the image provided the hashes of the original evidence seized and the image acquired are identical in order to extract relevant evidence for the case.



Figure 2. 12: Validating Data (Daniel, 2011)

Analysing digital evidence is the process where digital forensic examiners recover data that suspects have deleted on hard drives. This phase is typically the most time-consuming for digital forensic specialists as they are required to be thorough during the process of analysing the data as important details could be easily overlooked. Proper forensics tools are used in this phase to extract, process, and interpret digital evidence to provide valuable information in relation to the purpose of the investigation (Kent et al., 2006; McKemmish, 1999).

Digital forensic examiners main principle in general is to apply a systematic process to arrive at proper conclusions based on the evidence obtained from the seized digital evidence, or to conclude that there is no evidence to be obtained. The last phase is to document and report the results. Documenting the forensics investigation is a critical part of the process for law enforcement as the collection, examination, and extraction conducted by digital forensic examiners may be subject to rigorous questioning. Therefore, it is imperative for forensic experts to thoroughly document everything done from the beginning of the case to its closure. The documentation phase includes different types of important information related to each case such as a Chain of Custody form, timestamps, results and conclusion. The report presents relevant information gathered from the beginning phase of the DFRW model to the end.

2.6 CONCLUSION

Chapter 2 has reviewed literature ranging from the perspectives with which people value their privacy online and how they have adopted the use of private browsing on major browser vendors' products to its impact on digital forensics investigations. The chapter started by defining privacy and why Internet users care about their privacy. It discussed the various limitations and conditions associated with each major browsing vendor, which were then shown to have many implications for digital forensics investigations. Section 2.5 has highlighted the most common forensics frameworks that digital forensic investigators should adopt in digital forensics investigations. Digital forensic specialists need to be well prepared when handling the seized digital evidence. In addition, being familiar with the process of extracting and examining different digital evidence to reveal the latest evidence is essential. Any incompetent handling of the seized evidence may lead to tainting it, thus affecting the findings. Furthermore, improper handling of digital forensics evidence may affect its acceptability in a court of law. Therefore, the aim of the proposed research is to achieve a forensic ally sound and efficient procedure of examining web browsing artefacts left on local hard drives.

Chapter 3, the methodology chapter, outline the research methodology by reviewing similar works related to the research area and establish the main research questions in addition to the associated sub questions. Lastly, the limitation of the research design will be identified and discussed at the conclusion of chapter 3.

Chapter 3: Research Methodology

3.0. INTRODUCTION

Chapter 2 reviewed a range of literature relating to the topics of the value of privacy, users' online privacy, private browsing and forensics investigation associated with web browsers. In addition, the challenges and issues within the Web Browsing Forensics field have been discussed. The purpose of this chapter is to identify an appropriate research methodology that investigates browsing privacy using the private browsing feature in major browsers. Subsequently, research questions that are derived from this area are identified.

A number of similar studies to the proposed research are reviewed in section 3.1 to learn from the previous researchers' experiences in order to design a research methodology that is appropriate for the context of the proposed research. Six similar research studies are reviewed in order to shape the research design, identify the problem and to formulate relevant questions. In section 3.2 the research design is identified, which consists of the main question and related sub-questions of the research. In section 3.2.2., the research phases are discussed and explained.

Section 3.3 outlines the data requirements for the proposed research, which includes the following sections: testing process, data collection, data processing, and data analysis. This section is important for the proposed research as it enables to identify and plan thoroughly the collection of required data for this research. Section 3.4 introduces the testing environment setup and the scenario that will be followed to conduct the experiment. The chapter is then concluded with section 3.5.

3.1. REVIEW OF SIMILAR RESEARCH

This section reviews similar approaches by other researchers. Six related works are studied, and analysed in order to understand the approaches that have been utilised in order to develop an appropriate methodology for this proposed research.

Private browsing researches have been conducted in different forms either using local machines or virtual machines to test and forensically examine the feature. Said et al. (2011) research was conducted on three local machines, with the aim to investigate the privacy browsing feature on three different web browser vendors in order to develop a better understanding of what, if any, residual data is left behind, and to look at how this could affect digital forensics investigations. Other researchers have justified their use of

Virtual Machines (VM) in testing the privacy feature, stating that their main concern was to prevent cross-examination between experiments which had been done on the different web browsers (Satvat et al, 2014). Mahendrakar, Irving, & Patel (2011) used VM to investigate the private browsing mode and utilised the snapshot feature provided by the VMWare Workstation 6.5 to generate images of the physical memory of each virtual machine, which assisted during analysis of the results.

The testing by Said et al. (2011) was done on the Windows XP Professional Service Pack 2 operating system. One criticism of this method is that as the research was conducted in 2011, Windows 7 would have been a more applicable testing platform as it was becoming more popular at that time. Windows 7 Home Premium was released by Microsoft on October 22, 2009 (Microsoft, 2015).

The hard disk used by Said et al. (2011) was formatted with NTFS. However, formatting a disk to any file system does not ensure that the hard disk has been completely wiped. Formatting a hard disk means deleting the partition table to unlink all the files to the file system, and marking the hard disk as writable space; though files may still reside on the hard disk (Capelli, n.d.; Greene, 2014). This means that data could be forensically recovered using various tools such as Encase, if it has not been overwritten. Therefore, to run the experiments it would be preferable to wipe the hard disk to ensure that no data has been left behind and to perform a standardised experiment over multiple controlled devices, as performed by the researchers Ohana & Shashidhar (2013). The procedure used by Ohana & Shashider (2013) in the testing phase was conducted in a more conventional forensics process to perform a standardised experiment which is precise, completely documented and follows a well detailed plan that is repeatable.

Said et al. (2011) preferred the use of three available websites on the Internet to imitate users' behaviour in real life, while other researchers preferred to create their own website that contained different forms of data (Mahendrakar et al. 2011). The other researchers Mahendrakar et al. (2011) wanted to create a website that would include all the various data forms, such as SSL certificates, text entry forms, password forms, 16MB HTML files, JPEG files, and cookies of different sizes that could be easily traced during the analysis. Both sets of researchers used unique URLs and keywords to enhance the accuracy of the experiment.

When Said et al. (2011) used the private browsing feature on the selected website, an image of the physical memory was taken to analyse the different types of information that could be saved to the memory, such as the web browsing history and cache. This approach was beneficial, as Chivers (2014) stated that useful information could be

retrieved using this approach. However, physical memory is often not captured by forensic experts as it is not often available. In the testing phase, Encase was also utilised by Said et al. (2011), along with other tools, to capture an image of each hard disk used on the three workstations to further examine any artefacts on the hard disk. In addition, open source tools to view the history and cache of different browsers, such as MozillaCacheView, MozillaHistoryView, ChromeCacheView and IECacheView were used in the analysis. These cache viewer tools are capable of retrieving information about the web pages that have been visited and rebuilding them with the information stored in the Internet history file if they have been deleted (Lillard, Garrison, Schiller, & Steele, 2010).

Said et al. (2011) acquired an image of the three workstations, however they did not mention the use of a write blocker in either a software-based or hardware-based form, the use of which is critical during the acquisition phase. Ashcroft, Daniels, & Hart (2004) state that write protection should be used by forensic experts before acquiring an image, as original evidence should be acquired in a protected manner through basic steps to prevent changes in the evidence or alterations to the data, as preserving digital evidence is the most critical aspect in terms of forensics integrity (Ohana & Shashidhar, 2013). Furthermore, hashing, such as the MD5 and SHA1 hashing algorithms, should also be utilised to be certain that the original evidence and the acquired image are identical. This will ensure that they can be presented in civil or law enforcement cases (Ashcroft, Daniels, & Hart, 2004).

Said et al. (2011) first examined the history and cache using open source tools that did not reveal any information about the visited websites during the private browsing session. The open source tools used only recovered records of the browsing in the normal mode. Therefore, the records that could be recovered are limited only to the browsing session mode utilised. The researchers did not only rely on the history and cache viewers to trace the information; they analysed the physical memory using Winhex by searching for strings of the website typed in the private session mode, such as “ani-forensics.com”, “Sindbad”, and “kabamaro”. They found that Mozilla Firefox had several entries in each string search. In addition, Google Chrome retrieved several entries from the physical memory of the visited websites during the private session mode after it had been analysed by Winhex. Internet Explorer also gathered the same results after analysing the physical memory.

Using a variety of tools to extract and analyse the digital evidence is useful to search for the different artefacts that could be left behind in a private session mode. Each

tool has different functionalities in searching and retrieving information and has been designed for different purposes such as acquisition, validation and discrimination, extraction, reconstruction and reporting (Phillips, Godfrey, Steuart, & Brown, 2013). A criminal user, for instance, could change the trace of a particular piece of information on the computer being used to make the investigation of information harder for investigators. In addition, a criminal could overload his/her computer with a wide variety of data to make the analysing phase more complicated for investigators to distinguish between relevant and irrelevant information. Therefore, using a range of forensics tools that are able to search for information is preferable so that an investigator can be certain that he/she searched and analysed all the data being left that could be potential evidence in a legal case (Phillips et al., 2013).

The hard disk image taken by Said et al. (2011) was analysed through Encase version 6.8.1.8 to examine the common folders where the three modern browsers store information about the history and the cache, to search for any traces of information that could be saved or deleted. Researchers Said et al. (2011) examined the slack space and the unallocated space for the three web browser vendors, which revealed the following results:

- Mozilla Firefox – private browsing information saved in the pagefile.sys file
- Google Chrome – no traces found in the test conducted
- Internet Explorer – private browsing information is saved in many areas on the hard disk and is easily reconstructed

Much research has been conducted in the area where web browser vendors claim that private browsing is secure and that information about the session will not be saved on a local machine. However, the results of Said et al.'s (2011) tests revealed that artefacts are able to be recovered. The research performed by Said et al. (2011) had similar findings to that of Ohana & Shashidhar (2013), as the experiments revealed that neither Chrome nor Firefox wrote any data to the file system, while data about the private session in Internet Explorer was able to be recovered. In addition, Malmstrom & Teveldal (2013) examined Internet Explorer version 10 and found that a private browsing session is recoverable, as the Extensible Storage Engine (ESE) database deletes the private session records after the session is ended by the user which exists on the local hard disk until it is overwritten with other data.

Mahendrakar et al. (2011) also examined four modern web browsers: Mozilla Firefox, Internet Explorer, Google Chrome, and Safari. They found that all four browsers

retained information of the private session mode. However, the findings of the testing revealed that Safari retained more information from the private browsing session than other browsers. Noorulla's (2014) research looked at the information that could be left by users after using private mode in four modern web browsers, all of which could be important for investigators during an investigation. The results of their testing revealed a similar finding to that of Said et al. (2011). Internet Explorer versions 8 and 9 had information related to the browsing session and this was able to be recovered even though the database had deleted it, while Safari writes and stores the data to a "WebpageIcons.db" file. Thus, with appropriate tools, forensic experts are able to carve out and reconstruct the data that has been previously deleted.

However, nearly all the research that has been conducted in this area has resulted from the fact that Mozilla Firefox and Google Chrome are the web browsers that write and record the least data on either the hard disk or the physical memory, which could have an impact on an investigation if a criminal is trying to hide his/her browsing activity. These two web browsers are considered the most suitable browsers to surf the Internet privately without the user being worried about leaving traces. Researchers have therefore suggested that experiments in the area of private mode browsing need to be examined further in the areas where information is held, as web browsing activities could be potential evidence in a digital forensics investigation.

3.2. RESEARCH DESIGN

Six similar research studies have been reviewed and analysed in section 3.1 to establish an effective research methodology that can be adopted for the proposed research. The six related studies to the proposed research area are summarised in table 3.1.

Table 3. 1: Summary of the Six Research Studies

Author Methodology	Local Machine	Virtual Machine	Windows OS	Linux OS	Mac OS	IE	Firefox	Chrome	Safari	Created Website	Targeted Websites	HD image	RAM image	Main Tools Used
Mahendrakar et al. (2011)		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> XP			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Memory Parser
Malmstrom & Teveldal (2013)		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 7			<input checked="" type="checkbox"/>					<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Specified Files		ShadowCopy – ESEdatabase view – WinHex – wdsCarve
Noorulla (2014)	Not mentioned		<input checked="" type="checkbox"/> XP,7,8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Belkasoft Ram Capturer, Rekall, Magnet Internet Evidence Finder
Ohana & Shashidhar (2013)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/> 7			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Specified files	<input checked="" type="checkbox"/>	Tableau USB Write Blocker, DaemonFS, Disk Wipe, Nirsoft Internet Tools, AccessData FTK
Said et al. (2011)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/> XP			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	FTK imager, Winhex, Cache and history viewers, Encase
Satvat et al (2014)		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 7			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/> Specified files	<input checked="" type="checkbox"/>	Winhex, Index.dat analyser, SQLite browser, SQLite manager

The proposed research will be conducted with an empirical study using a systematic method to examine and analyse the problem area. The empirical study as defined by the American Psychological Association is a “study based on facts, systematic observation, or experiment, rather than theory or general psychological principle” (American Psychological Association, 2012). The scientific methodologies specifically in computing were developed by analysing the techniques and tools based on the empirical approaches (Santos, Dias, Silva, Ferreira, & Madeira, 2009). Furthermore, the empirical methods are being progressively identified as valuable approaches to any computer based research (Santos et al., 2009).

In the proposed research, the testing scenario was designed to emulate a realistic scenario that could be standardised across multiple controlled environments. Subsequently, a systematic forensics procedure will be conducted on the testing scenario with the use of several current forensics tools to learn what artefacts can be found in a system after browsing in both public and private modes. Photographs of the working area will be taken, forensics images of the seized digital evidence will be created, the procedures will be properly documented, and the seized evidence will be safely preserved. The findings of the experiment conducted will be used to answer the research’s main question. Furthermore, the conducted investigative steps on the experiment will be applied as a guideline for systematic web browsing evaluation.

3.2.1. Research Question

The main research question for the proposed research is generated from the literature review conducted in chapter 2, in addition to the previous studies, their findings, and concerns faced by local law enforcement and corporate forensics agencies relating to Web Browsing Forensics. The private browsing feature is a threat to forensics investigations if it leaves no traces of users’ browsing activity, especially in cases involving web browser forensics. Therefore, the main research question for the proposed research is stated as follows:

Does privacy mode allow users to browse the Internet without leaving any evidence behind?

In order to answer the research question sub-questions have been derived which can be answered accordingly:

Sub-question 1 (SQ1):

What are the browsing artefacts left on Windows 10 after browsing privately using the following browsers Internet Explorer, Google Chrome and Firefox?

Sub-question 2 (SQ2):

What are the browsing artefacts left on Mac OS after browsing privately using the following browsers Safari, Google Chrome and Firefox?

Sub-question 3 (SQ3):

What are the browsing artefacts left on Ubuntu 15.10 after browsing privately using the following browsers Opera,, Google Chrome and Firefox?

3.2.2. Research Phases

The research method and design have been adapted from previous research studies reviewed in section 3.1 and section 3.2. The proposed research is divided into five phases established on the empirical approach. Figure 3.1 illustrates the five phases that will be followed for the research. Phase 1 is a preparation stage which includes setting up the workstations and identifying their features, hardware and software characteristics. It includes wiping the hard drives for each experiment conducted and setting up the Internet connection to perform the next phases. Phase 2 involves progressing through the testing scenario, which aims to generate the data collection for the proposed research. The testing scenario steps are performed to depict as close as possible a real world event.

In Phase 3, a data acquisition stage will be applied to the collected digital evidence using a computer forensics guidance model. In Phase 4, the data acquired from the digital evidence will be examined and analysed in order to extract the evidence generated in Phase 2. Furthermore, a comparison will be performed to compare the leftover information on the local disk after the normal and private browsing sessions have ended.

The research method steps from the preparation phase to phase four will be thoroughly documented. Finally, in Phase 5 a recommended effective approach of initiating an investigation which includes web browsing will be suggested as an approach that should be followed in web browser forensics.

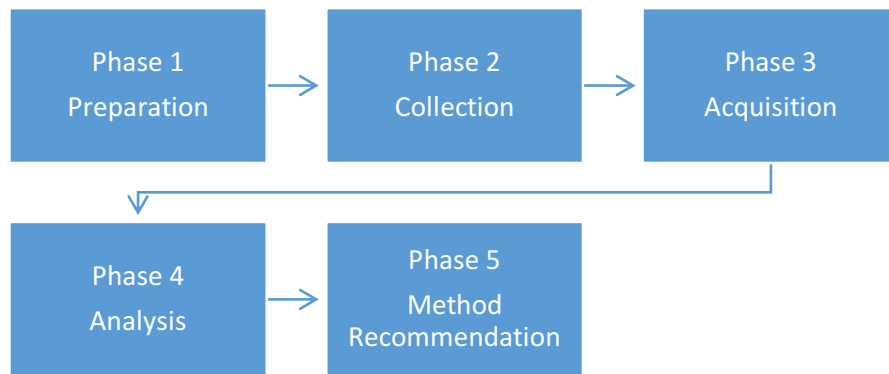


Figure 3. 1: Research Phases

3.3. DATA REQUIREMENTS

Several sources of data are required for the proposed research, including preparation, testing data, extracted data, analysing data, and the documented report of the investigation. The first data requirement is preparation, which consists of the first resource needed in order to begin the experiment. Preparation consists of setting up the workstation by installing the operating systems, Internet browsers, and setting up a non-firewalled network connection to enable normal and private browsing. The next resource is the sample evidence that is generated based on testing steps, which are to portray as closely as possible a real world event. The extracted data from the hard drive images taken are reconstructed, analysed, and recorded in a table to be used as comparative baseline for artefacts left after utilising both browsing modes, public and private. The extracted and reconstructed data will follow the digital forensics guidelines to avoid overlooking any information.

Before the extraction and reconstruction, the data is acquired following the digital forensics framework from the target machine where the testing scenario is performed. Once all the required data has been gathered, a comparative analysis will be performed with the intent of answering the research sub-questions and ultimately the main research question. The experimental case scenario will be recorded in journal form to ensure that the testing steps are repeatable.

3.3.1 Testing Process

The testing will be conducted in a laboratory environment consisting of a network with one desktop and two laptops. Twelve wiped hard disks are utilised to install the three operating systems. Encase version 7 is used to wipe each hard drive to ensure that any previous data is entirely wiped. For each experiment, a fresh operating system will be

installed on the wiped hard disk. The operating systems selected for the proposed research will be installed on a partition of 65GB. Each operating system will be installed on several hard drives to conduct the normal and private browsing individually without conflicting both artefacts. The testing will begin with the normal browsing session using one of the web browser vendors such as IE in Windows 10, the next Internet web browser will be installed to conduct the next testing scenario. After conducting the testing scenario on the three Internet browsers, the operating system will be shut down for acquisition. On the other hand, the private browsing session will be conducted on a single hard drive with the operating system installed which means that there will be one browser installed to test the private browsing artefacts on the local hard disk. The main difference between the normal browsing session and the private browsing session is that the former test all three browsers on one hard disk and then take an image whereas the later each browsers is installed on one hard disk to avoid the evidence being mixed.

The next step after conducting the testing on all browsers will be to acquire the data from the target machine following the appropriate digital forensics procedures by utilising forensics bridges and proper forensics tools to preserve the evidence. Lastly, the original evidence will be preserved and stored in a secure controlled environment. The research testing process is simplified in figure 3.2.

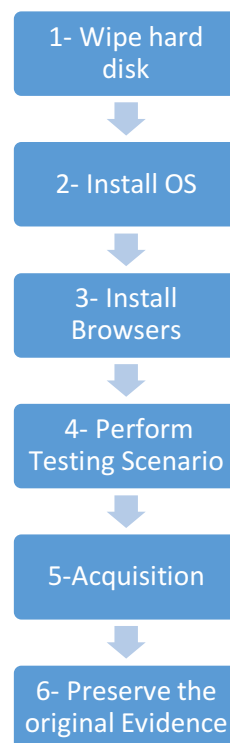


Figure 3. 2: Research Testing Process

3.3.2 Testing Scenario

The testing plan as shown in table 3.2 will be conducted on three operating systems to test how private browsing is secure compared to normal browsing. The most recent operating system will be installed and the latest Internet browsers will be downloaded to test their approaches to storing web browsing artefacts. There will be one unique browser on each operating system as shown in table 3.2; for instance, Windows 10 will have Internet Explorer (IE) as a unique web browser for that OS, while Firefox and Chrome will be used on all three operating systems to test their reliability in leaving no information of browsing activities.

Table 3. 2: Testing Scenario

Operating System	Device Type	Method 1	Method 2	Browser Type	Browser Version
Windows 10 Education	HP Desktop	Browser on Normal Mode	Browse on Private Mode	Internet Explorer	11.103.10586.0
				Firefox	45.0.2
				Chrome	50.0.2661.94
OS X El Captain	MacBook Pro	Browser on Normal Mode	Browse on Private Mode	Safari	9.1
				Firefox	45.0.2
				Chrome	50.0.2661.94
Ubuntu 16.04	HP Laptop	Browser on Normal Mode	Browse on Private Mode	Opera	38.0.2220.41
				Firefox	45.0.2
				Chrome	51.0.2704.106

There will be one scenario to test if information of the browsing activities will remain on the local hard disk of the device. The testing will be conducted through different browsers on different platforms using both normal browsing mode and private browsing mode to compare both modes' results and verify that private browsing leaves no traces of the user's browsing activity.

Once a private browsing session is launched, the same series of steps that is performed on the normal browsing mode is repeated for each browser, such as: searching for articles on hacking, searching for different images and videos, keywords, and logging into different email accounts and sending attachments. The experiment is performed on five social media websites and other common websites such as YouTube, Gmail, Google, Google Maps and Wikipedia to emulate a realistic scenario as much as possible.

The testing will be conducted by using unique URLs and keywords to ensure the accuracy of the test. Table 3.3 illustrates the URLs and keyword searches conducted for the proposed research.

Table 3. 3: Experiment URL and keywords

URLs	Keywords used in search queries
https://www.youtube.com/	Hacking methods (Videos)
https://mail.google.com/	Logs in and sends attachments (Password + Form + Attachment)
https://www.google.co.nz/	Hacking articles (Documents + Texts)
https://www.google.co.nz/maps	55 Wellesley St E, Auckland 1010
https://en.wikipedia.org/wiki/Wik	Hacker (Computer Security)

3.3.3 Data Collection

The collection of data is an important procedure in the proposed research. The data collected from the test scenarios has to be collected in the proper manner and be accurate in order to produce rigorous research. There will be twelve hard disks that will be used to collect data. The data collection will be conducted through the use of accepted forensics frameworks. Tableau Forensics bridges are used to prevent the forensic workstation from writing any information to the acquired digital evidence. The forensic workstation is Windows 7 operating system with the latest version of Encase installed. The hard disks are entirely acquired using Encase version 7.10 to examine the data for analysis. Encase generates the hash value for each hard disk to ensure its integrity.

3.4. WEB BROWSING ENVIRONMENT SETUP & TESTING SCENARIO

The experiments are conducted on three devices as follows. The first experiment was conducted on an HP EliteDesk computer with wired network connection, Intel® Core™ i5-6500 CPU, 3.20GHz, 16 GB RAM and Western Digital 320 GB hard drive. Microsoft Windows 10 64-bit operating system [Version 10.0.10586] was installed on a 65 GB partition to be used for testing. The second experiment was conducted on a MacBook Pro Laptop with Wi-Fi connection, Intel® Core™ i5-3210 CPU, 2.5GHz, 4 GB RAM and Western Digital 320 GB hard drive. OS X El Capitan operating system [Version 10.11.4] was installed on a 65 GB partition to be used for testing. The third experiment was conducted on a HP laptop with Wi-Fi connection, Intel® Core™ i5-4300 CPU, 2.5GHz,

16 GB RAM and Western Digital 320 GB hard drive. Ubuntu 64-bit operating system [Version 16.04] was installed on a 65 GB partition to be used for testing. There was one single scenario that will be followed on all three devices after wiping each 320 GB hard drive using Encase [Version 7.10.03] then installing the latest versions of each operating systems to conduct the experiments. The process of browsing in both modes is shown in figure 3.3.

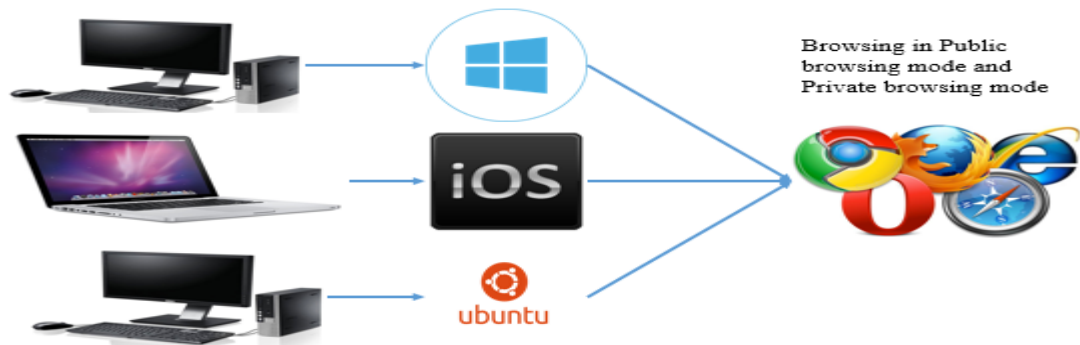


Figure 3. 3: Lab Environment Web Browsing Process

After installing the operating systems, the unique web browsers on each operating system are launched to conduct the tests. After conducting the first scenario on the unique web browser, a USB was plugged in to install the Mozilla Firefox and Google Chrome applications. The two web browsers were launched to conduct the testing on both modes; public and private as previously done with the unique web browser on each operating system. The websites that would be visited during the testing were shown earlier in table 3.3. The browsers used for each operating system and the version installed are illustrated in table 3.2.

3.5. CONCLUSION

Chapter 3 has given an overview of the proposed research framework, which includes the research methodology, research question and sub-questions, research phases, data required for the research as well as the limitations encountered in the research. Similar research studies to this research have been studied and analysed in order to identify suitable methodology that can be used for this research. The studies conducted by previous researchers were reviewed in order to establish the proper research methodology and design. Chapter 4 will report the research findings of the experimental testing scenario gained by applying the defined methodology from this chapter.

Chapter 4: Research Findings and Analysis

4.0. INTRODUCTION

Chapter 3 has established a research framework for investigating the private browsing features on different operating systems and browsing vendors and the procedures taken for digital forensics investigation in this environment. Web browsing forensics has become one of the important sources of forensic evidence due to changes of the browsers' functionality and the different areas where browsing information is stored. Digital forensic experts are required to examine and reconstruct the web browsing activities performed by the subject which can only be done from the forensics evidence left behind by the user.

Similar studies from previous research have been selected to be reviewed and to identify the appropriate research methodology for the research. The main research question and sub-questions have been presented in chapter 3 to identify the challenges that might face forensic investigators during digital forensics investigations involving web browsing. The data requirements for the research experiment were presented and the limitations have been discussed.

The purpose of chapter 4 is to report the analysis and findings of the research phases outlined in chapter 3. Chapter 4 consists of four main sections. Section 4.1 discusses the variations between the proposed research methodology detailed in the previous chapter and the actual testing experiment performed. Section 4.2 presents the digital forensics workstation setup which consists of hardware and software equipment. The findings from the collecting, processing and analysing the data will be presented in section 4.3. Chapter 4 concludes with section 4.4.

4.1. VARIATION ENCOUNTERED

Most of the testing process remained with the test plan, however it was expected that some unforeseen circumstances may be encountered during the actual experiment. The purpose of this section is to report and clarify the changes and variations that were encountered from the planned methodology in chapter 3. The variations encountered in the testing process, testing scenario and the data collection that may affect the outcome of the research findings are explained in the following section.

4.1.1. Testing Process

There were some changes to the hardware equipment that was used to test the normal and privacy browsing mode in Ubuntu 16.04. The initial plan was to use a desktop based computer with Ubuntu 16.04 installed on it. As there were issues in the laboratory environment in connecting the suspect's computer to the Internet, the desktop computer was replaced with an HP laptop which solved the Internet connectivity problem. In addition, the unique web browser that was planned to be tested was the Ubuntu Web browser as it was preinstalled. The Ubuntu web browser had been tested in both browsing modes normal and private. The hard disk was seized and then examined in Encase version 7. The Ubuntu web browser was not recognised in Encase which could affect the research findings; therefore, the web browser was replaced with Opera.

Furthermore, the hardware that was initially planned to be used to conduct the Mac OS examination was the Mac mini. Several digital forensics articles were read suggesting the hard drive not be removed from the case as this may damage the hard drive and the motherboard. In addition, the process of removing the hard drive from a Mac mini is quite difficult. The articles recommend the use of a hard drive docking station or the use of a MacBook laptop when conducting a testing experiment so the proposed research used a MacBook Pro laptop.

The private browsing experiment on all three browsers for each operating system was initially conducted to be tested all at once. Although when analysing the data for the private browsing artefacts it was difficult to determine which browser left the data on the local hard disk. Therefore, each operating system had one installed web browser vendor to test the private browsing activity on the testing scenario specified to be certain of what web browser that left the information on the storage medium of the target machine.

4.1.2. Testing Scenario & Data Collection

The testing scenario on the suspect's computer had no major changes as discussed in section 3.3.2. Similarly with data collection of the suspect's seized evidence there were no major changes to the discussion in section 3.3.3.

4.2. FORENSICS INVESTIGATION ENVIROMENT SETUP

The suspect's environment setup which includes the detailed software and hardware used and the details of the installed web browsers and their versions was discussed in section 3.4. This section discusses the digital forensics investigation environment and the software and hardware prepared for the process of acquiring, examining, analysing and reporting.

The forensic investigator computer is located in a controlled lab environment and equipped with an Intel® Ethernet Connection (2) I219-LM. The computer is an HP EliteDesk Intel® Core™ i5-6500 CPU @ 3.20GHz with 16.0 GB of installed RAM and 500 GB of hard drive storage. A Windows 7 Enterprise operating system with Service Pack 1 was installed on the investigator's machine. The hardware and software equipped with the digital forensic investigator's workstation is shown in table 4.1.

Table 4. 1: Hardware and Software Specifications

Hardware/Software	Version/Model	Purpose
Encase Forensic Software	Version: 7.10.03	Used for acquisition, examination and reporting of the suspect's local hard disk
Tableau eSATA Forensics Bridge	Model: T35es	Digital forensics SATA/IDE bridge used to acquire the suspect's local hard disk in a forensic manner without it being altered or changed
ADATA External hard drive	1 TB size storage compatible with USB 3.0	External hard drive formatted with NTFS file system to store the image files taken of the evidence
Antistatic Wrist Strap	Manufacturer: POSH	Prevents any electrostatic discharge when handling with hard drives
Antistatic Bag	Size: 6 in x 8 in	Used to bag and label the original evidence seized when transferring or after acquiring the evidence
SQLite Viewer	Version 3.8.0	Open source tool used to view the SQLite database files
ESE Database Viewer	Version: 1.41	Open source tool used to view the ESE database files
Irfan View	Version 4.36	To view the image recovered from Encase
16GB USB	Manufacturer: Strontium	Used to store the browser installation file

4.3. DIGITAL FORENSICS

The process of a digital forensics investigation is a critical process that must be conducted by forensic specialists as any mishandling of the digital evidence seized may invalidate it; thus the evidence might not be acceptable in a court of law. The digital forensics process that will be followed in the proposed experimental testing scenario was adapted from the National Institute of Standards and Technology (NIST) discussed in chapter 2. The digital forensics investigation process follows four basic phases: collection of seized evidence, examining the evidence with reliable digital forensics tools, analysis of the resulting evidence and finally reporting the case.

4.3.1. Evaluation and Assessment

- Suspect's devices were powered off when seized
- All three devices' power cords were pulled and sent to the forensics laboratory
- Suspect's hard drives were taken out of the seized devices for acquisition
- Tools needed: Antistatic Wrist Strap to prevent electrostatic discharge (ESD), eSATA to USB connector, Encase 7.10.

4.3.2. Acquisition of Digital Evidence

Each of the suspect's hard drives were acquired using a Tableau eSATA Forensics Bridge that was connected to the digital forensic investigator workstation. The connection of the eSATA Forensics Bridge with the seized hard drive and then with the investigator's machine was conducted by employing the guidelines given in the Ultra Block User Guide. The investigator's workstation had Encase 7.10 which has a feature to acquire forensics images as shown in figure 4.1.



Figure 4. 1: Encase Acquisition

Encase version 7.10 is capable of acquiring different types of evidence such as local devices, network previews, evidence files, raw images, smartphones and crossover

previews. The forensic examiner, as pointed out earlier, connected the hard drive via the Tableau device to the workstation. The hard drive was then connected to the workstation as a local device. Encase acquisition of local devices has an option to detect only Tableau hardware. This option is able to assist the forensic examiner to identify the hard disk connected to the workstation as shown in figure 4.2.

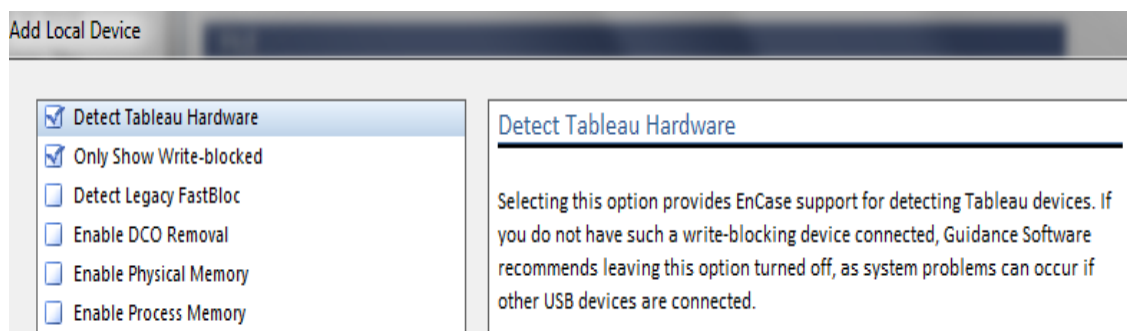


Figure 4. 2: Encase Acquisition Options

A physical image of the connected hard drive was taken and then saved into an external hard drive for all three operating systems Windows 10, Mac OSX and Ubuntu 16.04. The imaged or acquired files from each hard drive has an .E01 extension that is added after the evidence file which is an exact duplicate copy of the seized and acquired hard drives. The integrity of the forensics images was verified with MD5 and SHA1 hash values as shown in Appendix 3. The hard disk acquisition and verification is shown in figure 4.3.



Figure 4. 3: Acquisition & Verification Process of Seized Hard Disk

The forensic examiner summary of the steps taken to acquire the hard drives are as follows:

- Suspect's hard drives were taken out from the seized devices
- Seized hard drives are Western Digital hard drives
 - Model: WD3200LPVX
 - Storage: 320 GB
 - 4 Windows 10 hard drives – one to test the normal browsing mode and 3 hard drives each installed with one browser to test the private browsing feature
 - 4 OS X El Capitan hard drives – one to test the normal browsing mode and 3 hard drives each installed with one browser to test the private browsing feature
 - 4 Ubuntu 16.04 HD hard drives – one to test the normal browsing mode and 3 hard drives each installed with one browser to test the private browsing feature
- Tableau eSATA Forensic Bridge and Encase were used to acquire the hard drives
- Encase images were taken for all seized hard drives

4.3.3. Survey of the Digital Scene

This process is important in order to evaluate the suspect's skill level of competency. The imaged hard drives in section 4.3.2 were mounted in Encase version 7.10 to perform image mounting of the drive with the use of the Block Device/Read Only mode. Each hard disk imaged was examined to find evidence such as stored passwords in common locations. In addition, the browsers used by the suspect as indicated in browser files which were IE, Safari, Opera, Mozilla Firefox and Google Chrome. The evaluation process has indicated that there were not any destructive processes performed on the device data storage and there was no encryption used to secure data. There was one user account found on each hard drive which was an administrator account under the name of each operating system with "Test" at the end such as Windows10Test, ElCapitanTest and Ubuntu16Test. The administrator account found on each hard drive was used to browse in public and private mode on all three browsers. The data recorded on the Application Data files under the users' file of the Windows 10 operating system was 17/04/2016 which was the date when the simulation data for the testing scenario performed (Appendix 1).

4.3.4. Digital Evidence Examination

Once the suspect's technological skill was evaluated, the hard drive evidence files were entered into Encase version 7.10 which is a digital forensics tool for data extraction and data processing. In this process, there was one case file under the name of ENCASE_ACQ_EXAMINATION that had all the evidence files for comparison. Each file within the hard drive evidence files was hashed with MD5 and SHA1 hash values to ensure the integrity of the data while extraction and analysis was conducted. The Internet activity was automatically extracted within the Encase processing. The Encase Record tab had each of the forensics images along with four folders which included Archive, Internet, Thumbnails and Email. The Internet folder is the most critical file to examine as it will reveal the type of browsers the suspect has used. Figure 4.4 reveals that three web browsers had been used by the suspect: Internet Explorer, Mozilla and Chrome.

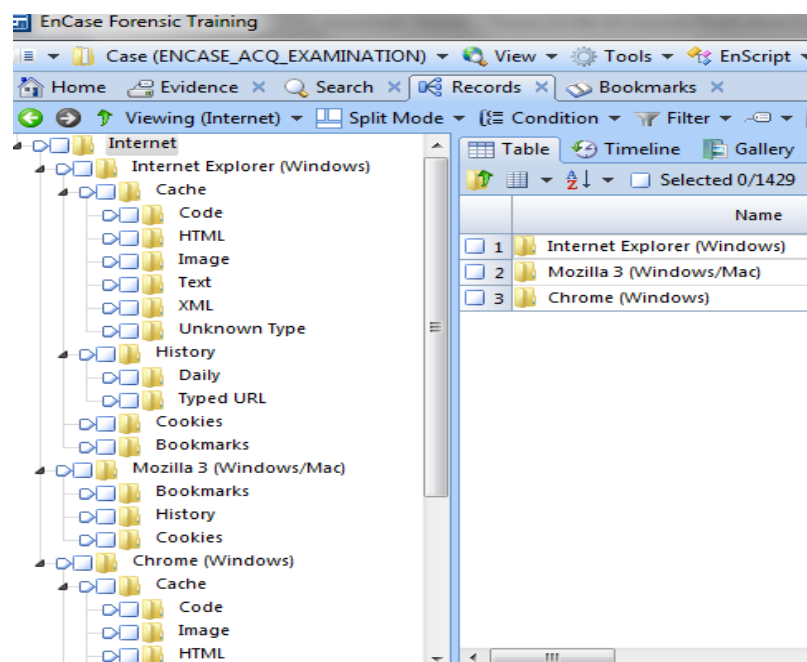


Figure 4.4: Evidence Extracted using Encase Forensic Tool

4.3.5. Locating Windows 10 Browser Artefacts

This section is important for digital forensic examiners as it determines a baseline to identify and locate the area to investigate for files during the normal and private browsing mode. The locations of the web browser artefacts such as the history, cache and cookies in the Windows 10 operating system are shown in Table 4.2.

Table 4. 2: Default locations of the three common web browsers in Windows 10

Default locations of Internet Explorer artefacts in Windows 10	
Artefact	<i>Location within C:\Users\{userhomedir}\AppData\Local\Microsoft\</i>
History	...\Windows\History\
Cache	...\Windows\WebCache\ ...\Windows\Temp...Files\Content.IE5\ ...\Windows\Temp...Files\Low\Content.IE5\
	<i>Location within C:\Users\{user}\AppData\</i>
Cookies	...\Roaming\Microsoft\Windows\Cookies\ ...\LocalLow\Microsoft\Internet Explorer\DOMStore\
Default locations of Mozilla Firefox artefacts in Windows 10	
Artefact	<i>Location within C:\Users\{userhomedir}\AppData\Local\Mozilla\Firefox\Profiles</i>
Cache	...\<randomtext>.default\Cache ...\<randomtext>.default\jumpListCache
	<i>Location within C:\Users\{user}\AppData\Roaming\Mozilla\Firefox\Profiles</i>
Cookies	...\<randomtext>.default\cookies.sqlite
History	& ...\<randomtext>.default\places.sqlite
Bookmarks	
Default locations of Google Chrome artefacts in Windows 10	
Artefact	<i>Location within</i> <i>C:\Users\{userhomedir}\AppData\Local\Google\Chrome\UserData\Default</i>
History	...\History ...\History-journal
Cookies	...\Cookies ...\Cookies-journal
Cache	...\Cache; ...\Favicons; ...\Favicons-journal

4.3.6. Results of Analysing the Windows 10 Operating System

This section discusses the common web browser artefacts left after the suspect browsed on the Windows 10 operating system. The discussion is divided into two sections. The first section which is the Windows 10 normal browsing mode will start analysing the suspect's normal or public browsing activity on the three web browsers. The second section discusses the Windows 10 private browsing on the three web browsers. After the section is concluded a comparison between the browsers is done on both modes, normal and private, to identify the difference between both modes.

4.3.6.1. Windows 10 OS Normal Browsing Mode

The experiment, as pointed out earlier, was started with a Windows operating system on with the use of Internet Explorer as a web browser. The discussion will firstly point out the information extracted and analysed from the three used browsers on normal browsing mode on the Windows 10 operating system. Once the normal browsing discussion is concluded the information extracted from the private browsing on the three web browsers on the Windows 10 OS will be to be analysed. Finally, a comparison chart will be introduced to illustrate the types of the information that could be revealed after browsing privately.

The analysis of Internet Explorer in the normal browsing mode of the acquired hard disk contained different areas where information was found. The evidence found in Encase was located in various areas such as the cache, cookies, typed URLs and history. All the URLs were found with further information such as the times and dates the URL had been visited. Images of the visited websites were identified in the cache folder of Internet Explorer. The cache images are stored on the hard drives for a period of time as discussed in chapter 2. For example, the file favicon[1].ico which is an image stored in the cache, has an expiration date of 25/4/2016 at 7am. Other images stored in the cache were maintained for a lesser period of time.

WebCacheV01.dat database is an Extensible Storage Engine (ESE) database file that replaced the previously file known as index.dat. The forensics examiner used ESEDatabaseView to view the database file for examination and analysis. The tool recovered the cookies that were stored in the database file with further information relating to the creation, modification and expiration time of each cookie as shown in figure 4.5. The browsing activity that was performed by the suspect was all recovered.

CreationTime	ExpiryTime	ModifiedTime	Url	Filename
18/04/2016 8:36:15 p.m.	17/04/2018 8:36:30 p.m.	18/04/2016 8:36:15 p.m.	Cookiewindows10test@bing.com/	ZGROAPFK.txt
18/04/2016 8:36:15 p.m.	17/04/2018 8:36:30 p.m.	18/04/2016 8:36:15 p.m.	Cookiewindows10test@api.bing.com/	7T5D0JJ.txt
17/04/2016 8:36:58 p.m.	17/04/2018 8:36:58 p.m.	17/04/2016 8:36:58 p.m.	Cookiewindows10test@youtube.com/	91170MFL.txt
17/04/2016 8:45:59 p.m.	17/04/2018 8:36:38 p.m.	17/04/2016 8:45:59 p.m.	Cookiewindows10test@doubleclick.net/	Y340LMA3.txt
17/04/2016 8:45:59 p.m.	17/10/2016 9:46:00 p.m.	17/04/2016 8:45:59 p.m.	Cookiewindows10test@google.com/	4Z8ITM07.txt
17/04/2016 8:46:01 p.m.	17/10/2016 9:46:02 p.m.	17/04/2016 8:46:01 p.m.	Cookiewindows10test@google.co.nz/	K7H0DA6L.txt
17/04/2016 8:41:00 p.m.	17/04/2016 8:51:00 p.m.	17/04/2016 8:41:00 p.m.	Cookiewindows10test@www.google.co.nz/	GISV8Y9T.txt
17/04/2016 8:46:01 p.m.	17/04/2018 8:46:02 p.m.	17/04/2016 8:46:01 p.m.	Cookiewindows10test@accounts.google.com/	BHLIOTMX.txt
17/04/2016 8:41:49 p.m.	17/04/2018 8:41:49 p.m.	17/04/2016 8:41:49 p.m.	Cookiewindows10test@www.google.com/intl/en/mail/help/	TKLZT1T9.txt
17/04/2016 8:42:06 p.m.	19/05/2016 12:00:00 p.m.	17/04/2016 8:42:06 p.m.	Cookiewindows10test@www.wikipedia.org/	6/05/1829 11:56:02 a.m.
17/04/2016 8:42:10 p.m.	19/05/2016 12:00:00 p.m.	17/04/2016 8:42:10 p.m.	Cookiewindows10test@en.wikipedia.org/	G1AK0XR8.txt
17/04/2016 8:42:10 p.m.	19/05/2016 12:00:00 p.m.	17/04/2016 8:42:10 p.m.	Cookiewindows10test@upload.wikimedia.org/	VFWHN9YG.txt
17/04/2016 8:42:18 p.m.	19/05/2016 12:00:00 p.m.	17/04/2016 8:42:18 p.m.	Cookiewindows10test@login.wikimedia.org/	N0ISUHT0.txt
17/04/2016 8:45:59 p.m.	27/04/2016 8:42:48 p.m.	17/04/2016 8:45:59 p.m.	Cookiewindows10test@mail.google.com/mail	H9B3PGX0.txt
17/04/2016 8:42:58 p.m.	17/05/2016 8:42:58 p.m.	17/04/2016 8:42:58 p.m.	Cookiewindows10test@apis.google.com/	0JLXFTGP.txt
17/04/2016 8:43:32 p.m.	9/10/2017 8:00:00 p.m.	17/04/2016 8:43:32 p.m.	Cookiewindows10test@google.com/ads	RB93HWY5.txt
17/04/2016 8:43:32 p.m.	9/10/2017 1:00:00 p.m.	17/04/2016 8:43:32 p.m.	Cookiewindows10test@googleadservices.com/	DJXQUHC0.txt
17/04/2016 8:45:59 p.m.	17/04/2018 8:46:00 p.m.	17/04/2016 8:45:59 p.m.	Cookiewindows10test@accounts.youtube.com/accounts	EU6UB8C9.txt
17/04/2016 8:46:00 p.m.	17/04/2018 8:46:01 p.m.	17/04/2016 8:46:00 p.m.	Cookiewindows10test@www.google.com/accounts	E2FR2C7X.txt
17/04/2016 8:46:01 p.m.	17/04/2018 8:46:01 p.m.	17/04/2016 8:46:01 p.m.	Cookiewindows10test@www.google.co.nz/accounts	46KN2C3S.txt
17/04/2016 8:46:02 p.m.	17/04/2016 8:46:12 p.m.	17/04/2016 8:46:02 p.m.	Cookiewindows10test@accounts.youtube.com/accounts/	3QH3H9N.txt

Figure 4. 5: WebCacheV01.dat Database analysis

Encase examination of the Windows 10 Mozilla Firefox (normal browsing mode) revealed that the evidence was stored in two different locations in Encase: history and cookies. Mozilla Firefox had further information related to the title of the URLs visited; for instance when visiting YouTube the suspect has typed hacking methods which were stored in the places.sqlite file. In addition, the address typed in Google Maps and the keyword typed in Wikipedia and Google were all stored in the places.sqlite. Furthermore, the email that the suspect used to send email and documents was identified.

The analysis of the Google Chrome default browsing mode in Encase had more information compared to Internet Explorer and Mozilla Firefox. Evidence was found in different areas in the imaged file such as the cache that identified the video being watched in the video folder and the keyword search in the keyword search folder. Google Chrome caches had stored the most images of the visited webpages. The images are stored for in the caches of Google Chrome. Figure 4.6 presents data_3 file which is a Google Maps cache image that will be kept until the 29/12/2016 at 10:32am.

	Name	
<input type="checkbox"/> 1	() Record Last Acc...	17/04/16 08:53:13 p.m.
<input type="checkbox"/> 2	() Last Modificatio...	17/04/16 08:53:13 p.m.
<input type="checkbox"/> 3	() Reuse Count	0
<input type="checkbox"/> 4	() Refetch Count	0
<input type="checkbox"/> 5	() Entry State	Normal
<input type="checkbox"/> 6	() Url Name	https://www.google.co.nz/maps/v
<input type="checkbox"/> 7	() Url Host	www.google.co.nz/
<input type="checkbox"/> 8	() Http Request Ti...	17/04/16 08:53:13 p.m.
<input type="checkbox"/> 9	() Http Response T...	17/04/16 08:53:13 p.m.
<input type="checkbox"/> 10	() Created	16/04/16 04:42:06 a.m.
<input type="checkbox"/> 11	() Expiry Time	29/12/16 10:32:28 a.m.
<input type="checkbox"/> 12	() Content Type	image/png
<input type="checkbox"/> 13	() Internet Artifact ...	Cache\Image




Figure 4. 6: Google Chrome Cache Extracted from Encase Software

4.3.6.2. Internet Explorer Private Browsing Mode

The Windows 10 operating system with Internet Explorer preinstalled did not reveal any information of the browsing activities in private browsing mode when examined in the records tab of Encase. The WebCacheV01.dat database file was extracted and viewed in the ESE viewer software and there were no URLs related to the private browsing activity. Nor in the cache, the images, the cookies or HTML files was there any sign of private browsing when examined. The forensic image has been further examined in Encase which revealed that private browsing activity was identified in different locations.

The keyword search in Encase software has been useful as it goes throughout the hex of each file and locates any word that could lead to evidence. Thus, the file image was processed to identify any hidden keywords and information related to the testing scenario.

All the URLs typed in Internet Explorer have been identified in different locations and the keywords typed by the suspect were revealed; however the times and dates the private browsing activity was conducted by the suspect cannot be identified for all the URLs as most of the information had been located in unallocated clusters. As discussed in chapter 2, the unallocated clusters record and store data. Table 4.3 identifies the IE private browsing activity for each webpage.

Table 4. 3: Internet Explorer Privacy Mode Evidence

URLs	Keywords used in search queries	Location of the evidence
https://www.youtube.com/	Hacking methods	Unallocated clusters WebCacheV01.dat V01tmp.log Sway.exe
https://www.gmail.com	Logs in and sends a text attachment	Unallocated clusters WebCaheV01.dat V010000B.log V01.log
https://www.google.co.nz/	Hacking terms	Unallocated clusters WebCacheV01.dat V01tmp.log
https://www.google.co.nz/maps	55 Wellesley St E, Auckland 1010	Unallocated clusters WebCacheV01.dat V01tmp.log V010000B.log fISOUE076.txt(deleted file) f6EOI1X0J.txt(deleted file) fV2Z3OO7Y.txt(deleted file) fZOD016T1.txt(deleted file) f6EOI1X0J.txt(deleted file)
https://en.wikipedia.org/wiki/Wik	Hacker (Computer Security)	Unallocated clusters WebCacheV01.dat V01tmp.log V010000B.log \$UsnJrnl-\$J \$LogFile \$MFT UVW46F7M Folder

The most interesting artefact found is that the email the suspect sent to the user “Norah Alomirah” with the email nalomirah@gmail.com has been recorded and stored in the unallocated clusters. The Windows 10 operating system has deleted a file from the system that was recovered later by Encase software with the name of (Package_1517_for_KB3163018~31bf3856ad364e35~amd64~~10.0.1.2.cat) which had also recorded the receiver’s name and email. In addition, the deleted file and the unallocated clusters have recorded what the suspect has written as shown in figure 4.7. The suspect has written the following text in the email (Hi Norah, The document is attached to the following email. Regards, MISDF).

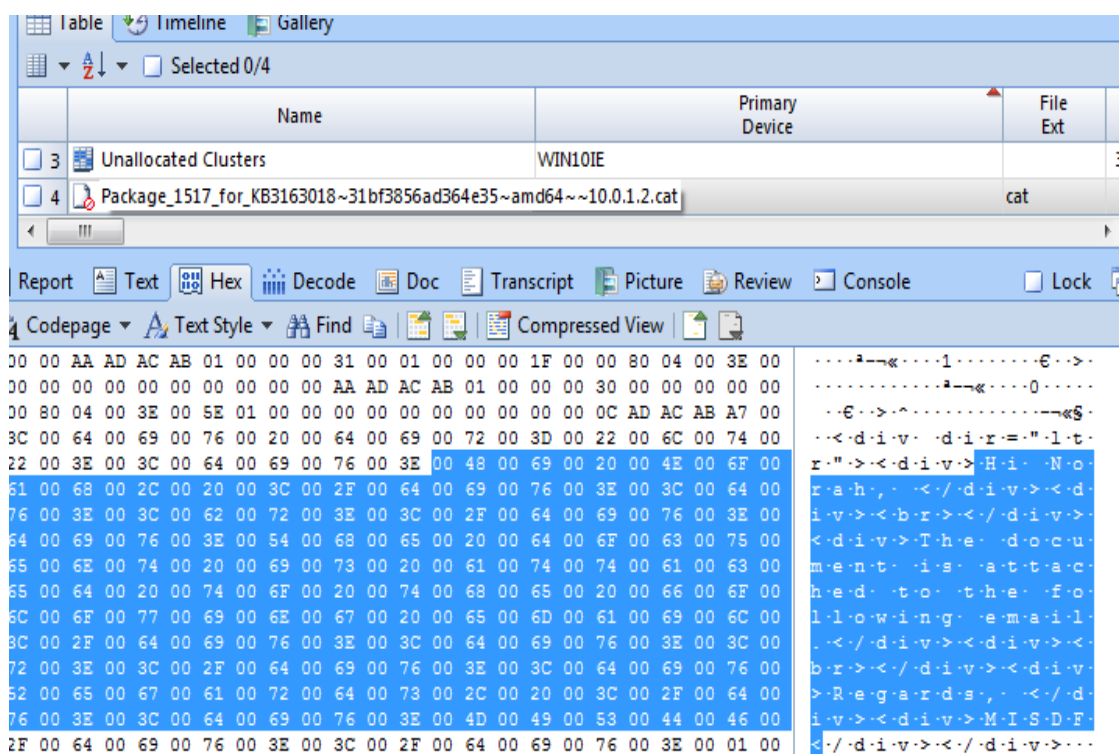


Figure 4. 7: Email Sent by Suspect Recovered in Encase Software

Internet Explorer in the Windows 10 operating system has stored and recorded all the data that the suspect has been using during the private browsing activity. As discussed in section 2.4, Table 2.2, Internet Explorer in Windows operating systems clears, deletes or does not record the private browsing activity. Encase software was able to recover the deleted files and reveal the evidence that was stored in various locations on the hard drive.

4.3.6.3. Mozilla Firefox Private Browsing Mode

The evidence image of the Windows 10 OS with Mozilla Firefox browser installed has been examined through Encase software. The record tab has not revealed any information

compared to the information revealed in the normal browsing mode. The two main files which are places.sqlite and cookies.sqlite where information or evidence could be retrieved did not show any data recorded when examined in Encase and ESE viewer software.

The evidence image has been analysed to reveal hidden browsing artefacts that Encase was not able to detect automatically. A keyword search has been performed to find evidence hidden within the hex file. There were some indications that the URLs had been typed but there is no sign that the user had typed any keywords. The keyword (hacking) has been recovered in Encase software in the hibernation file of the Windows 10 operating system with the use of Firefox as a medium. In addition, the keyword (hacker) has been recovered in the WebCacheV01.dat and hiberfil.sys. The Mozilla Firefox private browsing feature in the Windows 10 operating system had less data stored on the hard drive compared to Internet Explorer. Table 4.4 indicates the location of the potential evidence found in Encase software.

Table 4. 4: Mozilla Firefox Privacy Mode Evidence

URLs	Keywords used in search queries	Location of the evidence
https://www.youtube.com/	Hacking methods	Hiberfil.sys
https://www.gmail.com	Logs in and sends a text attachment	Hiberfil.sys
https://www.google.co.nz/	Hacking terms	Hiberfil.sys
https://www.google.co.nz/maps	55 Wellesley St E, Auckland 1010	Not Identified
https://en.wikipedia.org/wiki/Wik	Hacker (Computer Security)	WebCacheV01.dat

4.3.6.4. Google Chrome Private Browsing Mode

The evidence image of the Windows 10 OS with Google Chrome browser installed has been examined through Encase software. The record tab has not revealed any information compared to the information revealed in the normal browsing mode.

Google Chrome has not revealed as much information as Internet Explorer in the Windows 10 operating system. However, there were some artefacts left in different areas of the suspect's local hard disk. Some indications have been found that the URLs have

been typed. The suspect's email and the receiver's email and name that was written by the suspect was recovered in the hibernation file of the Windows 10 operating system as shown in figure 4.8 where the suspect email (misdftest@gmail.com) and the receiver's email (nalomirah@gmail.com) are recorded in the hibernation file.

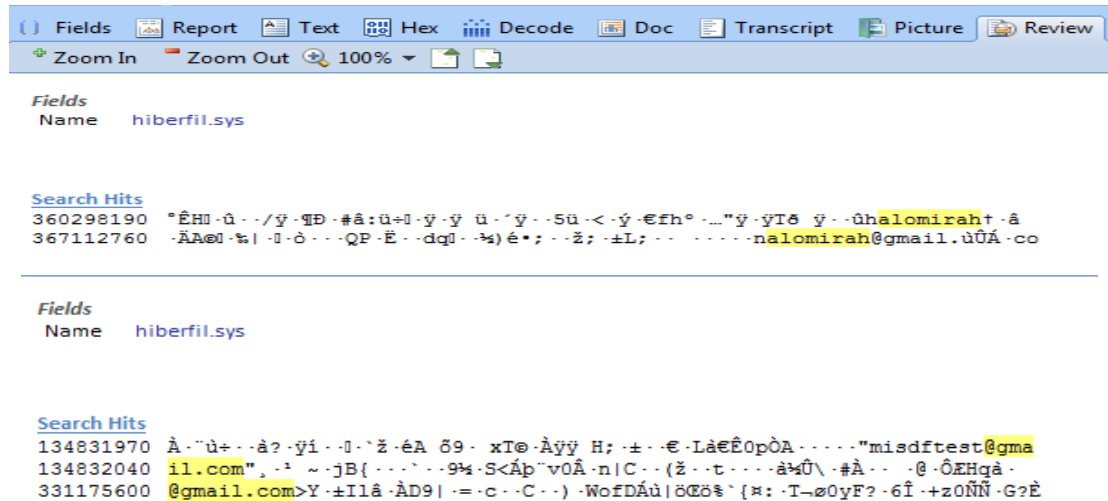


Figure 4. 8: Email Recovered Viewed in Encase

In addition, there was more information extracted when analysing and examining the hard disk of the suspect. The hibernation file had more information than any other file on the suspect's local hard drive as it stores and records data of the activities conducted by the user until the device goes into hibernation mode. Few words from the email sent from the suspect have been recovered in the hibernation file as shown in figure 4.9.

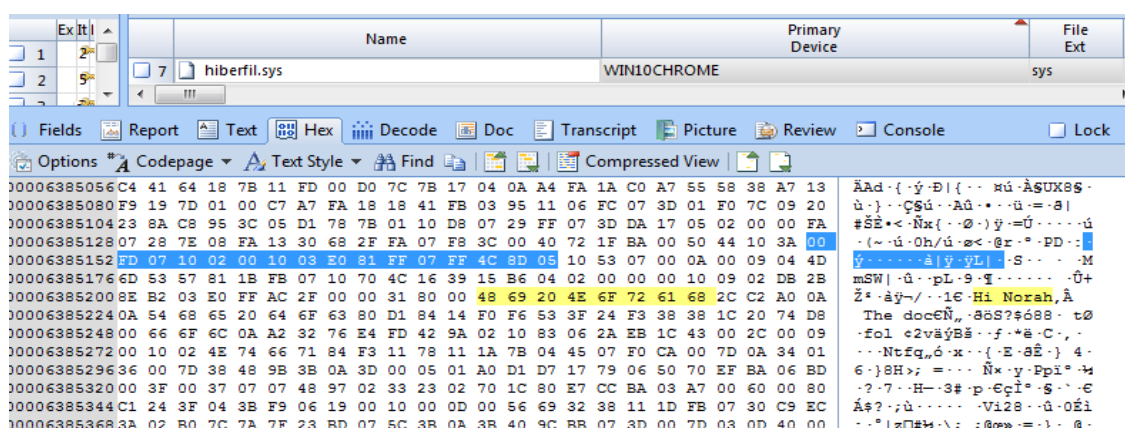


Figure 4. 9: Texts from the Email Sent by the Suspect Viewed in Encase Software

The URLs typed by the suspect and the keywords used to search have been located in different areas on the local hard disk of the suspect. The locations of potential evidence that has been found in Encase software are presented in Table 4.5.

Table 4. 5: Google Chrome Privacy Mode Evidence

URLs	Keywords used in search queries	Location of the evidence
https://www.youtube.com/	Hacking methods	Unallocated clusters – Hiberfil.sys Log File – Sway.exe
https://www.gmail.com	Logs in and sends a text attachment	Hiberfil.sys
https://www.google.co.nz/	Hacking terms	Hiberfile.sys – Data_1
https://www.google.co.nz/maps	55 Wellesley St E, Auckland 1010	Hiberfil.sys
https://en.wikipedia.org/wiki/Wik	Hacker (Computer Security)	Hiberfil.sys

4.3.7. Comparison of Common Web browsers in two modes on Windows OS

This section compares the browsing artefacts found in all three browsers in both browsing modes, private and public. The Internet Explorer normal browsing mode on the Windows 10 operating system has revealed all the browsing artefacts conducted by the suspect with information of the times and dates the website page has been visited. Google Chrome was installed to test the normal browsing activities left by the suspect. Google Chrome has as well revealed all the suspect browsing activity with all the details of the keyword typed in the search bar of the web page and the times and dates the website has been accessed. Finally, Mozilla Firefox has been tested which revealed the normal browsing artefacts conducted by the suspect as resulted with the two previous web browser vendors.

The three web browsers in normal browsing mode have been tested on the Windows 10 operating system. Next the private browsing mode on all thee web browsers is tested. The first web browser to be tested was Internet Explorer where all the information has been found in different locations on the suspect’s local hard disk. The URLs and keywords typed by the suspect have all been identified and recovered from the deleted files.

Google Chrome private browsing mode has revealed some information of the browsing activity conducted such as the suspect emails used to send and receive email messages while Mozilla Firefox has not revealed as much information as was found with

Internet Explorer and Google Chrome. Most of the information of Chrome and Firefox has been found in the hibernation file of the Windows 10 operating system.

Figure 4.10 illustrates the comparison of all three web browser vendors on the Windows 10 operating system in both browsing activity modes. The first bar indicates the three web browser vendors on Windows 10 which resulted in a 100% result of the normal browsing activity on those three web browsers. The following bar is the private browsing artefacts that remained on the suspect's local hard drive. Internet Explorer resulted in 100% due to the fact that all URLs typed by the suspect have been recovered. Google Chrome has indicated some of the information which resulted in 30% of private browsing artefacts left on the suspect's local hard disk. The last bar indicates Mozilla Firefox in private browsing mode where there was a little information related to the browsing activity but there was not any solid evidence found on the local hard disk of the suspect.

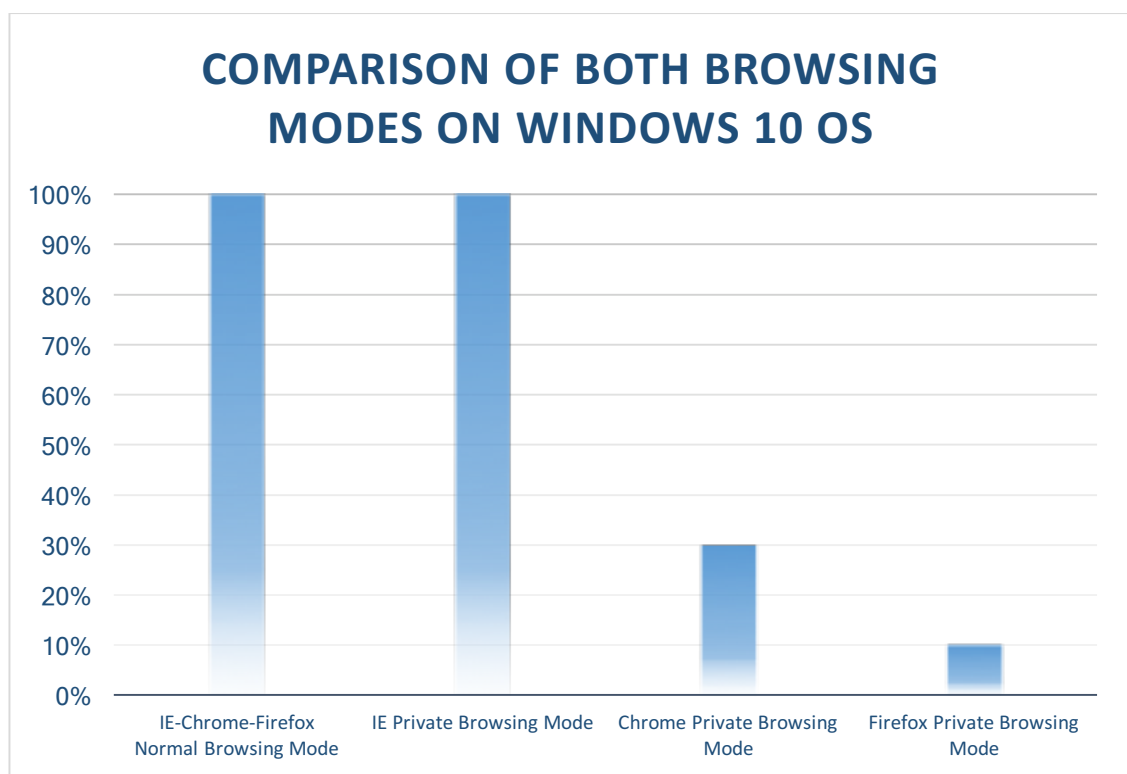


Figure 4. 10: Comparison of Web Browsers Artefacts on Windows 10 OS

4.3.8. Locating Mac OS Browser Artefacts

This section is important for digital forensic examiners as it determines a baseline to identify and locate the area to investigate for files during the normal and private browsing

mode. The location of the web browser artefacts such as the history, cache and cookies in Mac OS X operating system are shown in Table 4.6.

Table 4. 6: Default locations of the three common web browsers in Mac OS X

Default locations of Safari artefacts in Mac OS	
Artefact	
	<i>Location within ~/Users/{userhomedir}/Library/</i>
History	.../Safari/History.plist
History Index	...Safari/HistoryIndex.sk
History Cache	.../Caches/Metadata/Safari/History/*
Cache	.../Caches/com.apple.Safari/Cache.db
Extensions Cache	.../Caches/com.apple.Safari/Extensions/*
Cookies	.../Cookies.binarycookies
Default locations of Mozilla Firefox artefacts in Mac OS	
Artefact	
	<i>Location within ~/Users/{userhomedir}/Library/Application Support/Firefox</i>
Cache	... /Profiles/{profile folder}
Cookies	.../Profiles/{profile folder}/Cookies.sqlite
History	.../Profiles/{profile folder}/Places.sqlite
Form History	.../Profiles/{profile folder}/Formhistory.sqlite
Default locations of Google Chrome artefacts in Mac OS	
Artefact	
	<i>Location within ~/Users/{userhomedir}/Library/Application Support/Google/Chrome/</i>
History	... /{profile folder}/History ... /*/Archived History
Cookies	... /*/Cookies ... /*/Local Storage/*.localstorage
	<i>Location within ~/Users/{userhomedir}/Library/Caches/</i>
Cache	.../com.google.Chrome/Cache.db

4.3.9. Results of Analysing the Mac OS Operating System

This section discusses the common web browser artefacts left after the suspect browsed on the Mac OS operating systems. The discussion is divided into two sections. The first section which is the Mac OS normal browsing mode will begin with analysing the suspect's normal or public browsing activity on three web browsers. The second section discusses the Mac OS private browsing on the three web browsers. After this section is concluded a comparison will be done between the browsers on both modes, normal and private, to locate the difference between the modes.

4.3.9.1. Mac OS Normal Browsing Mode

The experiment was then conducted on the Mac OS operating systems, utilising the OS X series. The web browser Safari was launched to start the normal web browsing activity. The discussion will firstly point out the information extracted and analysed from the three used browsers on normal browsing mode on the EI Captain operating system. Once the normal browsing discussion is concluded, the information extracted from the private browsing on the three web browsers on the EI Captain operating system will be introduced and analysed. Finally, a comparison chart will be used to illustrate the types of information that could be revealed after browsing privately.

The analysis of Safari on the normal browsing mode of the acquired hard disk contained different areas where information was found. The evidence found in Encase was located in various areas such as the cache and history. The record tab in Encase software has not automatically analysed the Safari artefacts compared to analysis of the three web browsers on the Windows 10 operating system; therefore, the safari browser artefacts had to be manually searched in Encase for potential evidence.

All the URLs were found with further information such as the times and dates the URL had been visited. Images of the visited websites have been identified in the cache folder under the WebkitCache. EI Captain stores the cache of each URL accessed in a separate folder as shown in figure 4.11. Google, YouTube and Wikipedia caches have been stored in different folders, each folder containing cache images of the website visited and caches of some of the websites' codes.

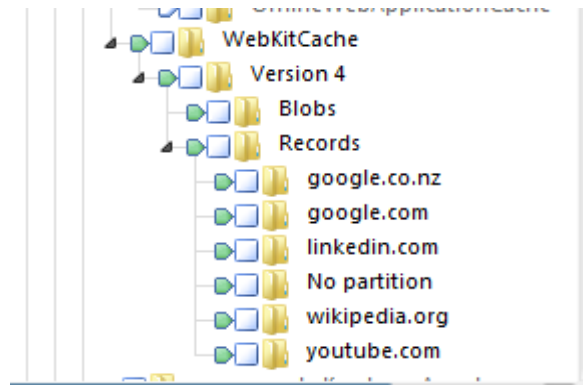


Figure 4. 11: Safari Cache Viewed in Encase Software

The history.db file has been viewed in an SQL viewer to reveal the information that Safari has stored. All the URLs typed and the keywords search are all recorded in this file. In addition, when analysing the evidence file in Encase software, the history folder under Safari has stored the full URLs typed by the suspect. The browsing activity was stored in various locations on the suspect's hard drive.

Encase examination of the Mac OSX-Mozilla Firefox (normal browsing mode) revealed that the evidence was stored in two different locations in the Encase record tab: history and cookies. The history had a file named places.sqlite which stores the visited websites in a SQL database. The places.sqlite has been viewed in the SQL viewer to identify the website visited by the suspect. All the URLs visited, along with the title of each visited page, have been recorded in the moz_places of the places.sqlite database file. There are 36 cookies stored in the cookies.sqlite database file, all of them being from the visited websites. The creation of each cookie, last access of recorded cookie and expiration are all identified in Encase in the Fields tab and in the SQL viewer. The cookies are stored for a period of time identified with an expiration date as shown in figure 4.12.

Database Structure									
Table: moz_cookies									
	id	baseDomain	originAttributes	name	value	host	path		
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	mozilla.org		optimizelyEnd...	oeu14609564...	.mozilla.org	/		2026-04-16 05:13:57
2	5	mozilla.org		optimizelySeg...	%7B%222456...	.mozilla.org	/		2026-04-16 05:13:58
3	6	mozilla.org		optimizelyBuc...	%7B%7D	.mozilla.org	/		2026-04-16 05:13:58
4	9	mozilla.org		_gat_UA-3611...	1	.mozilla.org	/		2016-04-18 05:23:58
5	10	optimizely.com		end_user_id	oeu14609564...	.246059135.log.optimizely.com	/		2026-04-16 05:13:59
6	11	mozilla.org		optimizelyPen...	%5B%5D	.mozilla.org	/		2016-04-18 05:14:14
7	12	mozilla.org		_ga	GA1.2.432091...	.mozilla.org	/		2018-04-18 05:14:01
8	13	youtube.com		VISITOR_INF...	KZ0xBXiosFs	.youtube.com	/		2016-12-17 17:07:14
9	16	doubleclick.net		id	2201aba95b0...	.doubleclick.net	/		2018-04-18 05:14:16
10	17	doubleclick.net		IDE	AHWqTUmSw...	.doubleclick.net	/		2018-04-18 05:14:16
11	18	youtube.com		PREF	f1=50000000...	.youtube.com	/		2018-04-18 05:14:17
12	23	mookie1.com		id	10593732961...	.mookie1.com	/		2016-05-18 05:18:16
13	24	mookie1.com		mdata	1 105937329...	.mookie1.com	/		2016-05-18 05:18:16
14	27	google.co.nz		DV	MspEg-zOBLQ...	.www.google.co.nz	/		2016-04-18 05:29:10
15	28	google.co.nz		OGPC	5061821-2:	.google.co.nz	/		2016-06-17 05:19:14
16	29	wikipedia.org		WMF-Last-Ac...	18-Apr-2016	.www.wikipedia.org	/		2016-05-20 00:00:00
17	30	wikipedia.org		WMF-Last-Ac...	18-Apr-2016	.en.wikipedia.org	/		2016-05-20 00:00:00
18	31	wikimedia.org		WMF-Last-Ac...	18-Apr-2016	.upload.wikimedia.org	/		2016-05-20 00:00:00
19	32	wikimedia.org		WMF-Last-Ac...	18-Apr-2016	.login.wikimedia.org	/		2016-05-20 00:00:00
20	37	google.com		__utmt	1	.www.google.com	/intl/en/mail/...		2016-04-18 05:30:17
21	39	google.com		__utma	145581362.19...	.www.google.com	/intl/en/mail/...		2018-04-18 05:20:19
22	40	google.com		__utmb	145581362.2...	.www.google.com	/intl/en/mail/...		2016-04-18 05:50:19
23	41	google.com		__utmz	145581362.14...	.www.google.com	/intl/en/mail/...		2016-10-17 17:20:19
24	43	youtube.com		CheckConnect...	625515	.accounts.youtube.com	/accounts/		2016-04-18 05:20:30

Figure 4. 12: Mozilla Firefox Cookies.sqlite Database File Viewed in SqliteBrowser

Mozilla Firefox in Mac OS X has stored many images and the URL visited from YouTube, Google, Gmail, Google Maps and Wikipedia in the caches folder. The Mozilla Firefox browser has captured the website page included the keyword that was written by the suspect in all websites entered. The images were stored in the thumbnails folder under the cache of Mozilla Firefox. As shown in figure 4.13 the suspect has entered the YouTube website and typed in the keyword hacking in the search bar. The image was viewed in Irfan view to maximise the image to be make it easily readable.

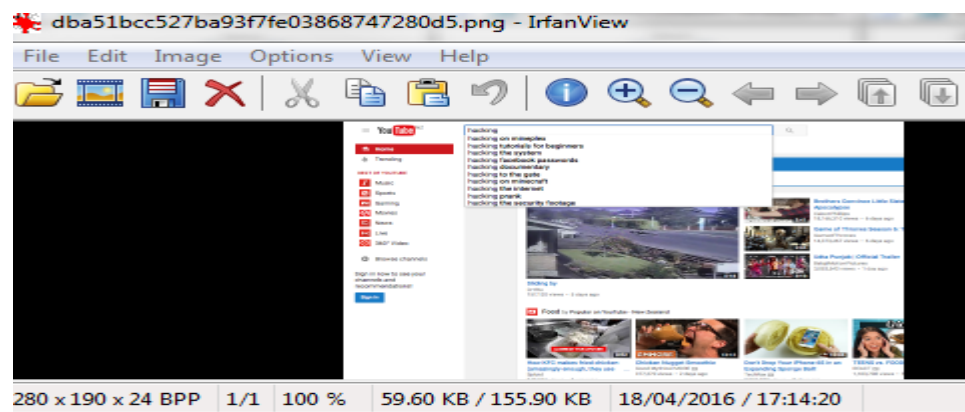


Figure 4. 13: Mozilla Firefox Cached Image Viewed in IrfanView

The analysis of the Google Chrome default browsing mode in Encase had more information compared to Safari and Mozilla Firefox. The record tab of Encase software has revealed many folders such as the cache folder which has subfolders within it, keyword search, history, top sites, cookies and login data. The cache sub folders contained the image folder, code folder, HTML folder, video folder, fonts folder, audio folder, text folder and unknown type folder. Each folder contained the type of the files within it, for instance all the images cached are stored in the image folder. The keyword search folder has the two typed keywords in the search bar of YouTube and Google which were hacking methods and hacking terms. The history file which is a SQLite database file format has been viewed within the file viewer SQL viewer. All the URLs have been identified with the time the file has been accessed, the title of the page and the keywords searched. The cookies were also examined in both tools, Encase and SQL viewer, which stored cookies from the website visited by the suspect. Finally, unallocated clusters of EI Captain OS have stored all the browsing activity and artefacts conducted on all three web browsers.

4.3.9.2. Safari Private Browsing Mode

The Safari private browsing mode in EI Captain OS has not revealed any evidence in the Encase record tab as identified in the normal browsing mode. Even when the history.db has not revealed any information when examined in both tools Encase and SQL viewer. A keyword search has been performed to search for the evidence. The suspect's email (misdftest@gmail.com) has been identified in the unallocated clusters as shown in figure 4.14. There was not any other information stored on the suspect's local hard disk except the suspect's email.

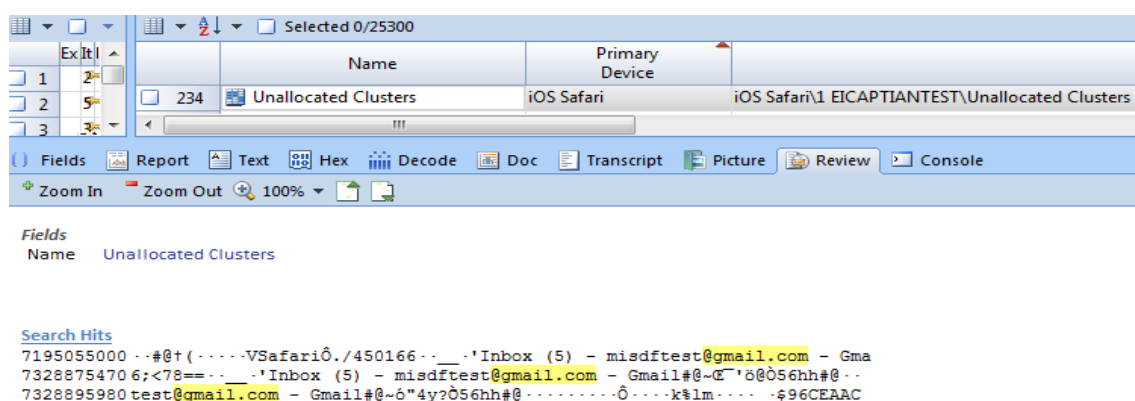


Figure 4. 14: Suspect's Email Viewed in Encase Software

4.3.9.3. Mozilla Firefox Private Browsing Mode

The evidence image of EI Captain with the Mozilla Firefox browser installed has been examined through Encase software. The record tab has not revealed any information compared to the information revealed in the normal browsing mode. The places.sqlite and cookies.sqlite have been also examined in both tools, Encase software and the SQL viewer. There was not any information found in those two files. Firefox revealed no information of the private browsing artefacts when examined in Encase software.

4.3.9.4. Google Chrome Private Browsing Mode

The evidence image of EI Captain OS with Google Chrome browser installed has been examined through Encase software. The record tab has not revealed any information compared to the information revealed in the normal browsing mode. The history and cookies files have been also examined in both tools, Encase software and the SQL viewer. There was not any information found in those two files. Google Chrome in EI Captain

OS has revealed no information of the private browsing artefacts when examined in Encase software.

4.3.10. Comparison of Common Web browsers in two modes on Mac OS X

This section compares the browsing artefacts found in all three browsers in both browsing modes, private and public. The Safari normal browsing mode on the Mac OS X operating system has revealed all the browsing artefacts conducted by the suspect with the times and dates the website page has been visited. Next, Google Chrome was installed to test the normal browsing activities left by the suspect. Google Chrome has as well revealed all the suspect browsing activity with all the details of the keywords typed in the search bar of the web page with the times and dates the website has been accessed. Finally, Mozilla Firefox has been tested which revealed the normal browsing artefacts conducted by the suspect.

As the three web browsers in normal browsing mode have been tested on the Mac OS X operating system, next the private browsing mode on all three web browsers was tested. The first web browser to be tested was Safari where just the suspect's email was recovered. There was no other sign that there was browsing activity conducted. Analysis of Google Chrome and Mozilla Firefox has not revealed any data that has been conducted and stored on the suspect's local hard disk.

Figure 4.15 illustrates the comparison of all three web browser vendors on the Mac OS X operating system in both browsing activity modes. The first bar indicates the three web browser vendors on EI Captain OS which resulted in a 100% result of the normal browsing activity on those three web browsers. The second bar indicates Safari which resulted in 5% due to the fact that the suspect's email was recovered. Google Chrome and Mozilla Firefox has 0% as there was no information recovered when analysed in Encase and other open source tools.

COMPARISON OF BOTH BROWSING MODES ON MAC OS X

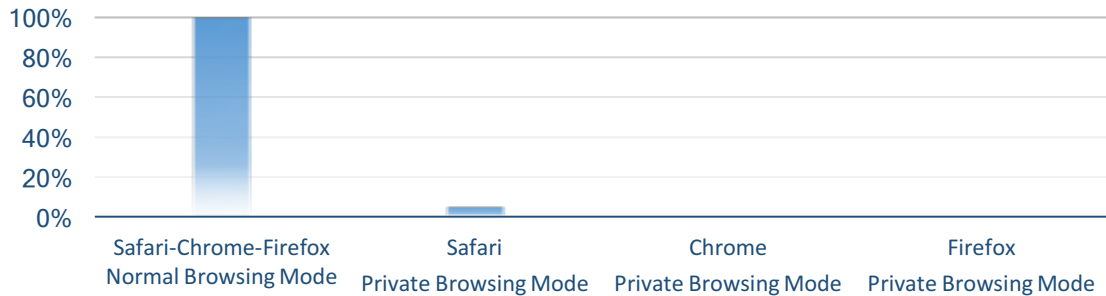


Figure 4. 15: Comparison of Web Browsers Artefacts on Mac OS X

4.3.11. Locating Ubuntu 16 Operating System Browser Artefacts

This section is important for digital forensic examiners as it determines a baseline to identify and locate the area to investigate for files during the normal and private browsing mode. The location of the web browser artefacts such as the history, cache, and cookies in the Ubuntu 16 operating system are shown in table 4.7.

Table 4. 7: Default locations of the three common web browsers in Ubuntu 16

Default locations of Opera artefacts in Ubuntu 16	
Artefact	
	<i>Location within ~/home/{userhomedir}/.config/opera/</i>
History	... /History/
History Provider	.../History Provider Cache/
Cache	
Cookies	... /Cookies/
	<i>Location within ~/home/{userhomedir}/.cache/opera/</i>
Cache	.../Cache/
Default locations of Mozilla Firefox artefacts in Ubuntu 16	
Artefact	
	<i>Location within ~/.config/mozilla/firefox/</i>
Cache	.../<randomtext>.default/Cache

Cookies	.../<randomtext.default>/cookies.sqlite
History	.../<randomtext>.default/places.sqlite
Default locations of Google Chrome artefacts in Ubuntu 16	
Artefact	
	<i>Location within ~/.config/google-chrome/Default</i>
History	.../History .../History-journal
Cookies	.../Cookies .../Cookies-journal
Cache	.../Cache\; .../Favicons; .../Favicons-journal

4.3.12. Results of Analysing the Ubuntu 16 Operating System

This section discusses the common web browser artefacts left after the suspect browsed on the Ubuntu operating system. The discussion is divided into two sections. The first section which is the Ubuntu 16 normal browsing mode will begin by analysing the suspect's normal or public browsing activity on the three web browsers. The second section discusses the Ubuntu private browsing on the three web browsers. After the section is concluded a comparison will be done between the browsers in both modes, normal and private, to locate the difference between the two modes.

4.3.12.1. Ubuntu 16 Normal Browsing Mode

The testing experiment was conducted on Linux operating systems, the Ubuntu 16.04 version. The web browser Opera was launched to start the normal web browsing activity. The discussion will firstly point out the information extracted and analysed from the three browsers on normal browsing mode on the Ubuntu operating system. Once the normal browsing discussion is concluded the information extracted from the private browsing on the three web browsers on Ubuntu operating system will be introduced and analysed. Finally, a comparison chart will be introduced to illustrate the types of information that could be revealed after browsing privately.

The analysis of Opera on the normal browsing mode of the acquired hard disk contained different areas where information was found. The evidence found in Encase was located in various areas such as the cache and history. The record tab in Encase software has not automatically analysed the Opera artefacts. Therefore, Opera browser artefacts had to be manually searched in Encase for potential evidence.

All the URLs have been found with further information such as the times and dates the URLs have been visited. The history database file had all the URLs typed by the suspect when examined in Encase and SQL viewer as shown in figure 4.16. In addition, the history provider cache file, the current session file and favicons database file which were under the Opera file had as well stored all the links typed in by the suspect during the default browsing activity.

id	url	title	visit_count	typed_count
1	http://www.youtube.com/	YouTube	1	1
2	https://www.youtube.com/	YouTube	3	0
3	https://www.youtube.com/results?search_query=hacking+methods	hacking methods - YouTube	2	0
4	https://www.youtube.com/watch?v=Pb6Nd7Ct5XM	Hacking Using HTTP Methods - YouTube	1	0
5	http://www.google.com/	Google	1	1
6	http://www.google.co.nz/7gfe_rd=cr&ei=U1mHV6ikk8nN8gftmbCABQ	Google	1	0
7	https://www.google.co.nz/7gfe_rd=cr&ei=U1mHV6ikk8nN8gftmbCAB...	Google	1	0
8	https://www.google.co.nz/7gfe_rd=cr&ei=U1mHV6ikk8nN8gftmbCAB...	hacking terms - Google Search	1	0
9	https://www.google.co.nz/7gfe_rd=cr&ei=U1mHV6ikk8nN8gftmbCAB...		1	0
10	https://www.google.co.nz/7gfe_rd=cr&ei=U1mHV6ikk8nN8gftmbCAB...		1	0
11	http://www.googlemaps.com/	Google Maps	1	1
12	http://maps.google.com/	Google Maps	1	0
13	http://maps.google.com/maps	Google Maps	1	0
14	http://www.google.com/maps	Google Maps	1	0
15	https://www.google.com/maps	Google Maps	1	0
16	https://www.google.co.nz/maps?source=tliso		2	0
17	https://www.google.co.nz/maps/@-36.8321416,174.7610047,13z	55 Wellesley Street East, Auckland - Google Maps	1	0
18	https://www.google.co.nz/maps/place/55+Wellesley+Street+East,+A...	55 Wellesley St E - Google Maps	1	0
19	https://www.google.co.nz/maps/place/55+Wellesley+St+E,+Auckland...		1	0
20	https://www.google.co.nz/maps/place/55+Wellesley+St+E,+Auckland...		1	0
21	http://www.wikipedia.org/	Wikipedia	1	1
22	https://www.wikipedia.org/	Wikipedia	1	0
23	https://en.wikipedia.org/wiki/Hacker_(computer_security)	Hacker (computer security) - Wikipedia, the free encycl...	1	0
24	http://www.gmail.com/	Gmail	1	1

Figure 4. 16: Opera History Database Viewed in SQL Viewer

After analysing the history database in the SQL viewer the cookies database file was examined to reveal that there were 35 cookies stored on the local hard drive of the suspect. The 35 cookies were all from the visited websites: YouTube, Gmail, Google, Wikipedia and Google Maps. Furthermore, the images of the visited websites have been identified in the cache folder of Opera. The cache has stored the typed links that were written by the suspect.

Encase examination of Mac OSX-Mozilla Firefox (normal browsing mode) revealed that the evidence was stored in two different locations in the Encase record tab which were history and cookies. The history had a file named places.sqlite which stores the visited websites in a SQL database. The places.sqlite has been viewed in the SQL viewer to identify the website visited by the suspect. All the URLs visited along with the title of each visited page have been recorded in the moz_places of the places.sqlite database file. There are 28 cookies stored in the cookies.sqlite database file. The cookies are from the visited websites. The creation of each cookie, last access of recorded cookie and the expiration of all are identified in the Encase in the Fields tab and in the SQL viewer. The cookies are stored for a period of time identified with an expiration date as shown in figure 4.17.

Database Structure Browse Data Edit Pragmas Execute SQL									
Table: moz_cookies									
	id	baseDomain	originAttributes	name	value	host	path	expiry	
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	
1	1	youtube.com		VISITOR_INF...	54AxqeK1WV4	.youtube.com	/	2017-03-14 20:55:39	
2	10	doubleclick.net		id	22cef7147108...	.doubleclick.net	/	2018-07-14 09:02:43	
3	11	doubleclick.net		IDE	AHWqTUnbPT...	.doubleclick.net	/	2018-07-14 09:02:43	
4	16	youtube.com		PREF	f1=50000000...	.youtube.com	/	2018-07-14 09:04:20	
5	17	youtube.com		dkv	c84ef65a1bc7...	.youtube.com	/	2016-10-12 09:04:23	
6	19	google.co.nz		OGPC	5061821-1:	.google.co.nz	/	2016-09-12 09:07:44	
7	20	google.co.nz		DV	0vwxgl58pRof...	www.google....	/	2016-07-14 09:18:05	
8	21	wikipedia.org		WMF-Last-Ac...	14-Jul-2016	www.wikipedi...	/	2016-08-15 00:00:00	
9	22	wikipedia.org		WMF-Last-Ac...	14-Jul-2016	en.wikipedia....	/	2016-08-15 00:00:00	
10	23	wikimedia.org		WMF-Last-Ac...	14-Jul-2016	login.wikimedi...	/	2016-08-15 00:00:00	
11	28	google.com		__utmt	1	.www.google....	/intl/en/mail/...	2016-07-14 09:21:21	
12	30	google.com		__utma	145581362.17...	.www.google....	/intl/en/mail/...	2018-07-14 09:11:23	
13	31	google.com		__utmb	145581362.2....	.www.google....	/intl/en/mail/...	2016-07-14 09:41:23	
14	32	google.com		__utnz	145581362.14...	.www.google....	/intl/en/mail/...	2017-01-12 21:11:23	
15	34	youtube.com		CheckConnect...	655598	accounts.yout...	/accounts/	2016-07-14 09:11:34	
16	36	google.com		S	gmail=L5j9RS...	mail.google.c...	/mail	2016-07-14 10:11:31	
17	37	google.com		COMPASS	gmail=CiQAC...	mail.google.c...	/mail	2016-07-24 09:11:31	
18	39	google.com		RMME	false	accounts.goo...	/	2018-07-14 09:11:50	
19	50	google.com		AID	A3HaeXIaVj_...	.google.com	/ads	2018-01-05 08:00:00	
20	51	googleadservi...		AID	A3HaeXIaVj_...	.googleadservi...	/	2018-01-05 00:00:00	
21	53	google.com		NID	82=E0h_Oa6J...	.google.com	/	2017-01-13 09:13:28	
22	54	youtube.com		GAPS	1:eOb7D3oKR...	accounts.yout...	/accounts	2018-07-14 09:13:29	
23	55	google.com		GMAIL_IMP	v*2%2Fmc-ht...	mail.google.c...	/mail	2016-07-15 09:13:29	
24	56	google.com		GAPS	1:RJaxChjYQy...	www.google....	/accounts	2018-07-14 09:13:29	

Figure 4. 17: Opera Cookies Database Viewed in SQL Viewer

The analysis of the Google Chrome default browsing mode in Encase had more information compared to Safari and Mozilla Firefox. The record tab of the Encase software has revealed many folders such as the cache folder which has subfolders within it: keyword search, history, top sites, cookies and login data. The cache sub folders contained the image folder, code folder, HTML folder, video folder, fonts folder, audio folder, text folder and unknown type folder. Each folder contained the types of the files within it; for instance all the images cached are stored in the image folder. The keyword search folder had the two typed keywords in the search bar of YouTube and Google which were hacking methods and hacking terms. The history file which is a SQLite database file format has been viewed within the file viewer SQL viewer. All the URLs have been identified with the times the file has been accessed, the title of the page and the keywords searched. The cookies were also examined in both tools, Encase and SQL viewer, which stored cookies from the website visited by the suspect. Finally, unallocated clusters of Ubuntu 16.04 have stored all the browsing activity and artefacts conducted on all three web browsers.

4.3.12.2. Ubuntu 16 Private Browsing Mode

There has been no information extracted from the three imaged files of the suspect's local hard disk. Opera, Google Chrome and Mozilla Firefox revealed no information of browsing artefacts conducted by the suspect. There has been no sign that a URL has been typed or any keyword has been searched on all three web browsers.

4.3.13. Comparison of Common Web browsers in two modes on Ubuntu 16 OS

This section compares the browsing artefacts found in all three browsers in both browsing modes, private and public. The Opera normal browsing mode on the Ubuntu 16 operating system has revealed all the browsing artefacts conducted by the suspect with information of the times and dates the website page has been visited. Google Chrome was installed to test the normal browsing activities left by the suspect. Google Chrome has as well revealed all the suspect browsing activity with all the details of the keywords typed in the search bar of the web page with the times and dates the website has been accessed. Finally, Mozilla Firefox has been tested and revealed the normal browsing artefacts conducted by the suspect as resulted with the two previous web browser vendors.

The three web browsers in the normal browsing mode have been tested on the Ubuntu 16 operating system. Next, testing the private browsing mode on all three web browsers was performed. The first web browser to be tested was Opera which revealed no browsing artefacts left on the suspect's local drive. Furthermore, the analysis of Google Chrome and Mozilla Firefox did not reveal any data that had been stored on the suspect's local hard disk.

Figure 4.18 illustrates the comparison chart of all three web browser vendors on the Ubuntu operating system in both browsing activity modes. The first bar indicates the three web browser vendors on Ubuntu 16 which resulted in a 100% result of the normal browsing activity on those three web browsers. The three private browsing bars indicate each web browser vendor had a zero percentage as there was no information recovered when analysed in Encase and other open source tools.

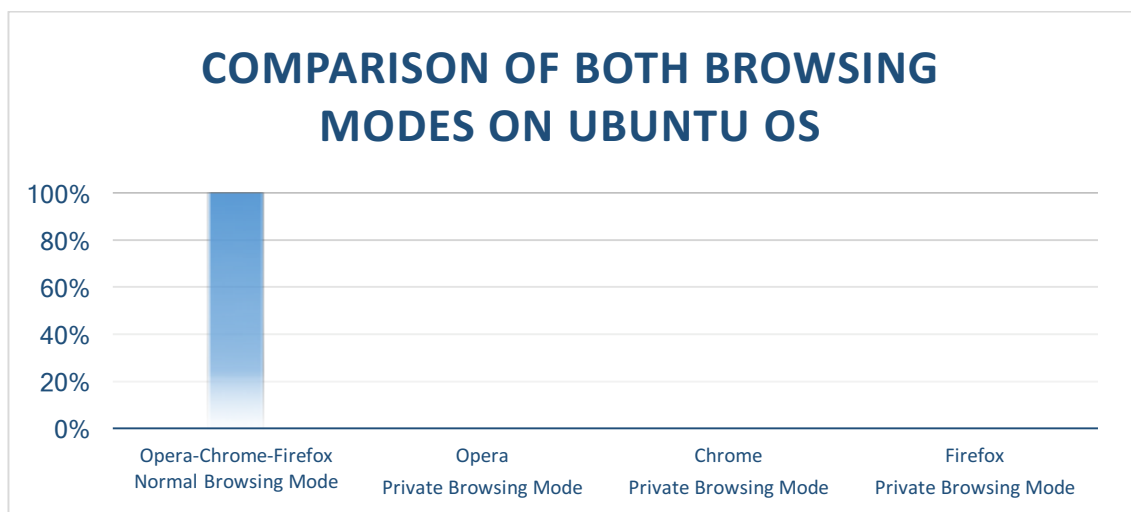


Figure 4. 18: Comparison of Web Browsers Artefacts on Ubuntu OS

4.4. CONCLUSION

Chapter 4 has reported the findings and analyses of three web browser vendors on three different operating systems that were used to find the browsing activities conducted in normal and private browsing mode. The experiment has confirmed that each browser on each operating system has different artefacts stored on the local hard drive of the digital device. The normal browsing mode on all web browsers on different operating systems has stored the browsing activity. The private browsing activity on Internet Explorer in Windows 10 had the most information stored on the hard disk. Google Chrome and Mozilla Firefox had little information stored on the Windows 10 operating system and the Mac OS X. Furthermore, the private browsing activity performed on Ubuntu has revealed no forensic information. A further discussion will be carried out in chapter 5, which will link the research findings to the research question and sub-questions.

Chapter 5: Research Discussion

5.0. INTRODUCTION

Chapter 4 reported the findings of the experiments performed according to the research methodology design established in chapter 3. The findings of the experiment in chapter 4 enabled to answer the research question and sub-questions. The findings of the experiment are then discussed with respect to the theory in chapter 2. The results of the research design in chapter 3 was evaluated and discussed with respect to the experiments performed in chapter 4.

Chapter 5 consists of four main sections. Section 5.1 answers the main research question and the three sub-questions specified in section 3.2.1. The followings; section 5.2 provides a discussion of the findings from the experiments guided by the literature review in chapter 2. Section 5.3 discusses the best practises and recommendations, based on this research to be followed by the digital forensics investigator. The last section, 5.4 contains the conclusions formulated from the discussion.

5.1. ANSWERING THE RESEARCH QUESTIONS

The purpose of this section is to provide a basis for answering the research sub-questions that were established in section 3.2.1 utilising the findings in chapter 4, specifically section 4.3.6, 4.3.9, and 4.3.12. Section 5.1.1 will start by answering the sub-questions according to the evidence collected from the experiment. After answering the sub-questions, the main research question is answered in section 5.1.2.

5.1.1. Answers to Sub-Questions

In order to answer the research main question, there are three sub-questions outlined in section 3.2.1 that need to be answered. The following tables present each sub-question and their associated answers, in table 5.1 to table 5.3.

Table 5. 1: Sub-Question 1 and Answer

Sub-Question (SQ1): What are the browsing artefacts left on Windows 10 after browsing privately using the following browsers; Internet Explorer, Google Chrome and Firefox?
Answer: From the experimental results, Internet Explorer had the most browsing artefacts recorded on the local hard disk of the suspect. Each URL typed by the suspect was identified and recovered in Encase software. The information was stored in different locations. Most of the Internet Explorer private browsing artefacts in Windows 10 OS were found in Unallocated clusters, WebCacheV01.dat, and V01tmp.log. Google Chrome had some information related to the private browsing activity but showed different results from Internet Explorer. The evidence was found in the hibernation file of Windows 10 OS. Mozilla Firefox had the least information stored on the local hard disk of the suspect. The URLs have been stored but there was no sign that the suspect had been searching for anything in particular. The evidence was found in the hibernation file of Windows 10 OS.

Table 5. 2: Sub-Question 2 and Answer

Sub-Question (SQ2): What are the browsing artefacts left on a Mac OS X after browsing privately using the following browsers; Safari, Google Chrome and Firefox?
Answer: From the experimental results, it was noted that Safari stored the suspect's email only for the duration of the private browsing activity in unallocated clusters. Examination and analysis of Google Chrome and Mozilla Firefox has not revealed any information on the local hard disk of the suspect.

Table 5. 3: Sub-Question 3 and Answer

Sub-Question (SQ3): What are the browsing artefacts left on Ubuntu 16.04 after browsing privately using the following browsers; Opera, Google Chrome and Firefox?
Answer: The experimental results revealed that there were no private browsing artefacts from the three web browsers stored on the local hard drive of the suspect when examined by Encase.

5.1.1. The Research Question

This section aims to answer the main research question developed in section 3.2.1. The main research question was:

Does privacy mode allow users to privately browse the Internet without leaving any evidence behind?

The aim of this research is to examine the private browsing mode on different operating systems and web browser vendors to test the web vendors' claims that private browsing activities are not stored or recorded on the local hard drive of the digital device.

Chapter 2 outlines how browsing artefacts are stored on the file system of an operating system and the type of data that is recorded or deleted when browsing privately. In chapter 3, a review of similar research was performed in order to identify similar research carried out in this area and to provide context for the development of the research methodology that follows.

To answer the main research question, the results indicate that each operating system has a different file system to record or store browsing artefacts. Privacy mode on some operating systems allows users to browse the Internet without leaving any evidence behind, while other operating systems store all or some of the private browsing activity performed by the user on the local hard disk of the digital device, demonstrated by the results seen in chapter 4. Therefore, there is no straightforward answer for the research question as it depends on the operating system and web browser used when browsing privately.

Based on the comparison chart in section 4.3.7, 4.3.10, and 4.3.13, Internet Explorer in Windows 10 operating system was the browser that stored all the private browsing artefacts on the local hard drive. Conversely, Opera had no private browsing information

stored on the file system of Linux operating systems. Google Chrome and Mozilla Firefox private browsing artefacts stored on the local disk of the hard disk differ from one operating system to another. For instance, Google Chrome in Windows 10 OS reveals all the information browsed by the suspect in the hibernation file and the other locations referred to in table 4.5. Mozilla Firefox reveals all the URL typed except keywords searched by the suspect, and the address searched in Google Maps. Google Chrome in Mac OS X and Ubuntu 16 did not reveal any of the private browsing activities performed by the suspect.

5.2. DISCUSSION

This section discusses the significant findings of the research which have been investigated and tested in the digital forensics investigation procedure. The investigation of the privacy feature began with setting up the testing environment for each operating system. Both browsing modes have been tested on a single scenario to identify all the artefacts where each file system records and stores. Section 5.2.1 discusses how the environment effected the web forensics investigation. Section 5.2.2 discusses the challenges faced during the private browsing evaluation in the digital forensics investigation which is reflected in the literature review studied in section 2.4. Finally, in section 5.3 recommendations are made as to which procedure and type of web browser forensics approach should be used in similar environments as a guide to digital forensics' examiners.

5.2.1. Discussion of the Case Scenario Environment

The experimental scenario presented in section 3.3.1 and section 3.3.2 has been set up to resemble as close as possible, a real world scenario. The first phase of the testing was to test the normal browsing mode in order to learn where the browsing artefacts are recorded and stored, so evidence from each site can be extracted and then used as forensic evidence. In each testing scenario, the target machine was initially zeroed and then each operating system was installed along with the web browsers identified in table 3.2. The normal browsing mode testing on each browser was tested simultaneously on each operating system. The private browsing mode on each web browser was tested individually on each operating system in order to recognize differentiation between the artefacts. In chapter 3, it is noted that previous research tested the private browsing feature on three well-known web browsers installed on one local hard disk. In the proposed research methodology the

private browsing mode has followed previous researchers which resulted in private browsing artefacts being identified but it was impossible to detect what type of web browser was used. Therefore, the private browsing testing had to be retested by installing each web browser on one local hard disk to be certain of the artefact found for the particular browser being tested.

There was a controlled testing scenario which existed of five typed URLs and keyword searches, required for accurate recording of the time and date that the website was accessed and visited. It was crucial to know what websites were visited in order to be able to show evidence of the visit when was extracted and analysed. Therefore, the investigator is aware of the expected evidence from the forensic image all three operating systems and web browsers, in this testing scenario on all three operating systems and web browsers. For example, when the documented email, sent on all web browsers was performed, Encase recovered some of the email details for Firefox and Google Chrome but not all the expected evidence was extracted.

The literature reviewed in chapter 2, section 2.3 discussed the private browsing mode in depth which primarily aims at prohibiting any data being recorded and stored on the local disk. Google Chrome has claimed that there will be no data stored related to private browsing activity. This was proven incorrect by the results of the experimental scenario. Furthermore, Internet Explorer developers ensured that data relating to browser history such as, temporary Internet files, form data, cookies and usernames are prevented from being stored. All web browser vendors have claimed that their browsing feature is secure and will not store any of the activities conducted during the session on the local hard disk. By way of the experimental environment set up, it was discovered that each browser had all or some information stored on the local disk which ultimately depends on the operating system where the browser is installed. Information related to the private browsing feature was mostly extracted from the hibernation file or unallocated clusters which could be overwritten over a period of time. In addition, not all the private browsing evidence expected to be recovered was stored in the local hard disk. Thus, sometimes live memory forensics may assist the investigator to obtain recent web browsing artefacts that may not be extracted in the target's local hard disk.

The scenarios in the research experiment were set up in three environments Windows 10, Mac El Captain, and Ubuntu 16. The private browsing feature activity was performed using Internet Explorer, Safari, Opera, Google Chrome, and Mozilla Firefox. In a genuine environment, the operating system and the Internet browser encountered by a digital examiner may be different then these tested, therefore the location of private

browsing artefacts in the system may also be different. The simulated research environments were able to highlight the importance of web browser forensics, specifically the private browsing feature in the digital forensics investigations procedure. All testing showed that, in general, when private browsing activity is performed, the target system would likely contain some type of private browsing artefacts.

5.2.2. Discussion on Data Acquisition and Analysis

The data acquisition and analysis conducted in Phase 3 and Phase 4 of the research used reliable digital forensics tools to acquire and extract the relevant evidence according to the evaluation of the testing scenario. The experimental scenario was intended to evaluate investigative procedures for the private browsing feature involved in web browsers. Therefore, the target's medium was acquired, extracted and analysed with regard to web browser forensics. Best practice was applied as discussed in the literature review in section 2.5.

The target hard disk was the only evidence acquired for the proposed research, which had little information related to the following web browsers, Google Chrome, Mozilla Firefox, Safari and Opera. The evidence images taken were acquired, examined and analysed in Encase version 7.10. However, other digital forensics tools have been used in this process to further examine the evidence files. Belkasoft Evidence Center is a digital forensics tool that is used to search, analyse, store and share digital forensics evidence found on digital devices. The tool was installed as a full functionality trial version on the digital forensic investigator's workstation with a time limitation of 30 days. The evidence files were loaded into Belkasoft to be further examined and analysed to reveal more information about the evidence found. Normal browsing activity was detected but there was no information related to the private browsing activity for all the forensic image files. Encase software was the most effective forensics tool in this case to examine and recover the deleted private browsing artefacts as it was able to detect potential evidence by indexing and keyword searching. Furthermore, it was able to recover the deleted files which in this instance, Internet Explorer had deleted when searching for a specific location on Google Maps.

Further examination has been undertaken in Belkasoft utilising the data carving option by selecting the data type to be carved particularly browsers and email services. This tool carves information found in allocated and unallocated space by default, yet there

were no data extracted from the tool regarding the private browsing activity from all the browsers.

Belkasoft was not the only tool tested. Magnet Internet Evidence Finder (IEF) was also tested. Magnet IEF recovered some of the experimental scenario of private browsing artefacts related to Internet Explorer on Windows 10. The Magnet IEF forensics tool was used to recover the private browsing artefacts from common web browsers. It was recommended to browse for several hours to capture the live RAM which contains information on the private browsing session, as suggested by Magnet support specialists. Therefore, with more time spent investigating private browsing it is expected that more data would be found stored on the local disk of the target machine

5.3. RECOMMENDATION FOR WEB BROWSER FORENSICS

This section aims to propose possible recommendations and best practice to provide guidance for digital forensic investigators in cases involving web browser forensics. The research was focused on analysing the private browsing feature that was added to many web browsers recently.

Firstly, the research was conducted in a controlled environment with particular operating systems and web browsers. As operating systems and web browsers are regularly updated it is recommended to test the recent updated operating system and web browser as there could be a difference in the way information is recorded and stored on the target machine. For instance, in section 2.4.1, where browsing storage areas have been discussed, Internet Explorer specifically, stored the browsing artefacts in a file called 'index.dat' which was later replaced with 'WebCacheV01.dat' in Internet Explorer 10 in August 2012. Thus, it is recommended that digital forensic expert have knowledge of the changes occurring on the storage areas of web browsers on each operating system in order to properly examine the target machine for potential evidence.

Secondly, the research examined the suspect's local hard disk to reveal potential evidence. The testing of the private browsing feature on different web browsers and operating systems proposed in this research has not found the expected outcomes. As seen in the results of previous research, reviewed in section 3.1, the outcomes of their research has indicated that nearly all private browsing artefacts, especially Google Chrome and Mozilla, are indicated. This is due to the fact that some researchers did not rely only on imaging the hard disk of the suspect's device but also taking an image of the RAM

From a digital forensics perspective, it is recommended that information should be looked for in different areas. For instance, if the digital device was powered on during

the collection of digital evidence it is recommended to acquire the RAM as there may be evidence related to recent activities conducted by the user, such as passwords, browsing activities, or some other sensitive data (Lai, Gu, Jin, Wang, & Li, 2011). Therefore, for digital forensics investigations related to web browsing forensics it is advisable to image different sources for examination and analysis.

Encase Forensic Software, produced by Guidance Software, was the main tool used to acquire, extract and analyse the suspect's local disk. In addition, it was the only tool capable of detecting files where potential evidence related to the private browsing activity, conducted by the suspect. From a digital forensics perspective, a forensic examiner should not rely on a single forensics tool to examine the evidence image when possible (Hayes, 2014). Each digital forensics software has different features. Some might be more comprehensive, and provide more value than other tools. It depends in the end on the requirements of the examiner. In addition, one forensics tool may be insufficient to attend to all requirements and may need support from other tools. Furthermore, having more than one digital forensics tool as an investigator, enables cross-validation between the findings of one tool and another. Tools previously used were not able to extract the expected results. These tools, it was claimed, were able to detect private browsing activity by relying on the image of the local hard disk. It is, however recommended that an image of the RAM is also imaged to detect the private browsing artefacts.

5.4. CONCLUSION

This chapter has discussed the research findings according to the research experiment results presented in chapter 4. It is not straightforward to answer to the main research question as the results of the private browsing session have identified that each operating system and web browser differs in the way of recording or storing the data on the local hard disk. The main aim of the research was to determine whether or not private browsing activities are able to be detected on the hard drive. All the sub-questions formulated in chapter 3 have been discussed and answered based on the findings as shown in section 4.3.6, 4.3.9 and 4.3.12.

Subsequently, the difficulties encountered during the proposed research were outlined in section 5.2.1. The relative success of the methodology used as well as its shortcomings and improvements were also examined in detail. In addition, the challenges faced when acquiring and examining the hard disk have been highlighted. In section 5.2.3, recommendations were presented which focused on improving the performance and scope of the investigation procedures for web browser forensics. Chapter 6, concludes the

thesis by summarising the research findings. The limitations, recommendations and potential future research will be discussed in order to provide a link for further research in the field of web browser forensics.

Chapter 6: Research Conclusion

6.0. INTRODUCTION

This chapter concludes the thesis and presents a final conclusion based on the research findings in chapter 4 and the discussion in chapter 5. The research limitations and future challenges are briefly discussed. In addition, the limitations identified in the current research are presented as this indicates opportunities for future research that could assist in further developing the field of web browser forensics.

Chapter 6 presents a summary of the research and the research findings in section 6.1. The limitations of the research and the experiments that occurred are summarised in section 6.2. The recommendations raised in chapter 5 will be summarised for future research, based on the testing environment. Future research related to area will be delivered in section 6.3.

6.1. SUMMARY OF RESEARCH

In this thesis, chapter 1 introduced the research topic and the motivations behind conducting this type of research. In chapter 2, the literature review surrounding the research area was reviewed providing an opportunity to expand the understanding on the area of the research. Chapter 3, the methodology chapter, primarily evaluated and selected the best possible methodology, and expanded on the research design which was developed after reviewing previous research methods presented in this area of study. Chapter 4, outlined the results of forensically investigating the private browsing mode on several web browsers and operating systems. Chapter 5 discussed the findings after examining and analysing the forensics images in regards to the private browsing artefacts that were stored in the local hard disk.

The main consideration of this research was the private browsing mode implemented on many web browsers. Private browsing is a feature that is added to many well-known browsers these days, such as Internet Explorer, Google Chrome, Mozilla Firefox and many more, to secure the users' browsing activity on the Internet. The feature, as claimed by web browser vendors, is that it will not save the history of browsing, cookies, passwords or any keyword searches. The feature is a form of 'security through obscurity' in security speak. It, however is also provides a form of security for the execution of nefarious deeds where the user is able to hide his/her digital footprints without being

identified by law enforcement or relevant authorities. This threat has raised awareness of the digital forensic investigators to investigate and identify private browsing artefacts.

The research consisted of five phases, starting with preparation of the environment, collection of the evidence, acquiring the digital evidence, analysing forensics images for potential evidence, and finally recommending a basic guideline that could be followed by web browser forensic investigators. The three most popular operating systems and six well-known web browsers were installed in order to identify the private browsing artefacts that could be stored on the local hard disk of the target machine as shown in figure 3.3. The experimental testing followed a single testing scenario which consisted of five websites that involved watching a video, reading articles, sending an email or browsing the Internet as presented in table 3.3. As testing progressed there were some minor modifications and changes to the experimental scenario that were discussed in section 4.1. The acquisition phase was conducted in a recommended forensics procedure which involved the use of a forensics bridge to prevent the investigator's forensics workstation from altering or modifying the original evidence. The forensics images were acquired using Encase Forensic Software which were then saved on external hard disks for examination and analysis. The forensics tool used to examine and analyse the forensics images was Encase Forensic Software. Research found that Encase Forensic Software is better than other digital forensics tools in this area based on the experimental results. Encase was able to recover some of the private browsing artefacts deleted by the operating system.

The results of the research phases were reported in chapter 4. The three operating systems with the installed browsers had different private browsing artefacts recovered from the local hard disk of the suspect. Internet Explorer on Windows 10 operating system had the most browsing artefacts saved at different locations on the local hard disk. Linux on the other hand had none of the private browsing artefacts recorded or stored on the local hard disk of the suspect machine. Mac OS X had few items of information related to the private browsing activity conducted on Safari, Mozilla Firefox and Google Chrome. Private browsing artefacts on Windows 10 operating system and Mac OS X varied as in the former examples there was information indicating that private browsing had been performed and the latter had no information related to the private browsing activity. Thus, the findings have answered the main research question; that private browsing artefacts are able to be recovered depending on the operating system used and the web browser as each web browser has a different process of recording and storing the data on the local hard disk. Some web browsers do not store any information related to the private

browsing activity performed by users while other browsers save all the private browsing activity. In addition, the private browsing activity is recoverable depending on the digital forensics tool used. Not all digital forensics tools are capable of recovering the browsing artefacts. Thus, the digital forensics tools assessed in the evaluation require further improvements in order to reliably detect the private browsing activity conducted on the local hard disk.

A comparative analysis of each operating system with the installed browser was performed in chapter 5. The objective of the comparative analysis was to identify the ability of forensics tools in recovering the private browsing activity from the local hard disk of the target machine. In addition, the study recognises the difficulties that could face the forensic investigator when examining cases involving web browser forensics. As the seized evidence must be admissible in court.

Ultimately, after employing the best practices and a suitable methodology during the research phases, recommendations have been presented to assist digital forensic investigators in cases involving web browser forensics especially private browsing.

6.2. LIMITATIONS OF RESEARCH

The purpose of this study was to investigate the possibility of locating and extracting evidence from a local hard disk after a user has used the private browsing feature. Although the test bench was setup and experiments were successfully conducted there were some limitations identified, which are presented in this section.

The limitations indicate that the experiments are limited to specific versions of operating systems and web browser vendors as there are many more web browsers which offer the private browsing feature that have not been tested in this research. The operating systems used in the experiments are limited to one desktop-based operating system, an HP laptop, and a MacBook pro with the latest version release for each operating system at the time of conducting the experiments. The forensics investigation methods may differ with other operating systems such as Android and BlackBerry which are designed primarily for smartphones and tablets. In addition, the type of digital devices used may have a different way of storing information. Furthermore, there are different versions and updates of each operating system, which means that the file structure of systems could differ compared to the operating system versions used for the experimental testing.

Similarly, the web browsers used for the experimental case are limited to five well-known browsers with the latest version released for each operating system. There are many different web browsers available that are not considered in this research. These

include Flock, Avant, Maxthon, Netscape and others. The web browsers all have different versions and updates to secure users' browsing activity. For example, the Tor Browser, which was developed with the aim of secure web page browsing. As web browser vendors are developing and improving their security measures, the likelihood that these browsers will be used to conduct suspicious activities without the risk of leaving evidence may increase. This in turn may make the process of digital forensics investigation even more challenging.

Thirdly, there are many digital forensics tools that could be used during the digital forensics process of collecting, examining, analysing and reporting of evidence. The chosen tools for the proposed research are selected based on their reputation and availability. The tools are capable of acquiring the evidence, examining the hard drives, and extracting and analysing the evidence from the web browser artefacts and files. The main selected tool was Encase software for this research, along with other open source tools used to view images and SQL databases. Other digital forensics tools were not selected and tested due to the time constraints of this particular research. It is simply not possible in limited time to test all the digital forensics tools available in this type of study.

The investigation techniques used in the proposed research are limited to a shutdown system during the seizure of the hard disk which means that live forensics and network forensics are not included. In addition, the hard disk was the only original seized evidence from the experimental testing scenario, so memory imaging was not conducted. The research suggests conducting further similar research on memory forensics as this would likely provide valuable forensics evidence.

6.3. FUTURE RESEARCH

In this research project, Windows, Ubuntu, and Mac OS X were the operating systems used to install three web browsers on each operating systems. The unique web browsers on each operating system were Internet Explorer on Windows 10 OS, Opera on Ubuntu, and Safari on EI Captain in addition to Google Chrome and Mozilla Firefox that were installed on all three operating systems. For future research, other operating systems versions could be tested such as Debian, Fedora, Sun OS and the latest version of Windows. Similarly with the web browsers used in the study further research could be carried out in this area to investigate the private browsing feature on web browsers such as Microsoft Edge and Tor Browser. In addition, as mobile devices are adopted more by users, so browsers have been specifically developed to operate on them. Thus, for further

research in the area, investigating those specific browsers in private mode on mobile devices would contribute to web browser forensics knowledge.

Future research in this field may include further hard disk experiments and more efficient approaches to extract the relevant data. This would be particularly interesting and possibly valuable if the private browsing feature was used over an extended period of time. As suggested by Magnet Internet Evidence Finder, browsing privately for hours could reveal some of the private browsing activity.

As the proposed research has only acquired the local hard disk of the target machine, acquiring an image of the RAM when conducting the experiment would bring value to the area as there could be more information stored in the memory. Most results of the findings of previous research indicate that information related to the private browsing activity is stored in the RAM, specifically the pagefile.sys.

Furthermore, digital forensics tools or improved carving techniques may need to be developed to provide more assistance to digital forensics investigations involving web browser forensics cases. This would bring more value if the digital forensics tools is able to distinguish if the webpage has been accessed using the normal browsing mode or the private browsing mode when carving the data for examination and analysis. In this research, Encase Software was the only tool that was able to detect the private browsing activity conducted on different browsers and operating systems. Further research could be performed on testing common privacy erasing software such as Privacy Eraser developed by Cybertron Software to investigate if the tool would in fact clean all private browsing activity related to a session as is claimed. This is true of other similar software that could also be tested to see if vendors' claims of complete privacy are in fact achieved.

REFERENCES

- Acquisti, A., Gritzalis, S., Lambrinoudakis, C., & di Vimercati, S. (2007). *Digital privacy: theory, technologies, and practices*: CRC Press.
- Aggarwal, G., Bursztein, E., Jackson, C., & Boneh, D. (2010). *An Analysis of Private Browsing Modes in Modern Browsers*. Paper presented at the USENIX Security Symposium.
- Alharbi, S., Weber-Jahnke, J., & Traore, I. (2011). *The proactive and reactive digital forensics investigation process: A systematic literature review*. Paper presented at the International Conference on Information Security and Assurance.
- Allmer, T. (2015). *Critical Theory and Social Media: Between Emancipation and Commodification* (Vol. 144): Routledge.
- Altheide, C., & Carvey, H. (2011). *Digital Forensics with Open Source Tools*: Elsevier Science.
- Anderson, J. J. (2011). *Wikipedia: The Company and Its Founders*: ABDO Publishing Company.
- Anderson Ross, J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*: Willey, Hoboken.
- Apple. (2015). Safari 8 (Yosemite): Use Private Browsing windows. Retrieved 20 August 2016, from https://support.apple.com/kb/PH19216?locale=en_US
- Banks, M. J. (2008). Moving to the Net *On the Way to the Web: The Secret History of the Internet and its Founders* (pp. 157-175). Berkeley, CA: Apress.
- Bidgoli, H. (2006). *Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations*: Wiley.
- Bocij, P. (2004). *Cyberstalking: Harassment in the Internet Age and how to Protect Your Family*: Praeger.
- Bunting, S., & Wei, W. (2006). *EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide*: Wiley.
- Cady, G. H., & McGregor, P. (2001). *Protect your digital privacy: Survival skills for the Information Age*: Que Publishing.
- Camenisch, J., Leenes, R., & Sommer, D. (2011). *Digital Privacy: PRIME - Privacy and Identity Management for Europe*: Springer.
- Carrier, B. D. (2009). Digital forensics works. *IEEE Security & Privacy*, 2(7), 26-29. doi:10.1109/MSP.2009.35
- Cherry, D. (2013). *The Basics of Digital Privacy: Simple Tools to Protect Your Personal Information and Your Identity Online*: Syngress.

- Cohen-Almagor, R. (2011). Internet History. *International Journal of Technoethics*(2(2)), 45-64. doi: 10.4018/jte.2011040104
- Cox, M., Mulder, E., & Tadic, L. (2006). *Descriptive Metadata for Television: An End-to-end Introduction*: Focal Press.
- Danesh, A., Lau, F., & Mehrassa, A. (2002). *Safe and Secure: Secure Your Home Network, and Protect Your Privacy Online*: Sams.
- EC-Council. (2009). *Computer Forensics: Investigating Network Intrusions and Cyber Crime*: Cengage Learning.
- Flegel, U. (2007). *Privacy-Respecting Intrusion Detection*: Springer US.
- Frackman, A., Martin, R. C., & Ray, C. (2002). *Internet and Online Privacy: A Legal and Business Guide*: ALM Publishing.
- Friedewald, M., & Pohoryles, R. J. (2016). *Privacy and Security in the Digital Age: Privacy in the Age of Super-Technologies*: Taylor & Francis.
- Gao, X., Yang, Y., Fu, H., Lindqvist, J., & Wang, Y. (2014). *Private browsing: An inquiry on usability and privacy protection*. Paper presented at the Proceedings of the 13th Workshop on Privacy in the Electronic Society.
- Gellman, R., & Dixon, P. (2011). *Online Privacy: A Reference Handbook*: ABC-CLIO.
- Girard, J. E. (2013). *Criminalistics: Forensic Science, Crime, and Terrorism*: Jones & Bartlett Learning, LLC.
- Gogolin, G. (2012). *Digital Forensics Explained*: CRC Press.
- Google. (2016). *Browse in private with incognito mode*. Retrieved 20 August 2016, from <https://support.google.com/chrome/answer/95464?hl=en>
- Government of Ontario. (2015). *The legal and privacy issues of doing E-business*. Retrieved from http://www.onebusiness.ca/sites/default/files/MEDI_Booklet_Legal_Privacy_Issues_accessible_E.pdf.
- Gunnarsson, A., & Ekberg, S. (2003). *Invasion of Privacy: Spam - one result of bad privacy protection*. Retrieved from <http://www.mimersbrunn.se/article?id=50658>
- Harvell, B. (2013). *iConnected: Use AirPlay, iCloud, Apps, and More to Bring Your Apple Devices Together*: Wiley.
- Hayes, D. R. (2014). *A Practical Guide to Computer Forensics Investigations*: Pearson Education.
- Internet Live Stats. (2015). *Total number of Websites*. Retrieved 20 August 2016, from <http://www.internetlivestats.com/total-number-of-websites/#trend>

- Jacobson, D., & Idziorek, J. (2016). *Computer Security Literacy: Staying Safe in a Digital World*: CRC Press.
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>
- Kohn, M., Eloff, J., & Olivier, M. (2006). Framework for a digital forensic investigation. *Proceedings of the ISSA 2006 from Insight to Foresight Conference*. Retrieved from http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/101_Paper.pdf
- Lai, X., Gu, D., Jin, B., Wang, Y., & Li, H. (2011). *Forensics in Telecommunications, Information and Multimedia: Third International ICST Conference, e-Forensics 2010, Shanghai, China, November 11-12, 2010, Revised Selected Papers* (Vol. 56): Springer.
- Laud, P. (2012). *Information Security Technology for Applications: 16th Nordic Conference on Security IT Systems, NordSec 2011, Tallinn, Estonia, 26-28 October 2011, Revised Selected Papers* (Vol. 7161): Springer.
- Lerner, B. S., Elbert, L., Poole, N., & Krishnamurthi, S. (2013). *Verifying Web Browser Extensions' Compliance with Private-Browsing Mode*. Paper presented at the Computer Security--ESORICS 2013: 18th European Symposium on Research in Computer Security, Egham, UK, September 9-13, 2013, Proceedings.
- Liska, A. (2014). *Building an Intelligence-Led Security Program*: Elsevier Science.
- McPherson, S. S. (2009). *Tim Berners-Lee: Inventor of the World Wide Web*: Lerner Publishing Group.
- Microsoft. (2016). *Internet Explorer 9 features*. Retrieved 20 August 2016, from <http://windows.microsoft.com/en-NZ/internet-explorer/products/ie-9/features/in-private>
- Miller, R. L. R., & Cross, F. B. (2012). *The Legal Environment Today: Business In Its Ethical, Regulatory, E-Commerce, and Global Setting*: Cengage Learning.
- Miller, R. L. R., & Jentz, G. A. (2011). *Business Law Today: Comprehensive: Text and Cases*: Cengage Learning.
- Montasari, R., & Peltola, P. (2015). *Computer Forensic Analysis of Private Browsing Modes*. Paper presented at the International Conference on Global Security, Safety, and Sustainability.
- New Zealand Government. (2015). *National Plan to Address Cybercrime*. Retrieved from <http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-cybercrime-plan-december-2015.pdf>.
- New Zealand Police. (2009). *Electronic crime strategy, to 2010 policing with confidence*. Retrieved from <https://www.police.govt.nz/resources/2007/e-crime-strategy/e-crime-strategy.pdf>

- New Zealand Police. (2015). *Electronic crime – what it is and how to report it*. Retrieved from <http://www.police.govt.nz/advice/email-and-internet-safety/electronic-crime>.
- Oppedisano, R. (2011). *Internet*: Infobase Publishing
- Palmer, G. (2001). *A Road Map for Digital Forensic Research*. Report from the First Digital Forensic Research Workshop: DFRWS Technical Report, DTR-T001-01 FINAL, Air Force Research Laboratory, Rome, New York.
- Parsons, J. J. (2015). *New Perspectives on Computer Concepts 2016, Introductory*: Cengage Learning.
- Payton, T., Claypoole, T., & Schmidt, H. H. A. (2014). *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*: Rowman & Littlefield Publishers.
- Poole, H. W., Lambert, L., Woodford, C., & Moschovitis, C. J. (2005). *The Internet: a historical encyclopedia* (Vol. 1): Abc-Clio Inc.
- Sadhya, D., & Verma, S. (2015). Privacy Preservation in Information Systems *Encyclopedia of Information Science and Technology* (Vol. Third Edition, pp. 4393-4402).
- Salinger, L. M. (2013). *Encyclopedia of White-Collar and Corporate Crime*: SAGE Publications.
- Satvat, K., Forshaw, M., Hao, F., & Toreini, E. (2014). On the privacy of private browsing – a forensic approach *Data Privacy Management and Autonomous Spontaneous Security* (pp. 380-389): Springer.
- Schneider, G., Evans, J., & Pinard, K. T. (2009). *The Internet - Illustrated*. Boston, US: Cengage Learning.
- Schneier, B. (2011). *Secrets and Lies: Digital Security in a Networked World*: Wiley.
- Schwartz, M., & Kleinrock, L. (2010). History of communications: an early history of the internet. *IEEE Communications Magazine*, 48(8), 26-36. doi: 10.1109/MCOM.2010.5534584.
- Selfe, C. L., & Hawisher, G. E. (2004). *Literate Lives in the Information Age: Narratives of Literacy From the United States*: Taylor & Francis.
- Shah, D. N. (2009). *A Complete Guide To Internet And Web Programming*: Dreamtech Press.
- Shavers, B., & Zimmerman, E. (2013). *X-Ways Forensics Practitioner's Guide*: Newnes.
- Sklar, J. (2014). *Principles of Web Design: The Web Warrior Series*: Cengage Learning.
- Soe Yu, M. (2015). Security and Privacy on Personalized Multi-Agent System. In K.-P. Mehdi (Ed.), *Encyclopedia of Information Science and Technology, Third Edition* (pp. 5741-5753). Hershey, PA, USA: IGI Global.

- Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security*: Yale University Press.
- Song, Z., Jin, B., Zhu, Y., & Sun, Y. (2011). Investigating the Implications of Virtualization for Digital Forensics. In X. Lai, D. Gu, B. Jin, Y. Wang, & H. Li (Eds.), *Forensics in Telecommunications, Information, and Multimedia: Third International ICST Conference, e-Forensics 2010*, (pp. 110-121). Springer Berlin Heidelberg. doi:10.1007/978-3-642-23602-0_10.
- Stanger, J., & Grayson, A. (2006). *CIW Server Administration Study Guide: Exam 1D0-450*: Wiley.
- Steel, C. M. S. (2014). *Digital Child Pornography: A Practical Guide for Investigators*: Lily Shiba Press.
- Trepte, S., & Reinecke, L. (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social web*: Springer Science & Business Media.
- TRUSTe. (2015). TRUSTe 2015 Consumer Confidence Privacy Index
- Vacca, J. R., & Rudolph, K. (2010). *System Forensics, Investigation, and Response*: Jones & Bartlett Learning.
- Van den Hoven, J., & Weckert, J. (2008). *Information Technology and Moral Philosophy*: Cambridge University Press.
- Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, 4(5).
- Yeager, N. J., & McGrath, R. E. (1996). *Web Server Technology: The Advanced Guide for World Wide Web Information Providers*: Morgan Kaufmann Publishers.
- Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology (IJCSIT)*, 3(3), 17-31.
- Zainudin, N., Merabti, M., & Llewellyn-Jones, D. (2011). Online social networks as supporting evidence: A digital forensic investigation model and its application design. *International Conference on Research and Innovation in Information System (ICRIIS)*, 1-6. doi: 10.1109/ICRIIS.2011.6125728
- Zalewski, M. (2012). *The tangled Web: A guide to securing modern web applications*: No Starch Press.

APPENDICES

Appendix 1 – Normal Browsing Mode Testing Scenario on three Operating Systems

Windows 10 Education OS Internet Explorer Normal Browsing Mode		
Event #	Date/Time	Action
1.	17 April 2016 at 8:36pm	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	17 April 2016 at 8:36pm	Watch the whole video with the title (Best Method to Hack Facebook!!!!)
3.	17 April 2016 at 8:40pm	Type in the address bar: www.google.com & search for (Hacking Terms) in the search bar and view the first 3 pages
4.	17 April 2016 at 8:41pm	Type in the address bar: www.googlemaps.com & search for the following address: 55 Wellesley St E, Auckland, 1024
5.	17 April 2016 at 8:42pm	Type in the address bar: www.wikipedia.org & search for (Hacker (computer security)) in the search bar
6.	17 April 2016 at 8:42pm	Type in the address bar: www.gmail.com & login to misdftest@gmail.com
7.	17 April 2016 at 8:45pm	Send an email to nalomirah@gmail.com with a text file
8.	17 April 2016 at 8:46pm	Close the browser

Windows 10 Education OS Google Chrome Normal Browsing Mode		
Event #	Date/Time	Action
1.	17 April 2016 at 8:48pm	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	17 April 2016 at 8:48pm	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	17 April 2016 at 8:52pm	Type in the address bar: www.google.com
4.	17 April 2016 at 8:52pm	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	17 April 2016 at 8:53pm	Type in the address bar: www.googlemaps.com
6.	17 April 2016 at 8:53pm	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	17 April 2016 at 8:54pm	Type in the address bar: www.wikipedia.org
8.	17 April 2016 at 8:54pm	Type in the search bar (Hacker (computer security))
9.	17 April 2016 at 8:55pm	Type in the address bar: www.gmail.com
10.	17 April 2016 at 8:55pm	Send an email to nalomirah@gmail.com with a text file
11.	17 April 2016 at 8:56pm	Close the browser

Windows 10 Education OS Mozilla Firefox Normal Browsing Mode					
Event #	Date/Time				Action
1.	17	April	2016	at	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	17	April	2016	at	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	17	April	2016	at	Type in the address bar: www.google.com
4.	17	April	2016	at	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	17	April	2016	at	Type in the address bar: www.googlemaps.com
6.	17	April	2016	at	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	17	April	2016	at	Type in the address bar: www.wikipedia.org
8.	17	April	2016	at	Type in the search bar (Hacker (computer security))
9.	17	April	2016	at	Type in the address bar: www.gmail.com
10.	17	April	2016	at	Send an email to nalomirah@gmail.com with a text file
11.	17	April	2016	at	Close the browser

Mac OS X (EI Captain) Safari Normal Browsing Mode					
Event #	Date/Time				Action
1.	18	April	2016	at	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	18	April	2016	at	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	18	April	2016	at	Type in the address bar: www.google.com
4.	18	April	2016	at	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	18	April	2016	at	Type in the address bar: www.googlemaps.com
6.	18	April	2016	at	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	18	April	2016	at	Type in the address bar: www.wikipedia.org
8.	18	April	2016	at	Type in the search bar (Hacker (computer security))
9.	18	April	2016	at	Type in the address bar: www.gmail.com
10.	18	April	2016	at	Send an email to nalomirah@gmail.com with a text file
11.	18	April	2016	at	Close the browser

Mac OS X (EI Captain) Google Chrome Normal Browsing Mode					
Event #	Date/Time				Action
1.	18	April	2016	at	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	18	April	2016	at	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	18	April	2016	at	Type in the address bar: www.google.com
4.	18	April	2016	at	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	18	April	2016	at	Type in the address bar: www.googlemaps.com
6.	18	April	2016	at	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	18	April	2016	at	Type in the address bar: www.wikipedia.org
8.	18	April	2016	at	Type in the search bar (Hacker (computer security))
9.	18	April	2016	at	Type in the address bar: www.gmail.com
10.	18	April	2016	at	Send an email to nalomirah@gmail.com with a text file
11.	18	April	2016	at	Close the browser

Mac OS X (EI Captain)					
Mozilla Firefox Normal Browsing Mode					
Event #	Date/Time				Action
1.	18	April	2016	at	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	18	April	2016	at	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	18	April	2016	at	Type in the address bar: www.google.com
4.	18	April	2016	at	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	18	April	2016	at	Type in the address bar: www.googlemaps.com
6.	18	April	2016	at	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	18	April	2016	at	Type in the address bar: www.wikipedia.org
8.	18	April	2016	at	Type in the search bar (Hacker (computer security))
9.	18	April	2016	at	Type in the address bar: www.gmail.com
10.	18	April	2016	at	Send an email to nalomirah@gmail.com with a text file
11.	18	April	2016	at	Close the browser

Ubuntu 16.04 Mozilla Firefox Normal Browsing Mode				
Event #	Date/Time			Action
1.	14	July	2016 at 9:02pm	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	14	July	2016 at 9:02pm	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	14	July	2016 at 9:07pm	Type in the address bar: www.google.com
4.	14	July	2016 at 9:08pm	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	14	July	2016 at 9:08pm	Type in the address bar: www.googlemaps.com
6.	14	July	2016 at 9:09pm	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	14	July	2016 at 9:09pm	Type in the address bar: www.wikipedia.org
8.	14	July	2016 at 9:11pm	Type in the search bar (Hacker (computer security))
9.	14	July	2016 at 9:11pm	Type in the address bar: www.gmail.com
10.	14	July	2016 at 9:13pm	Send an email to nalomirah@gmail.com with a text file
11.	14	July	2016 at 9:14pm	Close the browser

Ubuntu 16.04 Opera Normal Browsing Mode				
Event #	Date/Time			Action
1.	14	July	2016 at 9:17pm	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	14	July	2016 at 9:17pm	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	14	July	2016 at 9:20pm	Type in the address bar: www.google.com
4.	14	July	2016 at 9:21pm	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	14	July	2016 at 9:21pm	Type in the address bar: www.googlemaps.com
6.	14	July	2016 at 9:22pm	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	14	July	2016 at 9:22pm	Type in the address bar: www.wikipedia.org
8.	14	July	2016 at 9:23pm	Type in the search bar (Hacker (computer security))
9.	14	July	2016 at 9:23pm	Type in the address bar: www.gmail.com
10.	14	July	2016 at 9:25pm	Send an email to nalomirah@gmail.com with a text file
11.	14	July	2016 at 9:26pm	Close the browser

Ubuntu 16.04 Google Chrome Normal Browsing Mode				
Event #	Date/Time			Action
1.	14	July	2016 at 9:32pm	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	14	July	2016 at 9:33pm	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	14	July	2016 at 9:36pm	Type in the address bar: www.google.com
4.	14	July	2016 at 9:37pm	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	14	July	2016 at 9:37pm	Type in the address bar: www.googlemaps.com
6.	14	July	2016 at 9:38pm	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	14	July	2016 at 9:38pm	Type in the address bar: www.wikipedia.org
8.	14	July	2016 at 9:39pm	Type in the search bar (Hacker (computer security))
9.	14	July	2016 at 9:39pm	Type in the address bar: www.gmail.com
10.	14	July	2016 at 9:42pm	Send an email to nalomirah@gmail.com with a text file
11.	14	July	2016 at 9:43pm	Close the browser

Appendix 2 – Private Browsing Mode Testing Scenario on Three Operating Systems

Windows 10 Education OS Internet Explorer Private Browsing Mode				
Event #	Date/Time			Action
1.	29 June 2016	at	11:42am	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	29 June 2016	at	11:42am	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	29 June 2016	at	11:46am	Type in the address bar: www.google.com
4.	29 June 2016	at	11:46am	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	29 June 2016	at	11:47am	Type in the address bar: www.googlemaps.com
6.	29 June 2016	at	11:47am	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	29 June 2016	at	11:48am	Type in the address bar: www.wikipedia.org
8.	29 June 2016	at	11:49am	Type in the search bar (Hacker (computer security))
9.	29 June 2016	at	11:50am	Type in the address bar: www.gmail.com
10.	29 June 2016	at	11:52am	Send an email to nalomirah@gmail.com with a text file
11.	29 June 2016	at	11:53am	Close the browser

Windows 10 Education OS Google Chrome Private Browsing Mode				
Event #	Date/Time			Action
1.	29 June 2016	at	1:09pm	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	29 June 2016	at	1:09pm	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	29 June 2016	at	1:12pm	Type in the address bar: www.google.com
4.	29 June 2016	at	1:12pm	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	29 June 2016	at	1:13pm	Type in the address bar: www.googlemaps.com
6.	29 June 2016	at	1:13pm	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	29 June 2016	at	1:14pm	Type in the address bar: www.wikipedia.org
8.	29 June 2016	at	1:14pm	Type in the search bar (Hacker (computer security))
9.	29 June 2016	at	1:15pm	Type in the address bar: www.gmail.com
10.	29 June 2016	at	1:17pm	Send an email to nalomirah@gmail.com with a text file
11.	29 June 2016	at	1:18pm	Close the browser

Windows 10 Education OS Mozilla Firefox Private Browsing Mode				
Event #	Date/Time			Action
1.	29 June 2016	at	2:53pm	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	29 June 2016	at	2:54pm	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	29 June 2016	at	2:57pm	Type in the address bar: www.google.com
4.	29 June 2016	at	2:57pm	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	29 June 2016	at	2:58pm	Type in the address bar: www.googlemaps.com
6.	29 June 2016	at	2:58pm	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	29 June 2016	at	2:59pm	Type in the address bar: www.wikipedia.org
8.	29 June 2016	at	2:59pm	Type in the search bar (Hacker (computer security))
9.	29 June 2016	at	3:00pm	Type in the address bar: www.gmail.com
10.	29 June 2016	at	3:02pm	Send an email to nalomirah@gmail.com with a text file
11.	29 June 2016	at	3:03pm	Close the browser

Mac OS X (EI Captain) Safari Private Browsing Mode				
Event #	Date/Time			Action
1.	30 June 2016	at	8:23pm	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	30 June 2016	at	8:23pm	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	30 June 2016	at	8:27pm	Type in the address bar: www.google.com
4.	30 June 2016	at	8:27pm	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	30 June 2016	at	8:28pm	Type in the address bar: www.googlemaps.com
6.	30 June 2016	at	8:28pm	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	30 June 2016	at	8:29pm	Type in the address bar: www.wikipedia.org
8.	30 June 2016	at	8:29pm	Type in the search bar (Hacker (computer security))
9.	30 June 2016	at	8:30pm	Type in the address bar: www.gmail.com
10.	30 June 2016	at	8:32pm	Send an email to nalomirah@gmail.com with a text file
11.	30 June 2016	at	8:33pm	Close the browser

Mac OS X (EI Captain)					Google Chrome Private Browsing Mode
Event #	Date/Time				Action
1.	30	June	2016	at 8:53pm	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	30	June	2016	at 8:53pm	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	30	June	2016	at 8:56pm	Type in the address bar: www.google.com
4.	30	June	2016	at 8:56pm	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	30	June	2016	at 8:57pm	Type in the address bar: www.googlemaps.com
6.	30	June	2016	at 8:57pm	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	30	June	2016	at 8:58pm	Type in the address bar: www.wikipedia.org
8.	30	June	2016	at 8:58pm	Type in the search bar (Hacker (computer security))
9.	30	June	2016	at 8:59pm	Type in the address bar: www.gmail.com
10.	30	June	2016	at 9:00pm	Send an email to nalomirah@gmail.com with a text file
11.	30	June	2016	at 9:01pm	Close the browser

Mac OS X (EI Captain)					Mozilla Firefox Private Browsing Mode
Event #	Date/Time				Action
1.	30	June	2016	at 9:15pm	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	30	June	2016	at 9:15pm	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	30	June	2016	at 9:19pm	Type in the address bar: www.google.com
4.	30	June	2016	at 9:19pm	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	30	June	2016	at 9:20pm	Type in the address bar: www.googlemaps.com
6.	30	June	2016	at 9:20pm	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	30	June	2016	at 9:21pm	Type in the address bar: www.wikipedia.org
8.	30	June	2016	at 9:21pm	Type in the search bar (Hacker (computer security))
9.	30	June	2016	at 9:22pm	Type in the address bar: www.gmail.com
10.	30	June	2016	at 9:24pm	Send an email to nalomirah@gmail.com with a text file
11.	30	June	2016	at 9:25pm	Close the browser

Ubuntu 16.04 Mozilla Firefox Private Browsing Mode				
Event #	Date/Time			Action
1.	13	July	2016	at 7:50pm
				Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	13	July	2016	at 7:50pm
				Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	13	July	2016	at 7:53pm
				Type in the address bar: www.google.com
4.	13	July	2016	at 7:53pm
				Type in the search bar (Hacking Terms) and view the first 3 pages
5.	13	July	2016	at 7:54pm
				Type in the address bar: www.googlemaps.com
6.	13	July	2016	at 7:54pm
				Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	13	July	2016	at 8:03pm
				Type in the address bar: www.wikipedia.org
8.	13	July	2016	at 8:03pm
				Type in the search bar (Hacker (computer security))
9.	13	July	2016	at 8:03pm
				Type in the address bar: www.gmail.com
10.	13	July	2016	at 8:05pm
				Send an email to nalomirah@gmail.com with a text file
11.	13	July	2016	at 8:04pm
				Close the browser

Ubuntu 16.04 Opera Private Browsing Mode				
Event #	Date/Time			Action
1.	13	July	2016	at 9:43pm
				Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	13	July	2016	at 9:43pm
				Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	13	July	2016	at 9:47pm
				Type in the address bar: www.google.com
4.	13	July	2016	at 9:47pm
				Type in the search bar (Hacking Terms) and view the first 3 pages
5.	13	July	2016	at 9:48pm
				Type in the address bar: www.googlemaps.com
6.	13	July	2016	at 9:48pm
				Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	13	July	2016	at 9:49pm
				Type in the address bar: www.wikipedia.org
8.	13	July	2016	at 9:49pm
				Type in the search bar (Hacker (computer security))
9.	13	July	2016	at 9:50pm
				Type in the address bar: www.gmail.com
10.	13	July	2016	at 9:52pm
				Send an email to nalomirah@gmail.com with a text file
11.	13	July	2016	at 9:53pm
				Close the browser

Ubuntu 16.04 Google Chrome Private Browsing Mode					
Event #	Date/Time				Action
1.	14	July	2016	at	Type in the address bar: www.youtube.com & search for (Hacking Methods) in the search bar
2.	14	July	2016	at	Watch the video with the title (Best Method to Hack Facebook!!!!)
3.	14	July	2016	at	Type in the address bar: www.google.com
4.	14	July	2016	at	Type in the search bar (Hacking Terms) and view the first 3 pages
5.	14	July	2016	at	Type in the address bar: www.googlemaps.com
6.	14	July	2016	at	Type in the search bar the following address: 55 Wellesley St E, Auckland, 1024
7.	14	July	2016	at	Type in the address bar: www.wikipedia.org
8.	14	July	2016	at	Type in the search bar (Hacker (computer security))
9.	14	July	2016	at	Type in the address bar: www.gmail.com
10.	14	July	2016	at	Send an email to nalomirah@gmail.com with a text file
11.	14	July	2016	at	Close the browser

Appendix 3 – Hashes of the Forensics Images

Name	Acquisition MD5	Verification MD5	Acquisition SHA1	Verification SHA1
MacOSXnormalmode	76121f31450735ceca6e45e4e38a4790	76121f31450735ceca6e45e4e38a4790	4c53b73157795d1dd32172fd208afa5cb6297077	4c53b73157795d1dd32172fd208afa5cb6297077
Normalmodeacquisitionphase2	953d30246cce6401f99d73c853f30327	953d30246cce6401f99d73c853f30327	1e7a287608a7fe6fdc346fc06fb05dacd90335e4	1e7a287608a7fe6fdc346fc06fb05dacd90335e4
iOS Safari	5d139ff453c1826be210e7e138e1c58c	5d139ff453c1826be210e7e138e1c58c	9dfa9a861cf0061e073c4691d0a5361c018ad85a	9dfa9a861cf0061e073c4691d0a5361c018ad85a
WIN10CHROME	2c067b68aa9ac4e442c9aa244ae3d33b	2c067b68aa9ac4e442c9aa244ae3d33b	3d129419a5ce9f140bfc2a4e763ffb39b2ac9e4	3d129419a5ce9f140bfc2a4e763ffb39b2ac9e4
WIN10FF	e622647803470456784455e51f0e367e	e622647803470456784455e51f0e367e	6d6218a5c7bb7275fe81b5d5402da10aad912d5e	6d6218a5c7bb7275fe81b5d5402da10aad912d5e
WIN10IE	3c0e3bb0a5f9a4e03ae59d920ec03668	3c0e3bb0a5f9a4e03ae59d920ec03668	d7cece23cdf65695bdfe2a5ce156fcbd89a5f558	d7cece23cdf65695bdfe2a5ce156fcbd89a5f558
iOS Chrome	6779a282956ee6718c77611422f08844	6779a282956ee6718c77611422f08844	48222daacd552946a34de1c7884c92c1680e2f9b	48222daacd552946a34de1c7884c92c1680e2f9b
iOS FF	1e555b9894f6647faf1adb39447f4b8c	1e555b9894f6647faf1adb39447f4b8c	e99ec90361891fda6abdbe3dac8277aa8f12e425	e99ec90361891fda6abdbe3dac8277aa8f12e425
UBUNTU FF	22690ae1573e368c185c849ccd4e7a9c	22690ae1573e368c185c849ccd4e7a9c	132754e39a7f053829713aa32a28141a70781709	132754e39a7f053829713aa32a28141a70781709
UBUNTU OPERA	83477cd5591b0d9ebbe18d848c8267a1	83477cd5591b0d9ebbe18d848c8267a1	032575e43f140124bb4798823d768968f70fd3a7	032575e43f140124bb4798823d768968f70fd3a7
UBUNTU Chrome	12fa5af25733817daf556ebd1670887e	12fa5af25733817daf556ebd1670887e	feae6a70a3db3fbfffea816383bf7ca7cafdd3e	feae6a70a3db3fbfffea816383bf7ca7cafdd3e
UBUNTU normal mode acq	7bd7f8acf77653d39f739546ac7f5087	7bd7f8acf77653d39f739546ac7f5087	bb86050b6e1b3628ce746f30159829b57788471a	bb86050b6e1b3628ce746f30159829b57788471a

Appendix 4 – Encase Generated Forensic Report

Examination Report

Case Information

Case Number	01
Examiner Name	Norah Alomirah
Description	Examining Normal and Private Browsing Artefacts Left on the Local Hard Drive of the Suspect

Evidence Files Generated by Encase

Name	MacOSXnormalmode
Primary Path	J:\Encase\ENCASE_ACQ_EXAMINATION\EvidenceCache\MacOSXnormalmode.Ex01
Actual Date	18/04/16 09:47:45 p.m.
Target Date	18/04/16 09:52:51 p.m.
File Integrity	Completely Verified, 0 Errors
EnCase Version	7.10.03
Error Granularity	64
Examiner Name	Norah Alomirah
Time Zone	(UTC+12:00) Auckland, Wellington
Serial Number	WD-WX61AC41JTHF
Model	00LPVX-2
Write Blocked	Tableau
System Version	Windows 7

Name	Normalmodeacquisitionphase2
Primary Path	I:\Encase\Normalmodeacquisitionphase2.Ex01
Actual Date	17/04/16 09:09:17 p.m.
Target Date	17/04/16 09:09:52 p.m.
File Integrity	Completely Verified, 0 Errors
EnCase Version	7.10.03
Error Granularity	64
Examiner Name	Norah Alomirah
Time Zone	(UTC+12:00) Auckland, Wellington
Serial Number	WD-WX71AC4EX32F
Model	00LPVX-2
Write Blocked	Tableau
System Version	Windows 7

Name	iOS Safari
Primary Path	G:\ENCASE\iOS Safari.Ex01
Actual Date	04/07/16 12:54:50 p.m.
Target Date	04/07/16 01:00:45 p.m.
File Integrity	Completely Verified, 0 Errors
EnCase Version	7.10.03
Error Granularity	64
Examiner Name	Norah Alomirah
Time Zone	(UTC+12:00) Auckland, Wellington
Serial Number	WD-WXR1E94C29WC
Model	00LPVX-2
Write Blocked	Tableau
System Version	Windows 7

Name	WIN10CHROME
Primary Path	G:\ENCASE\WIN10CHROME.Ex01
Actual Date	29/06/16 02:36:34 p.m.
Target Date	29/06/16 02:38:34 p.m.
File Integrity	Completely Verified, 0 Errors
EnCase Version	7.10.03
Error Granularity	64
Examiner Name	Norah Alomirah
Time Zone	(UTC+12:00) Auckland, Wellington
Serial Number	WD-WX71AC42HSSV
Model	00LPVX-2
Write Blocked	Tableau
System Version	Windows 7

Name	WIN10FF
Primary Path	G:\ENCASE\WIN10FF.Ex01
Actual Date	29/06/16 03:22:54 p.m.
Target Date	29/06/16 03:24:07 p.m.
File Integrity	Completely Verified, 0 Errors
EnCase Version	7.10.03
Error Granularity	64
Examiner Name	Norah Alomirah
Time Zone	(UTC+12:00) Auckland, Wellington
Serial Number	WD-WX71AC4EX15P
Model	00LPVX-2
Write Blocked	Tableau
System Version	Windows 7

Name	WIN10IE
Primary Path	G:\ENCASE\WIN10IE.Ex01
Actual Date	29/06/16 12:12:20 p.m.
Target Date	29/06/16 12:25:44 p.m.
File Integrity	Completely Verified, 0 Errors
EnCase Version	7.10.03
Error Granularity	64
Examiner Name	Norah Alomirah
Time Zone	(UTC+12:00) Auckland, Wellington
Serial Number	WD-WX91AC4PN6EV
Model	00LPVX-2
Write Blocked	Tableau
System Version	Windows 7

Name	iOS Chrome
Primary Path	G:\ENCASE\iOS Chrome.Ex01
Actual Date	04/07/16 03:06:11 p.m.
Target Date	04/07/16 03:08:58 p.m.
File Integrity	Completely Verified, 0 Errors
EnCase Version	7.10.03
Error Granularity	64
Examiner Name	Norah Alomirah
Time Zone	(UTC+12:00) Auckland, Wellington
Serial Number	WD-WX31AC4HTPU8
Model	00LPVX-0
Write Blocked	Tableau
System Version	Windows 7

Name	iOS FF
Primary Path	L:\ENCASE\iOS FF.Ex01
Actual Date	05/07/16 03:52:55 p.m.
Target Date	05/07/16 03:55:33 p.m.
File Integrity	Completely Verified, 0 Errors
EnCase Version	7.10.03
Error Granularity	64
Examiner Name	Norah Alomirah
Time Zone	(UTC+12:00) Auckland, Wellington
Serial Number	WD-WX11A15AFY4L
Model	00LPVX-0
Write Blocked	Tableau
System Version	Windows 7

Name	UBUNTU FF
Primary Path	L:\ENCASE\UBUNTU FF.Ex01
Actual Date	14/07/16 08:37:47 p.m.
Target Date	14/07/16 08:44:44 p.m.
File Integrity	Completely Verified, 0 Errors
EnCase Version	7.10.03
Error Granularity	64
Examiner Name	Norah Alomirah
Time Zone	(UTC+12:00) Auckland, Wellington
Serial Number	WD-WX31A15RC8J7
Model	00LPVX-0
Write Blocked	Tableau
System Version	Windows 7

Name	UBUNTU OPERA
Primary Path	L:\ENCASE\UBUNTU OPERA.Ex01
Actual Date	15/07/16 02:38:29 p.m.
Target Date	15/07/16 02:40:09 p.m.
File Integrity	Completely Verified, 0 Errors
EnCase Version	7.10.03
Error Granularity	64
Examiner Name	Norah Alomirah
Time Zone	(UTC+12:00) Auckland, Wellington
Serial Number	WD-WX11A15AFPHA
Model	00LPVX-0
Write Blocked	Tableau
System Version	Windows 7

Name	UBUNTU Chrome
Primary Path	L:\ENCASE\UBUNTU Chrome.Ex01
Actual Date	15/07/16 04:27:30 p.m.
Target Date	15/07/16 04:31:23 p.m.
File Integrity	Completely Verified, 0 Errors
EnCase Version	7.10.03
Error Granularity	64
Examiner Name	Norah Alomirah
Time Zone	(UTC+12:00) Auckland, Wellington
Serial Number	WD-WXQ1E948EWN2
Model	00LPVX-2
Write Blocked	Tableau
System Version	Windows 7

Name	UBUNTU normal mode acq
Primary Path	L:\ENCASE\UBUNTU normal mode acq.Ex01
Actual Date	17/07/16 09:48:39 p.m.
Target Date	17/07/16 09:50:33 p.m.
File Integrity	Completely Verified, 0 Errors
EnCase Version	7.10.03
Error Granularity	64
Examiner Name	Norah Alomirah
Time Zone	(UTC+12:00) Auckland, Wellington
Serial Number	WD-WX11EA41UWP0
Model	00LPVX-2
Write Blocked	Tableau
System Version	Windows 7

WIN10IE Findings

Name	resources.js
Start Sector	1,930,344
File Ext	js
Logical Size	55,718
Item Type	Entry
Category	Document
Signature Analysis	Alias
File Type	UTF-8 Document File
File Type Tag	utf8
Last Accessed	14/02/16 06:13:43 a.m.
File Created	14/02/16 06:13:43 a.m.
Last Written	14/02/16 06:13:43 a.m.
MD5	cf8c6307c170f84388f17bbe14928f78
SHA1	bfd92edcd6307c4308d0252cf724430e7ce5b984
Primary Device	WIN10IE
Item Path	WIN10IE\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\en-us\resources.js
Entry Modified	28/06/16 10:19:42 a.m.
True Path	WIN10IE\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\en-us\resources.js
Description	File, Archive, Hard Linked
Bookmark Type	Notable File
Name	sway.exe
Start Sector	2,164,328
File Ext	exe
Logical Size	12,548,160
Item Type	Entry
Category	Executable
Signature Analysis	Match
File Type	Windows Executable
File Type Tag	exe
Last Accessed	14/02/16 06:13:45 a.m.
File Created	14/02/16 06:13:45 a.m.
Last Written	14/02/16 06:13:46 a.m.
MD5	7afc679b5db3823fd0044f20c699561f
SHA1	2862611ac109ea20db49709b340e4c3eb3cc6cc2
Primary Device	WIN10IE
Item Path	WIN10IE\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\sway.exe
Entry Modified	28/06/16 10:19:45 a.m.
True Path	WIN10IE\Program Files\WindowsApps\Microsoft.Office.Sway_17.6216.20251.0_x64__8wekyb3d8bbwe\sway.exe
Description	File, Archive, Hard Linked
Bookmark Type	Notable File
Name	WebCacheV01.dat
Start Sector	9,674,624
File Ext	dat
Logical Size	26,738,688

Item Type	Entry
Category	Email
Signature Analysis	Alias
File Type	Microsoft Exchange Database
File Type Tag	edb
Last Accessed	28/06/16 10:31:46 a.m.
File Created	28/06/16 10:31:46 a.m.
Last Written	29/06/16 10:53:16 p.m.
MD5	b4bfd75599b371d3025e4aa342bd3ae2
SHA1	7b4b971922043dcda75175231f8fb278df079d4f
Primary Device	WIN10IE
Item Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
Entry Modified	29/06/16 10:53:16 p.m.
True Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
Description	File, Archive, Not Indexed
Bookmark Type	Notable File
Name	V01.log
Start Sector	957,448
File Ext	log
Logical Size	524,288
Item Type	Entry
Category	Document
Signature Analysis	Match
File Type	Log
File Type Tag	log
Last Accessed	29/06/16 10:33:52 p.m.
File Created	28/06/16 10:31:46 a.m.
Last Written	29/06/16 10:53:16 p.m.
MD5	41dcb73f9be97fe37aba36cd05fe035b
SHA1	43e1ddecee4f8306f385ec28c731769c11a8581c
Primary Device	WIN10IE
Item Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\WebCache\V01.log
Entry Modified	29/06/16 10:53:16 p.m.
True Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\WebCache\V01.log
Description	File, Archive, Not Indexed
Bookmark Type	Notable File
Name	V01tmp.log
Start Sector	5,708,288
File Ext	log
Logical Size	524,288
Item Type	Entry
Category	Document
Signature Analysis	Match
File Type	Log
File Type Tag	log
Last Accessed	29/06/16 10:42:52 p.m.
File Created	28/06/16 10:31:46 a.m.
Last Written	29/06/16 10:47:22 p.m.
MD5	a38ecb7e8961ecbc095bfed83b88f610
SHA1	33978a7ae27bb90ce440695e9984cd79637eff4d

Primary Device	WIN10IE
Item Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\WebCache\V01tmp.log
Entry Modified	29/06/16 10:50:27 p.m.
True Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\WebCache\V01tmp.log
Description	File, Archive, Not Indexed
Bookmark Type	Notable File
Name	fZOD016T1.txt
Start Sector	41,327,688
File Ext	txt
Logical Size	5,031
Item Type	Entry
Category	Document
Signature Analysis	Match
File Type	Text
File Type Tag	txt
Last Accessed	29/06/16 10:47:27 p.m.
File Created	29/06/16 10:47:27 p.m.
Last Written	29/06/16 10:47:27 p.m.
MD5	0806630612b8be942493fa808d415a34
SHA1	64c2dba13407126b0c3513869cd04b5d7f698d00
Primary Device	WIN10IE
Item Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\INetCache\Low\IE\8TH QGUVC\fZOD016T1.txt
Entry Modified	29/06/16 10:47:27 p.m.
True Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\INetCache\Low\IE\8TH QGUVC\fZOD016T1.txt
Description	File, Deleted, Archive, Not Indexed
Bookmark Type	Notable File
Name	fLSOUE076.txt
Start Sector	41,331,152
File Ext	txt
Logical Size	5,241
Item Type	Entry
Category	Document
Signature Analysis	Match
File Type	Text
File Type Tag	txt
Last Accessed	29/06/16 10:47:28 p.m.
File Created	29/06/16 10:47:28 p.m.
Last Written	29/06/16 10:47:28 p.m.
MD5	ff69d65f0bb29a2a8308b0e4649a7db9
SHA1	11ba1221eff84a59652630948eb12bb4343005ca
Primary Device	WIN10IE
Item Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\INetCache\Low\IE\EN2J ZKA3\fLSOUE076.txt
Entry Modified	29/06/16 10:47:28 p.m.
True Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\INetCache\Low\IE\EN2J ZKA3\fLSOUE076.txt
Description	File, Deleted, Archive, Not Indexed
Bookmark Type	Notable File
Name	f6EOI1X0J.txt
Start Sector	41,283,120
File Ext	txt
Logical Size	5,190

Item Type	Entry
Category	Document
Signature Analysis	Match
File Type	Text
File Type Tag	txt
Last Accessed	29/06/16 10:47:29 p.m.
File Created	29/06/16 10:47:29 p.m.
Last Written	29/06/16 10:47:29 p.m.
MD5	168552071b343360b1ab8bac5d5b140c
SHA1	9bb77d418033ae1edea298004d4dc5371a498a34
Primary Device	WIN10IE
Item Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\INetCache\Low\IE\EN2JZKA3\f6EOI1X0J.txt
Entry Modified	29/06/16 10:47:29 p.m.
True Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\INetCache\Low\IE\EN2JZKA3\f6EOI1X0J.txt
Description	File, Deleted, Archive, Not Indexed
Bookmark Type	Notable File
Name	fV2Z3OO7Y.txt
Start Sector	41,353,592
File Ext	txt
Logical Size	44,018
Item Type	Entry
Category	Document
Signature Analysis	Match
File Type	Text
File Type Tag	txt
Last Accessed	29/06/16 10:47:35 p.m.
File Created	29/06/16 10:47:35 p.m.
Last Written	29/06/16 10:47:35 p.m.
MD5	6d7ce101e2091888e0f3d0e17a4bd4bf
SHA1	426c8dabf3c5592f4be44b5b2b939898bc7035ff
Primary Device	WIN10IE
Item Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\INetCache\Low\IE\PON6I6VD\fV2Z3OO7Y.txt
Entry Modified	29/06/16 10:47:35 p.m.
True Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\INetCache\Low\IE\PON6I6VD\fV2Z3OO7Y.txt
Description	File, Deleted, Archive, Not Indexed
Bookmark Type	Notable File
Name	Unallocated Clusters
Start Sector	98,696
Logical Size	35,850,358,784
Item Type	Entry
Category	Unknown
Primary Device	WIN10IE
Item Path	WIN10IE\Unallocated Clusters
True Path	WIN10IE\Unallocated Clusters
Description	File, Unallocated Clusters
Bookmark Type	Notable File
Name	V010000B.log
Start Sector	5,697,248
File Ext	log
Logical Size	524,288

Item Type	Entry
Category	Document
Signature Analysis	Match
File Type	Log
File Type Tag	log
Last Accessed	29/06/16 10:43:05 p.m.
File Created	28/06/16 10:31:46 a.m.
Last Written	29/06/16 10:50:27 p.m.
MD5	013e7ca7af6cc969cf75a8c9ab07917d
SHA1	c8c129b8323750bce17e5ff9817548da8d03558f
Primary Device	WIN10IE
Item Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\WebCache\V010000B.log
Entry Modified	29/06/16 10:50:27 p.m.
True Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\WebCache\V010000B.log
Description	File, Archive, Not Indexed
Bookmark Type	Notable File
Name	Package_1517_for_KB3163018~31bf3856ad364e35~amd64~~10.0.1.2.cat
Start Sector	41,272,152
File Ext	cat
Logical Size	9,603
Item Type	Entry
Category	Document
Signature Analysis	Match
File Type	Quicken Categorization
File Type Tag	cat1
Last Accessed	29/06/16 10:47:29 p.m.
File Created	29/06/16 10:47:29 p.m.
Last Written	02/06/16 11:29:21 p.m.
MD5	19e2e516dd42625bc9247e6adf4b10dc
SHA1	896c664a31b895a1e06882dc627482f42632c31a
Primary Device	WIN10IE
Item Path	WIN10IE\Lost Files\Package_1517_for_KB3163018~31bf3856ad364e35~amd64~~10.0.1.2.cat
Entry Modified	29/06/16 10:49:19 p.m.
True Path	WIN10IE\Lost Files\Package_1517_for_KB3163018~31bf3856ad364e35~amd64~~10.0.1.2.cat
Description	File, Deleted
Bookmark Type	Notable File
Name	\$MFT
Start Sector	6,291,456
Logical Size	111,411,200
Item Type	Entry
Category	Unknown
Last Accessed	28/06/16 11:10:38 a.m.
File Created	28/06/16 11:10:38 a.m.
Last Written	28/06/16 11:10:38 a.m.
Primary Device	WIN10IE
Item Path	WIN10IE\ \$MFT
Entry Modified	28/06/16 11:10:38 a.m.
True Path	WIN10IE\ \$MFT
Description	File, Internal, Hidden, System
Bookmark Type	Notable File
Name	\$UsnJrnl-\$J

Start Sector	41,105,056
Logical Size	65,394,776
Item Type	Entry
Category	Unknown
Signature Analysis	Unknown
MD5	75ce47626817154ecf93c89c98e2ff18
SHA1	a4f1f0bc0868f6ef1eaae09ecd2fd533a447cf06
Primary Device	WIN10IE
Item Path	WIN10IE\Extend\UsnJrnl-\$J
True Path	WIN10IE\Extend\UsnJrnl-\$J
Description	File, Stream, System
Bookmark Type	Notable File
Name	UVW46F7M
Start Sector	17,485,056
Logical Size	98,304
Item Type	Entry
Category	Folder
Signature Analysis	Unknown
Last Accessed	29/06/16 10:52:47 p.m.
File Created	29/06/16 10:33:58 p.m.
Last Written	29/06/16 10:52:47 p.m.
MD5	ea980cae4c32698762105c462b4c4858
SHA1	c54c9ec99ed62b410fce620c3d5854a2a4af42e6
Primary Device	WIN10IE
Item Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\INetCache\Low\IE\UVW46F7M
Entry Modified	29/06/16 10:52:47 p.m.
True Path	WIN10IE\Users\Windows10test\AppData\Local\Microsoft\Windows\INetCache\Low\IE\UVW46F7M
Description	Folder, Hidden, System, Not Indexed
Bookmark Type	Notable File

WIN10FF Findings

Name	hiberfil.sys
Start Sector	22,018,464
File Ext	sys
Logical Size	17,054,482,432
Item Type	Entry
Category	Executable
Signature Analysis	Bad signature
Last Accessed	28/06/16 11:48:44 p.m.
File Created	28/06/16 11:48:44 p.m.
Last Written	30/06/16 02:03:36 a.m.
MD5	2a2124484f5b60b6f53684ce93fa1336
SHA1	0428d8342ebce851d1b6d86f71b0498bdeffff84
Primary Device	WIN10FF
Item Path	WIN10FF\hiberfil.sys
Entry Modified	30/06/16 02:03:36 a.m.
True Path	WIN10FF\hiberfil.sys
Description	File, Hidden, System, Archive, Not Indexed
Bookmark Type	Notable File
Name	Unallocated Clusters
Start Sector	355,008
Logical Size	35,873,026,048
Item Type	Entry
Category	Unknown
Primary Device	WIN10FF
Item Path	WIN10FF\Unallocated Clusters
True Path	WIN10FF\Unallocated Clusters
Description	File, Unallocated Clusters
Bookmark Type	Notable File

WIN10FF Findings

Name	\$LogFile
Start Sector	6,025,264
Logical Size	67,108,864
Item Type	Entry
Category	Unknown
Last Accessed	28/06/16 11:22:04 p.m.
File Created	28/06/16 11:22:04 p.m.
Last Written	28/06/16 11:22:04 p.m.
Primary Device	WIN10CHROME
Item Path	WIN10CHROME\ \$LogFile
Entry Modified	28/06/16 11:22:04 p.m.
True Path	WIN10CHROME\ \$LogFile
Description	File, Internal, Hidden, System
Bookmark Type	Notable File
Name	Unallocated Clusters
Start Sector	98,664
Logical Size	36,866,408,448
Item Type	Entry
Category	Unknown
Primary Device	WIN10CHROME
Item Path	WIN10CHROME\Unallocated Clusters
True Path	WIN10CHROME\Unallocated Clusters
Description	File, Unallocated Clusters
Bookmark Type	Notable File
Name	hiberfil.sys
Start Sector	21,989,304
File Ext	sys
Logical Size	17,054,482,432
Item Type	Entry
Category	Executable
Signature Analysis	Bad signature
Last Accessed	28/06/16 10:34:34 p.m.
File Created	28/06/16 10:34:34 p.m.
Last Written	30/06/16 12:18:16 a.m.
MD5	4d833ae3678e0f9f4ff8bf6bec2b22c8
SHA1	2290335172bccb57f09542012a46f8eb581cb11b
Primary Device	WIN10CHROME
Item Path	WIN10CHROME\hiberfil.sys
Entry Modified	30/06/16 12:18:16 a.m.
True Path	WIN10CHROME\hiberfil.sys
Description	File, Hidden, System, Archive, Not Indexed
Bookmark Type	Notable File
Name	hiberfil.sys
Start Sector	21,989,304
File Ext	sys
Logical Size	17,054,482,432
Item Type	Entry
Category	Executable
Signature Analysis	Bad signature
Last Accessed	28/06/16 10:34:34 p.m.
File Created	28/06/16 10:34:34 p.m.

Last Written	30/06/16 12:18:16 a.m.
MD5	4d833ae3678e0f9f4ff8bf6bec2b22c8
SHA1	2290335172bccb57f09542012a46f8eb581cb11b
Primary Device	WIN10CHROME
Item Path	WIN10CHROME\hiberfil.sys
Entry Modified	30/06/16 12:18:16 a.m.
True Path	WIN10CHROME\hiberfil.sys
Description	File, Hidden, System, Archive, Not Indexed
Bookmark Type	Notable File

iOS Safari

Name	Unallocated Clusters
Start Sector	1,291,056
Logical Size	51,460,796,416
Item Type	Entry
Category	Unknown
Primary Device	iOS Safari
Item Path	iOS Safari\1 EICAPTIANTEST\Unallocated Clusters
True Path	iOS Safari\1 EICAPTIANTEST\Unallocated Clusters
Description	File, Unallocated Clusters
Bookmark Type	Notable File