Forensic Data Storage for Wireless Networks: A Compliant Architecture

THOMAS LAURENSON
Dip. ACSE (UNITEC, NZ), Grad. Dip. Computing (UNITEC, NZ)

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

School of Computing and Mathematical Sciences

Auckland, New Zealand
2010

Declaration

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

....

Signature

Acknowledgements

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, New Zealand. Support was received from many people throughout the duration of the thesis. Firstly, I would like to thank my family, including my mother Jetta, father Alan and sister Sophie who all provided amazing support and encouragement during the course of the thesis project, as well as throughout my entire post graduate study.

Huge thanks also to Dr. Brian Cusack, my thesis supervisor, for the exceptional support given during the thesis project. Brian provided ongoing inspiration, without which the finalised copy of this thesis would not have been reached. There are a number of other staff members and lecturers at AUT that also deserve thanking for their support and encouragement; Petteri Kaskenpalo for always being a motivational influence in all aspects of my study and research, and visiting industry lecturers including Mike Spence and Campbell McKenzie for providing advanced knowledge of real world digital forensic procedures to ground my academic perspective.

I would also like to thank my fellow MFIT students, especially Ben Knight, Ar Kar Kyaw and James Liang. Together, providing stimulant discussions, challenging questions, peer encouragement and many exciting debates in our chosen area of Digital Forensic research, with a side of Information Security topics.

Furthermore, thanks to the members of various open source communities, without which the software used during the thesis research would not exist. Specifically, thanks to Mike Kershaw (aka Dragorn), who single-handedly develops the Kismet application. Also the entire OpenWRT, Wireshark and mac80211 open source communities for providing and maintaining superb wireless software. Thanks must also go to other prominent open source and Linux legends, including Richard Stallman and Linus Torvalds who provide inspiration in all manners for my chosen field of computer science.

Abstract

In the past 10 years there has been an explosion of unprecedented growth in wireless based technologies. Wireless networking has escalated in popularity since its inauguration due to the ability to form computer networks without the use of a wired base infrastructure. However, the very nature of wireless networking engenders inherent security threats and vulnerabilities. Furthermore, with the rapid growth of technology based digital services also comes intentional misuse and related corruption of those services. Therefore, potential issues outline the possibility of criminal activity. Now, the need exists for Digital Forensic procedures in wireless networks which are specifically aimed at obtaining viable digital evidence. The current academic literature mainly relates to traditional digital forensic principles and device evidence extraction rather than assurance and network layer architectures. Further research in the particular field of digital forensics in wireless networks is crucial.

The main focus of the research project addresses the development of a design system which is capable of acquiring and preserving wireless network traffic, where the resultant data contains viable evidentiary trails from 802.11g based Wireless Local Area Networks (WLAN). The proposed system architecture of the Wireless Forensic Model (WFM) consists of two components: a wireless drone and a Forensic Server. The model is specifically engineered for infrastructure based WLANs with multiple Access Points (APs). The proposed design system therefore monitors and acquires wireless network traffic from the APs using a distribution of wireless drones. These collect and forward the network traffic to the centralised Forensic Server which in turn stores and preserves the acquired data.

Four phases of research testing were conducted; two for initial testing and two for stabilised testing. Phase One and Two of initial testing involved the implementation of a test-bed WLAN infrastructure and the implementation of the prescribed WFM design system. Both entities were subjected to benchmark testing. The initial WFM was evaluated to determine the requirements and capabilities of acquiring and preserving data from the WLAN. Phase Three drew experience from the initial WFM testing and reconfigured a stable system design. Benchmark testing was again conducted to examine the system performance and whether a full data set of viable digital evidence could be obtained. In Phase Four the stabilised WFM was finally evaluated on the ability to obtain evidentiary trails from a series of recreated attacks conducted against the WLAN.

The findings illustrate that the WFM is capable of acquiring and preserving a large proportion of data generated at the maximum speeds of the 802.11g WLAN configuration. Integrity of the evidence was also maintained. Furthermore, recreated Denial of Service (DoS) and Fake Access Point (FakeAP) attacks against the WLAN infrastructure resulted in evidentiary trails being collected by the implemented WFM. The acquired wireless network traffic also provided details of the attack conducted and the possibility of linking the evidence of the attack to a specific device.

The research project has provided additional knowledge relating to forensic investigations in WLANs. The WFM design is also considered to be feasible through the use of readily available hardware and open source software to allow easy implementation of the system architecture. Wireless network traffic, as a source of evidence, has also been evaluated discovering information which may be extracted and the potential use of the collected data. The aim and the positive outcomes of the implemented Wireless Forensic Model, points to an exciting new development area in the realm of digital forensic procedures in wireless networks.

Table of Contents

Chapter One: Introduction

Chapter Two: Literature Review

Chapter Three: Research Methodology

Chapter Four: Research Findings

Chapter Five: Research Findings

Chapter Six: Conclusion

List of Tables

List of Figures

List of Abbreviations

ACPO	Association of Chief Police Officers
AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
AS	Authentication Server
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CCMP	Cipher Mode with Cipher Block Chaining Message Authentication Code Protocol
CLI	Command Line Interface
CPU	Central Processor Unit
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DS	Distributed System
EAP	Extensible Authentication Protocol
ES	Evidence Server
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
FakeAP	Fake Access Point
FCS	Frame Check Sequence
FMS	Fluhrer, Mantin & Shamir attack
FTP	File Transfer Protocol
GB	Gigabyte
GPL	General Public Licence
GPS	Global Positioning System
GTK	Group Temporal Key
GUI	Graphical User Interface
IBSS	Independent Basic Service Set
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
IV	Initialisation Vector

IEEE	Institute of Electrical and Electronics Engineers
IEEE-SA	Institute of Electrical and Electronics Engineers – Standards Association
IPS	Intrusion Prevention System
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
MAC	Media Access Control (device address)
MAC	Medium Access Control (protocol layer)
MB	Megabyte
MCS	Multi Channel Sniffer
MD5	Message Digest algorithm 5
MGEN	Multi-Generator application
MIMO	Multiple Input Multiple Output
MITM	Man in the Middle
NFAT	Network Forensic Analysis Tool
NIC	Network Interface Card
NIJ	National Institute of Justice
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
PCAP	Packet Capture
PC	Personal Computer
PCI	Peripheral Component Interconnect
PDA	Personal Desktop Assistant
PHY	Physical Layer
PMK	Pairwise Master Key
PPS	Packet Per Second
PSK	Pre-Shared Key
RAM	Random Access Memory
RC4	Rivest Cipher 4
RF	Radio Frequency
RFMON	Radio Frequency Monitor Mode
RSN	Robust Secure Network
RSNA	Robust Secure Network Association
SBC	Single Board Computer

SSID	Service Set Identifier
STA	Station
SWGDE	Scientific Work Group on Digital Evidence
SUID	Set User Identification
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UNII	Unlicensed National Information Infrastructure
USB	Universal Serial Bus
VoIP	Voice Over Internet Protocol
WEP	Wired Equivalent Protocol
WFM	Wireless Forensic Model
WFRM	Wireless Forensic Readiness Model
WIDS	Wireless Intrusion Detection System
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XML	Extensible Markup Language

Chapter One

INTRODUCTION

1.0 BACKGROUND

The chosen topic area for the thesis project consists of an overlap of two Information Technology (IT) areas. Firstly, wireless network technologies and secondly, digital forensic procedures. Therefore, an introduction will be provided for both areas to establish an extensive background of the topic area of research. Furthermore, specific consideration in the thesis is given to the process and principles governing the ability to perform digital forensic investigations in wireless networks. The vast amount of reviewed evaluative literature ranges from wireless networking technology and standards to digital forensic procedures, tools and techniques.

Wireless network communication technology can encompass many various types of technologies which communicate, or transfer information without the use of physical wired connections. Examples of commonly used wireless technology include handheld radios and cellular phones. The specific wireless networking technology being investigated in the thesis is Wireless Local Area Networks (WLAN). A WLAN "enables access to computing devices that are not physically connected to a network" (Frankel, Eydt, Owens & Scarfone, 2007, p.11) where the most frequently used family of standards is detailed by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard. The goal of the IEEE 802.11 standard is "to define one medium access control (MAC) and several physical layer (PHY) specifications for wireless connectivity for fixed, portable or moving Stations (STAs) within a local area" (IEEE Std. 802.11, 2007, p.1). Thus, the objective is to provide a wireless communications technology allowing wireless network communication between two or more capable devices. The IEEE 802.11 WLAN standard has commonly become known as Wi-Fi (Wireless Fidelity). However, Wi-Fi is in fact the trademark of the Wi-Fi Alliance which promotes and certifies 802.11 capable devices.

Since the release of the IEEE 802.11 standard and the subsequent availability of devices which support the standard, WLANs have become increasingly popular. "The main attraction of WLANs is their flexibility. They can extend access to local area networks, such as corporate intranets, as well as support broadband access to the Internet" (Varshney, 2003, p.102). WLANs are also being used as a substitute to traditional wired based networking infrastructures due to the difficulty in providing additions, deletions and changes to network topology which are experienced in conventional wired Local Area Network (LAN) environments (Crow, Widjaja, Kim & Sakai, 1997, p.116).

However, "accompanying the widespread usage is the presence of crime; the more popular the technology, the more opportunity exists for its misuse" (Turnbull & Slay, 2008, p.1355). Such crime includes intentional misuse of the WLAN technology, including unauthorized use and attacks conducted against the wireless network medium. Furthermore, the security of wireless networks also plays an important part towards the misuse of WLANs, due to potential risks of the wireless network design. "Wireless networks propagate signals into space, making traditional physical security countermeasures less effective and access to the network much easier" (Scarfone, Dicoi, Sexton & Tibbs, 2008, p.27). WLANs also typically suffer from loss of confidentiality and integrity of data due to various threats involving an attacker's ability to intercept and inject network communication between devices (Frankel et al., 2007, p.27). Therefore, security and misuse threats are an exceptionally important aspect of WLANs and all wireless networking technologies. The risks identified enforce the need to evaluate potential threats, security features in place and the likely requirements for digital forensic investigation if or when such scenarios occur.

Digital forensics currently has many definitions. However, the overall process can be defined as "the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data" (Kent, Chevalier, Grance & Dang, 2006, p.9). Digital forensics therefore, involves using specified methodologies to recover data from digital devices while at the same time ensuring that the collected data is similarly maintained to protect reliability. Moreover, digital forensic methodologies may differ depending on the type of device or data which needs to be processed. For example, traditional computer forensic methodologies involve collection of evidence from the hard disk of the device and subsequent analysis of the data. In comparison, network forensic investigations involve different methodologies due to the difference in data collection processes and the type of data acquired. In all cases, set specific procedures must be meticulously followed when conducting digital forensic investigations in order to obtain and preserve viable digital evidence.

Digital forensics is often associated with computer crime, also known as cybercrime, as the output of digital evidence from the forensic process provides evidential proof of particular events. Cybercrime involves the use of computers, or similar electronic devices, to commit, or aid in committing criminal acts. For example, hacking, copyright infringement or the theft of intellectual property from an organization to name a few of the more common issues. An issue is connected to cybercrime when the medium used or item stolen involves some form of digital data. “Computer crime is a lucrative criminal activity that continues to grow in its prevalence and frequency” (Rogers & Seigfried, 2004, p.12).

The background given has introduced the two focus areas of research. Firstly, wireless networks, specifically IEEE 802.11 based WLANs, and secondly, the area of digital forensics. The risks of wireless networks have been identified and the growing concern of associated computer crime. Methodologies and procedures have been developed for digital forensics, but most are aligned to traditional computer and wired network investigations. There is therefore, an apparent need for additional knowledge in the chosen research area which reinforces the demand for added information regarding how to obtain potential digital evidence from wireless networks, while also ensuring that digital forensic principles are met and viable evidence is collected. Accordingly, the proposed research question to be addressed in the thesis project is:

> *What are the capabilities of a design system to acquire and preserve wireless network traffic as viable evidential trails from 802.11 WLANs?*

1.1 MOTIVATIONS

Section 1.0 identified and briefly discussed the background to the chosen research area of WLAN environments and the processes of digital forensics. In order to understand the reasoning for the chosen research areas, the motivations of the writer will be presented and discussed ranging from the popularity of wireless networking to the lack of digital forensic procedures available for such specialised investigations.

Since the introduction of the IEEE 802.11 standard and availability of wireless devices, wireless technology has escalated in popularity. Following the demand in trend, advancement has been made in the technology through revised amendments to the 802.11 standards, as well as academic literature researching new branches of the technology, from physical layer improvements to security feature development. However, there is little literature of procedures for performing the digital forensic process in wireless networking.

WLANs have built-in security features outlined by the 802.11 standard which aim to protect security objectives such as confidentiality, integrity and availability. However, WLANs also may potentially suffer from various threats including eavesdropping, Man in the Middle (MITM) and Denial of Service (DoS) attacks (Frankel et al., 2007, p.28). In addition, the security features available have suffered much scrutiny, and currently there are numerous possible techniques and tools available to conduct attacks against WLANs. Furthermore, intentional or criminal misuse of WLANs is also becoming widely apparent with wireless technologies. Turnbull & Slay (2008, p.1355) state that misuse of wireless networks is due to the flexible nature of the technology and may encompass detecting and connecting to wireless networks, using the wireless network as a vector of attack and to conceal evidence from investigation. Both the security issues and potential criminal misuse, highlight the need for development of procedures and techniques to perform digital forensic investigations in WLANs.

Another motivation for researching the chosen project area is the rising trend of cybercrime, as well as the risk for individuals or organisations from such activity. As the goal of digital forensics is to produce viable electronic evidence, the rise in criminal acts further substantiates the need for further research. The CSI/FBI Computer Crime and Security survey is conducted every year to assess the current state of security based statistics in enterprise organisations, and state that misuse of wireless networks has increased from 5% in 2005, to 11% in 2008, based on the numbers of respondents affected (Richardson, 2008, p.15). Furthermore, only 27% of those respondents have a specialised wireless security system implemented. The statistics clearly illustrate the need for advancement of digital forensic procedures in wireless networks.

“Whilst 802.11a/b/g wireless security is well documented by academic literature, there is little work discussing the forensic issues associated with the technology” (Slay & Turnbull, 2006, p.124). Furthermore, the area of digital forensics is an exceptionally specialised field of science, and requires specific knowledge in order to produce viable digital evidence. There also continues to be a lack of standardisation for the digital forensic process.

> “Unfortunately, there does not exist a standard or consistent digital forensic methodology, but rather a set of procedures and tools built from the experiences of law enforcement, system administrators, and hackers” (Reith, Carr & Gunsch, 2002, p.3).

Moreover, due to the unique nature of wireless networking, and computer networking in general, traditional digital forensic processes which are well documented are difficult to follow. Such methods usually involve collection of non-volatile data off a computer’s hard drive, but “technologies such as wireless networking will make these processes ineffective and obsolete” (Turnbull & Slay, 2008, p.1360).

In addition, performing digital forensics in a wireless network is a difficult task due to the limited sources of evidence available. The potential sources of evidence from wireless networks may include either live collection of network traffic, or analysis of wireless devices such as embedded systems of computer information (Turnbull & Slay, 2008, pp.1356-1359). However, to obtain such evidence specialised methods are needed. For example, “digital investigators require specialised knowledge and tools to process network traffic as a source of evidence” (Casey, 2004, p.28). Current literature, procedures and techniques do not provide such detailed information and so there is a substantiated need for advancement in digital forensic procedures and techniques, and subsequent testing to ensure reliability of collected evidence.

In summary, the preceding discussion illustrates the demand for advancement of knowledge in the realm of digital forensic processes in WLANs. Motivations include the increasing popularity of wireless networking, potential security issues and the widespread intentional or criminal misuse. In such events digital evidence could greatly aid criminal investigations. Furthermore, digital forensic principles for wireless network investigations are, at present, greatly limited, requiring advancement of tested and proven procedures and techniques. In conclusion, “802.11 wireless is a medium which is only going to become more ubiquitous, and its presence at crime scenes and other investigative scenes of interest is going to increase” (Turnbull & Slay, 2007, p.10).

1.2 STRUCTURE OF THESIS

The thesis will be reported in a logical sequence to communicate the research conducted. The formalities section presents an abstract of the thesis, acknowledgements and a table of contents. Additionally, a list of figures and a list of tables are presented as well as a listing of the abbreviations used in the thesis.

Chapter One provides an introduction to the project. The chosen topic area and associated background is put forward including an outline of wireless communication technologies, specifically WLANs being the focus of the study for the research. A background to the processes and principles of digital forensics is also discussed. The motivations for the project identify the need for the proposed research and investigation in the chosen research area.

Chapter Two provides an extensive review and discussion of the available literature for the topic area in order to build a thorough understanding of the current state of knowledge. The IEEE 802.11 WLAN standard provides an overview of the technology being investigated followed by discussion of the security features available, associated attacks and apparent misuse in 802.11 based WLANs. The process of digital forensics is presented with specific association to WLAN investigation techniques and potential sources of evidence. Intrusion Detection Systems (IDS) are also covered from the perspective of use in WLANs and to provide additional evidence when wireless attacks are involved. In closing, the problems and issues surrounding digital forensic investigation in WLANs demonstrate specific aspects and emphasis which area to focus research on.

Research methodology for the project is critically evaluated in Chapter Three. First, several published similar studies are reviewed in order to be informed on previous research methodologies, as well as to highlight specific areas needed for further potential research. The research questions are then developed from the preceding literature discussed in Chapter 2 and the related similar studies. Each question is also accompanied by a hypothesis; a proposed explanation made on the basis of theoretical information and the gathered knowledge. The research questions provide a goal for the thesis and establish the research requirements needed to determine a resolution for each of the proposed questions. Next, the research model is proposed which outlines four specific phases of research testing divided into Phase One and Two for initial testing and Phases Three and Four for stabilised testing. The system architecture, the necessary components and the software and hardware requirements are also discussed to provide information regarding the proposed system design. The data requirements of the research model are then investigated, outlining the data generation, collection, analysis and reporting methodologies that are required for each of the testing phases. The expected outcomes of each phase of research testing are then outlined. The chapter concludes with a consideration of the limitations of the proposed research model establishing the scope of the testing to be conducted.

Chapter Four reports the findings for each of the research testing phases. First, the variations to the previously proposed data requirements are identified and the subsequent modifications then applied to the proposed methods. The reported testing findings are then divided into initial and stabilised testing, with the corresponding four separate phases of testing followed by the analysis of the data gathered. Summing up, the significant and analysed results from the research testing are finally presented in graphical form to visually display the attained findings.

Chapter Five is a discussion of the research findings. To start with, the research questions developed earlier are revisited and arguments made for and against the associated hypotheses are tabled so that a synopsis of the learnt information and results achieved from the testing phases can be viewed. The research findings are then examined at length; each phase of testing is discussed, as well as an extensive evaluation of the system design developed and implemented for the research testing. Finally, recommendations are suggested based on the outcomes which were discovered during the conducted research.

Chapter Six concludes the thesis and recommends further areas for study. A conclusion of the research project is presented, stating the most important findings that were achieved and discussing the capabilities of the proposed and tested system design. Limitations of the research are outlined and discussed to identify constraints in the research conducted and findings discovered. Finally, potential future research areas involving WLANs and performing digital forensic investigations complete the chapter.

The appendices at the end of the thesis provides additional information regarding the findings; including a full set of results from testing, the hardware and software specifications of the devices used, various configuration files and other log files collected during testing.

Chapter Two

LITERATURE REVIEW

2.0 INTRODUCTION

The main research objective of Chapter 2 is to critically review the current literature relevant to the two study areas which were introduced in Chapter One; namely Wireless Local Area Networks (WLAN) and digital forensic principles. First of all it is vital to understand all aspects of wireless networking technology, the standardization process, security, potential threats and attacks, and the growing concern involving the potentially illegal and intended misuse of WLANs. The link is then made to the second topic, that of wireless digital forensics and the need for enquiry into the present-day knowledge of the relatively new field for the acquisition, preservation, analysis and reporting of wireless digital evidence.

The literature review will not only serve as a fact-finding undertaking, but will also identify where prospective problems and issues exist from which to derive potential research questions. Chapter 2 is structured into eight main sections. Sections 2.1 to 2.4 will present WLAN standards, security capabilities relevant to WLAN technologies, threats and attacks and thereafter the details of how and why WLAN communications technology may be intentionally misused. Sections 2.5 and 2.6 will discuss the process of digital evidence that is able to be obtained from a WLAN. Intrusion Detection Systems (IDS) are also reviewed in depth in Section 2.7 for their capabilities and use in a WLAN. Finally, the problems and issues pertaining to WLANs that were encountered in the literature review are identified and these are listed and discussed in Section 2.8, forming the foundation of the research needed in the area of WLAN forensic investigation.

2.1 WLAN STANDARDS

WLAN technology first originated and was defined by the IEEE 802.11 standard in 1997. It was designed to support medium-range high data rate applications similar to Ethernet capabilities, as well as allowing the use of mobile and portable stations to be connected to the network (Karygiannis & Owens, 2002, p.19). The following section will discuss the IEEE 802.11 standard, the technology background, specific amendments made to the standard, WLAN network architecture and the commercialised version of the 802.11 standard in Wi-Fi certified devices.

2.1.1 IEEE 802.11 Standard

802.11 WLAN networking technology is detailed and maintained by the IEEE, a professional non-profit international organization whose goal is to advance innovation and technology. The 802.11 standard is written and controlled by a Working Group of IEEE members who contribute to producing the 802.11 standards and amendments. The IEEE Standards Association (IEEE-SA) controls the standardization process of technologies and produces the standards documents offering balance, openness, due process and consensus.

2.1.1.1 802.11 background

The first 802.11 standard, released by the IEEE-SA in 1997 and outlined in the IEEE Standard 802.11-1997 specification document, is now known as the 802.11 legacy. It defined the WLAN Medium Access Control (MAC) and Physical Layer (PHY) specifications for 802.11 WLANs. According to the IEEE Std. 802.11 (1997, p.1) the intention of the 802.11 legacy standard was to develop a specification for wireless connectivity for fixed, portable and mobile stations within a local area. Furthermore, the specification was to allow network communication over wireless links, in contrast to the wired Local Area Networks (LAN) infrastructure standards that were available at that time. In 1999 the 802.11-1997 standard was revised to become the 802.11-1999 standard (IEEE Std. 802.11, 1999, p.iv). Currently, the most recent published 802.11 standard is the IEEE Std. 802.11-2007 (IEEE Std. 802.11, 2007, p.iv), a fully revised version, incorporating the many amendments that had been made since the second revision in 1999.

2.1.1.2 802.11 standard amendments

The amendments made to the standards are technically not an officially released new standard, but instead are additional specifications applicable to the existing current standard at that time. Table 2.1 shows the published standards of IEEE 802.11 identified by the year in which they were released as well as major specification amendments associated with that standard.

According to Frankel et al. (2007, p.19), the IEEE introduced the first two amendments to the 802.11 standard, 802.11a and 802.11b, which define the radio transmission methods and equipment used in WLANs. “802.11b quickly became the dominant wireless technology” (Frankel et al., 2007, p.19). It operates on the Industrial, Scientific and Medical (ISM) 2.4 GHz frequency band that offers data rates of up to 11Mpbs, and was intended to provide WLAN performance and security features to rival wired LANs. In comparison, 802.11a operates on the Unlicensed National Information

Infrastructure (UNII) 5.0 GHz frequency band and is therefore not compatible with 802.11b WLANs. However, 802.11a offers higher data rates of up to 54Mbps and the possibility of less radio interference compared to the 2.4 GHz ISM frequency band.

Table 2.1: IEEE 802.11 WLAN Standards and Amendments (Varshney, 2003, p.103; IEEE Std. 802.11i, 2004, p.i; IEEE Std. 802.11, 2007, p.iv; IEEE Std. 802.11n, 2009, p.i).

Standard	Released	Comments
802.11-1997	1997	First WLAN standard, 2.4GHz, 2Mbps, known now as 802.11 legacy.
802.11-1999	1999	Revised version of the original standard.
802.11a	1999	5.0GHz, 54Mbps.
802.11b	1999	2.4GHz, 11Mbps.
802.11g	2003	2.4GHz, 54Mbps.
802.11i	2004	Revised security amendment to 802.11-1999.
802.11-2007	2007	Currently latest published standard, incorporating the amendments 802.11a, b, d, e, g, h, i and j.
802.11n	2009	2.4 & 5.0GHz, 100Mbps, higher bandwidth amendment.

Scarfone, Dicoi, Sexton & Tibbs (2008, p.12), state that 802.11g was released in 2003 as a further amendment to the 802.11-1999 standard. It specified updated radio transmission methods using the 2.4 GHz ISM band allowing increased data rates of 54Mbps compared to 11Mbps offered in 802.11b. Subsequently, 802.11g then became widely adopted as the preferred technology used in WLANs, because of the interoperability with the 802.11b technology and the higher data rates achieved by the amendment.

The 802.11i security amendment was published by the IEEE Std. 802.11i (2004, p.iv) in 2004. It established enhanced security services and mechanisms for IEEE 802.11 MAC layer beyond those provided by the Wired Equivalent Privacy (WEP) mechanism first outlined in the IEEE 802.11-1999 Standard. Frankel et al. (2007, p.11) state that the 802.11i amendment introduced the use of a Robust Security Network (RSN) framework allowing the creation of Robust Security Network Associations (RSNA). RSNA included the introduction of authentication servers (AS) to the existing 802.11 architecture providing service to stations using the Extensible Authentication Protocol (EAP) standard.

The latest amendment, currently applicable to the 802.11-2007 standard, was the addition of 802.11n in 2009. According to the IEEE 802.11 Std. 802.11n (2009, p.ii), the amendment defines modifications and enhancements to the MAC and PHY layers to enable modes of operation that are capable of higher throughput speeds up to 100Mbps. Furthermore, IEEE Std. 802.11n maintains backwards compatibility with 802.11a, b and g, through operation on the 2.4 and 5.0 GHz bands, and almost doubles the effective range of WLANs (Scarfone et al., 2008, p.12).

2.1.1.3 802.11 architecture

The 802.11 standard defines the wireless networking architecture that is used when implementing a WLAN based on these standards. There are two fundamental architectural components used in a WLAN; a Station (STA) and an Access Point (AP). A station is defined as "any device that contains an IEEE 802.11-conformant medium access control and physical layer interface to the wireless medium" (IEEE Std. 802.11, 2007, p.14). Therefore, a station is a wireless endpoint device, where typical examples include laptop computers, personal digital assistants (PDA), mobile phones and any other electronic devices with IEEE 802.11 capabilities (Frankel et al., 2007, p.22). In comparison, an AP is any entity that has STA functionality and also provides distributed services via the wireless medium for associated STAs (IEEE Std. 802.11, 2007, p.5). An AP is therefore used to establish connections for wireless devices to the Distributed System (DS), usually a wired infrastructure. Additionally, the IEEE Std. 802.11 defines two WLAN design structures or configurations when using the 802.11 technology with STAs and/or APs. These two modes are known as Ad Hoc mode and Infrastructure mode.

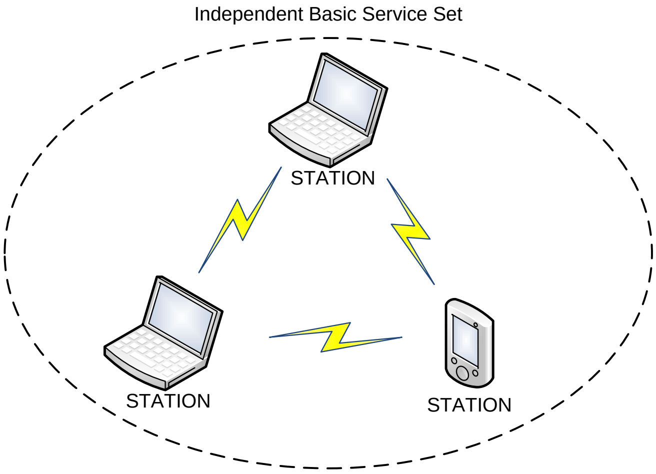

Figure 2.1: IEEE 802.11 Ad Hoc Mode (adapted from Frankel et al., 2007, p.22; Scarfone et al., 2008, p.15).

Ad Hoc mode, also known as peer-to-peer mode, is possible when two or more STAs communicate directly with each other (Frankel et al., 2007, p.22). Furthermore, STAs that are implemented in an Ad Hoc mode are collectively known as an Independent Basic Service Set (IBSS). "A fundamental property of IBSS is that it defines no routing or forwarding, so all the devices must be within radio range of one another" (Scarfone et al., 2008, p.14). Ad Hoc networks have the advantage of being able to establish network connectivity between multiple devices in any environment. However, they lack the ability of communication with external networks. The Ad Hoc mode is depicted in Figure 2.1 which displays two laptop computers and a PDA in an ad hoc architecture.

In comparison to Ad Hoc mode, Infrastructure mode requires the use of APs to forward traffic frames from the connected STAs to the distributed system (Frankel et al., 2007, p.25). Infrastructure mode architectures are thus comprised of basic service sets (BSS) which include the AP and one or more STAs. An extended service set (ESS) occurs when multiple BSS networks are connected via the DS. Figure 2.2 displays a WLAN ESS Infrastructure mode architecture. Each separate BSS area is connected to the wired network via a switch.

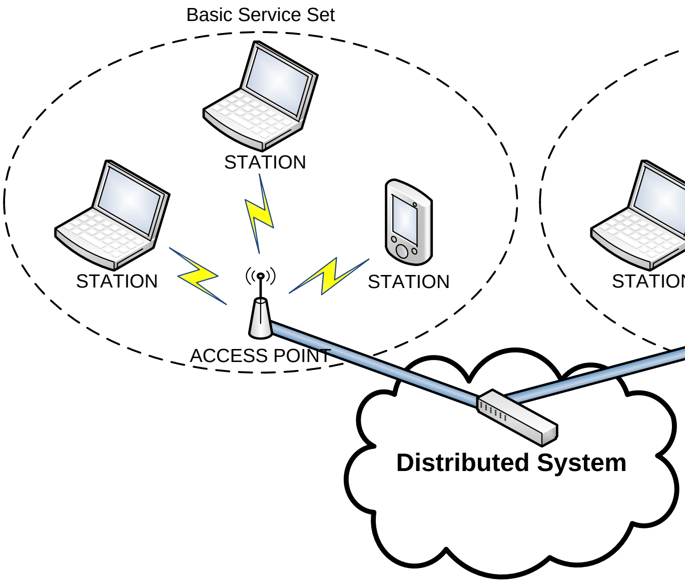

Figure 2.2: IEEE 802.11 Extended Service Set Infrastructure Mode (adapted from Frankel et al., 2007, p.24; Scarfone et al., 2008, p.17).

2.1.1.4 802.11 frames

In a WLAN, network communication is achieved by transporting wireless frames between devices in a network. The IEEE 802.11 standard outlines the MAC protocol to supply reliable delivery of user data over WLANs. According to Frankel et al. (2007, p.54), the IEEE 802.11 frame exchange protocol involves 3 different types of frames: management frames, control frames and data frames. Management frames carry the information necessary for managing the MAC layer, such as authenticating or associating devices, while control frames are implemented for requesting and controlling access to wireless media. An example of the use of control frames is the acknowledgement frame, which are sent after data frames to ensure reliability of the data transmitted over the wireless medium. Finally, “data frames encapsulate packets from upper layer protocols, such as Internet Protocol (IP) ... for the delivery of the upper layer protocol packets to a

STA or AP" (Frankel et al., 2007, p.54). Examples of such data include web pages or emails that may be transported using networking protocols such as Transmission Control Protocol (TCP).

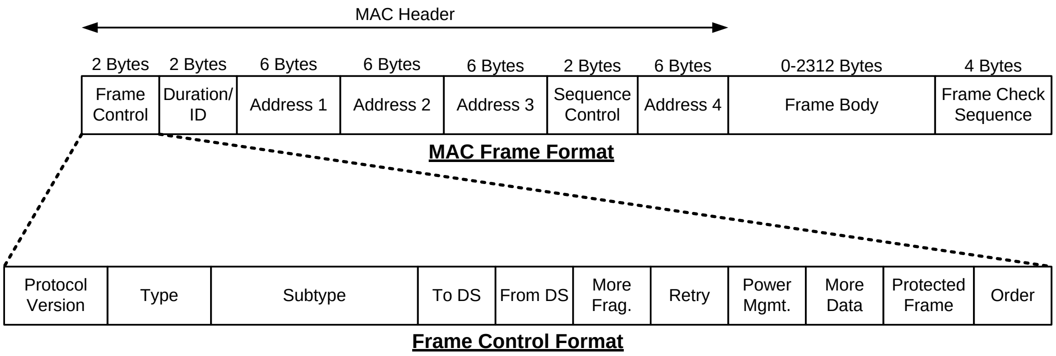

Figure 2.3: IEEE 802.11 Frame Format and Frame Control Field (adapted from IEEE Std. 802.11, 2007, p.60).

Figure 2.3 displays the frame format outlined by the IEEE 802.11 standard. The format described for 802.11 frames includes the MAC header, frame body and Frame Check Sequence (FCS) value. The MAC header is an especially important section of the 802.11 frame format, containing information regarding MAC addresses of the source and destination as well as the transmitter and receiver addresses (Frankel et al., 2007, p.55). An 802.11 data frame may also contain a frame body and a FCS value, which are not apparent in 802.11 control and management frames. The frame body is also known as the data field as it encapsulates higher level traffic, while the FCS value is utilized for error correction of the data frames being sent over the wireless network.

2.1.2 WiFi Alliance

The Wi-Fi Alliance (2009) is a global non-profit organization founded in 1999, with the goal of promoting a single worldwide standard for high-speed WLANs, based on the IEEE 802.11 standard of specifications. The Wi-Fi Alliance now has more than 300 member companies including large organizations such as Microsoft, Nokia, Intel, Dell and Cisco as well as prominent wireless chipset manufacturers such as Atheros and Broadcom. The Wi-Fi Alliance has grown to be an exceptionally important organization as they promote and certify the IEEE 802.11 set of standards with device manufacturers. The process is conducted via Wi-Fi Alliance Certification (2009) that test products according to the 802.11 industry standards for reliability, ease of installation, security and interoperability between devices of different manufacturers. Currently, the Wi-Fi Alliance has certified over 5,000 Wi-Fi products under four generations of Wi-Fi technology, 802.11a, b, g and n.

2.2 WLAN SECURITY

The following section discusses the built-in security features of the 802.11 standard for WLANs. The purpose is to identify and understand the security features available and to recognise the process by which they are implemented. Firstly, the general security objectives of Information Technology are identified and defined. Following are the WLAN security features, considered in terms of original 802.11 legacy security and also in terms of the subsequent release of the RSN framework (Figure 2.3). The security features implemented will be discussed only briefly so as to gain an insight to the methods used to secure WLANs. A more in-depth investigation would be both vast and complex and not in the scope of the literature review.

2.2.1 Security Objectives

As with other networking technologies and information systems, it is vital for WLANs to support and enforce several information security objectives. Fankel et al. (2007, p.27) outlines the following four common security features for WLANs: authentication, confidentiality, integrity and access control.

In terms of WLAN security, authentication can be defined as the service used to establish the identity of one STA as a member of the set of STAs authorized to associate with another STA or AP (IEEE Std. 802.11, 2007, p.5). Confidentiality ensures that communication cannot be read by an unauthorized party (Frankel et al., 2007, p.27), while integrity is the process of detecting changes to data that occur in transit, either intentional or unintentional. Finally, access control is defined as the process of the "prevention of unauthorized usage of resources" (IEEE Std. 802.11, 2007, p.5). These security objectives are intended to be met by using the built-in security features of the 802.11 standard.

2.2.2 802.11 Legacy Security

802.11 legacy security refers to the security features of the 802.11 standard prior to the 802.11i security enhancements amendment published in 2004. In some publications it is also known as Pre-Robust Security Networks (see Figure 2.4). Prior to the amendment IEEE 802.11i, WLAN security suffered from a number of serious flaws. These ranged from network encryption weaknesses to the implementation techniques of devices as many 802.11 legacy products had security disabled by default (Kent et al., 2006, p.28).

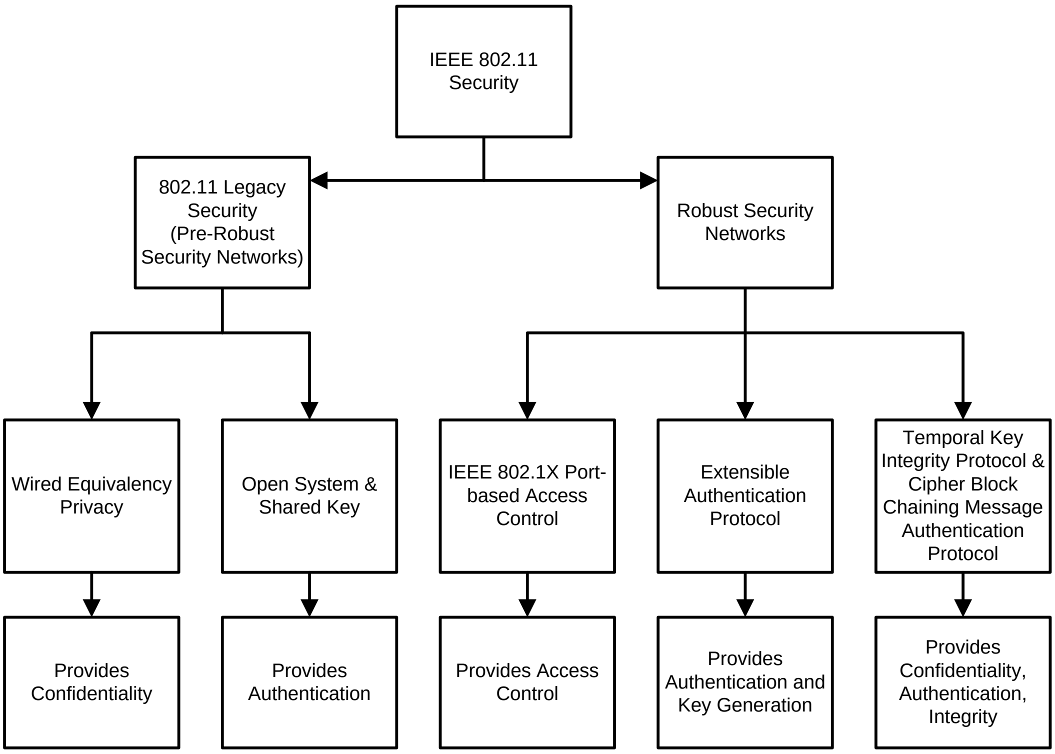
IEEE 802.11 Security
802.11 Legacy Security (Pre-Robust Security Networks)
Robust Security Networks
Wired Equivalency Privacy
Open System & Shared Key
IEEE 802.1X Port-based Access Control
Extensible Authentication Protocol
Temporal Key Integrity Protocol & Cipher Block Chaining Message Authentication Protocol
Provides Confidentiality
Provides Authentication
Provides Access Control
Provides Authentication and Key Generation
Provides Confidentiality, Authentication, Integrity

Figure 2.4: Taxonomy of 802.11 Security: 802.11 Legacy Security and Robust Security Networks (Kent et al., 2006, p.37).

The security services in 802.11 legacy networks are largely provided for by WEP. The technique is used to protect link-level data during wireless transmission between STAs and APs (Scarfone et al., 2008, p.29), but it is important to state here that WEP does not provide end-to-end security for network communication. Rather, the wireless traffic is encrypted between the STAs and APs only and, therefore, as soon as the transmission leaves the BSS it is no longer encrypted. The IEEE Std. 802.11 (1999, p.6) defines WEP as:

> The optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data 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.

WEP uses the RC4 (Rivest Cipher 4) stream cipher algorithm to encrypt wireless communication to protect transmitted data from disclosure (Scarfone et al., 2008, p.24). The originally released WEP standard implemented a 40-bit key, and is known as WEP-40 (IEEE Std. 802.11, 2007, p.158). However, the same algorithm has been widely used with a 104-bit key, known as WEP-104. An important input to the WEP protocol is the use of an initialisation vector (IV) as an input to initializing the cryptographic stream. The WEP protocol is conceptually illustrated in Figure 2.5.

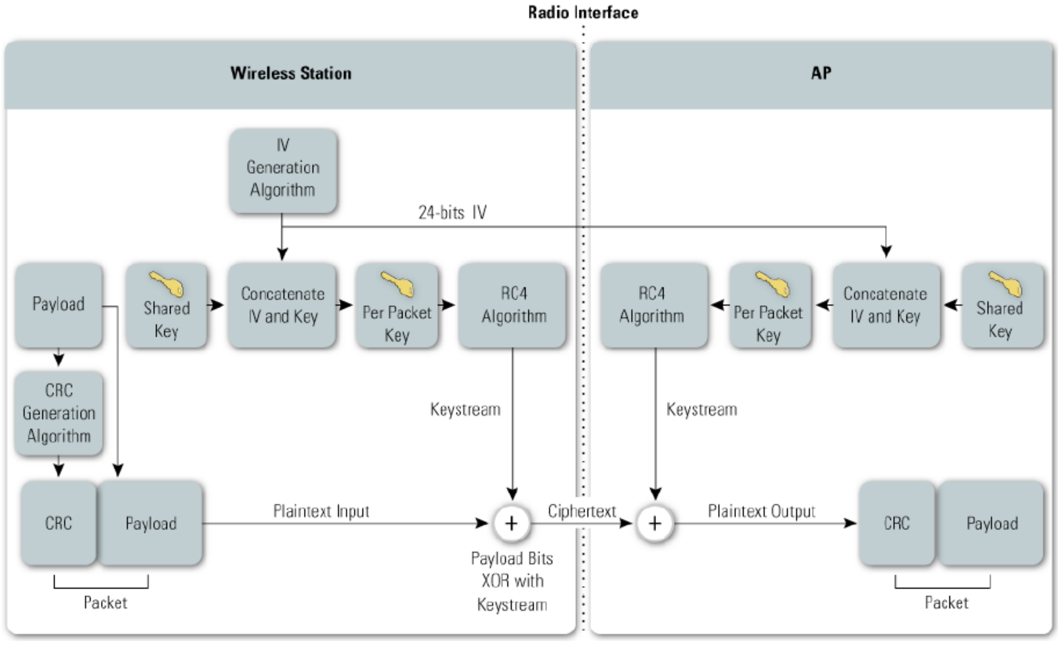

Figure 2.5: Wired Equivalent Privacy using the RC4 Algorithm (Scarfone et al., 2008, p.22).

Confidentiality in 802.11 WLANs is achieved with the use of WEP encryption which protects transmitted data from disclosure to eavesdroppers (Scarfone et al., 2008, p.23). Therefore, data may only be decrypted if the party has knowledge of the shared key used. With the shared key, the party is able to decrypt the encrypted network traffic into plaintext.

In 802.11 legacy security there are two forms of authentication techniques; open system and shared key. The open system authentication is a null authentication process where a STA always successfully authenticates with an AP (Housley & Arbaugh, 2003, p.33). The method dictates anybody is permitted to authenticate generating an ill-protected *modus operandi* that does not provide any authentication based on WLAN security objectives. The shared key authentication method utilizes a cryptographic technique. It is a simple challenge-response scheme which provides authentication based on whether the client has knowledge of a shared secret, the WEP key. “However, neither authentication method provides any true assurance of authentication” (Scarfone et al., 2008, p.22) due to the weakness of the generation method and the use of WEP keys. Ultimately, “WEP meets none of its security goals because of misuse of cryptographic primitives” (Cam-Winget, Housley, Wagner & Walker, 2003, p.39).

In 2003, as a response to the deficiencies associated with WEP, the Wi-Fi Alliance and IEEE 802.11 Working Group developed Wi-Fi Protected Access (WPA) as a security enhancement to replace the defunct WEP method (Scarfone et al., 2008, p.13). WPA uses the Temporal Key Integrity Protocol (TKIP) cipher suite to enhance the WEP protocol on 802.11 legacy hardware without causing the device performance degradation (Kent et al., 2007, p.44). Such performance degradation is easily possible due to the computational resources needed to perform encryption on digital devices. Therefore, WPA and the use of TKIP are based on the same RC4 algorithm used by the WEP protocol. However, the implementation of TKIP addresses security objectives such as integrity and stronger authentication which was lacking with the WEP protocol.

2.2.3 Robust Security Networks

The IEEE 802.11i amendment, published in 2004, allowed for enhanced security features with the introduction of the concept of RSNs via the process of creating RSNAs (Frankel et al., 2007, p.37). The developed concept is a type of authentication used by a pair of STAs when the authentication or association includes the 4-Way Handshake; that is, a pairwise key management protocol (IEEE Std. 802.11i, 2004, pp.3, 5). The protocol dictates that both parties possess a pairwise master key (PMK), while a Group Temporal Key (GTK) is distributed between them. However, "complete robust security is considered to be possible only when all devices in the network use RSNAs" (Frankel et al., 2007, p.38). As with 802.11 legacy security, "RSN security is at the link level only" (Frankel et al., 2007, p.38). As displayed in Figure 2.4, RSNs provide port-based access control, extended key management techniques to achieve authentication, TKIP and Cipher Block Chaining Message Authentication Protocol (CCMP) techniques to provide data confidentiality and integrity.

The Wi-Fi Alliance, endorsing the move to RSNS, then launched WPA2. "In conjunction with the ratification of the IEEE 802.11i amendment, the Wi-Fi Alliance introduced WPA2, its term for interoperable equipment that is capable of supporting IEEE 802.11i requirements" (Frankel et al., 2007, p.21). WPA2 is divided into Personal and Enterprise modes of operation. WPA2 Personal utilizes a pre-shared key (PSK, otherwise known as password mode) similar to WPA-PSK using TKIP, while WPA2 Enterprise utilizes central authentication with cryptographic certificates.

WPA2 Personal is accomplished by using the Counter mode with CCMP. It is a symmetric key block cipher introduced in the 802.11i amendment as a replacement for the use of TKIP. As with TKIP, CCMP was developed to address inadequacies of WEP. However, CCMP was also developed without constraint of implementation on existing hardware (Frankel et al., 2007, p.46). Therefore, CCMP utilizes a stronger core cryptographic algorithm in the form of the Advanced Encryption Standard (AES) and is considered a long-term solution for 802.11 WLAN security.

In comparison, WPA2 Enterprise implements EAP to authenticate devices in an IEEE 802.11 RSN. There are a number of EAP methods that may be implemented to ensure robust security between devices, utilizing authentication methods such as password, certificates and smart cards (Frankel et al., 2007, p.77). EAP is able to provide a higher level of security due to the methods of key generation and mutual authentication.

In summary, the IEEE 802.11 standard outlines a number of built-in security features to the wireless networking standard. These security features have greatly evolved since the initial publication in 1997. WEP, now seen as having major security deficiencies, has been replaced by WPA-PSK and WPA Enterprise modes of operation. These provide robust security for 802.11 WLANs from built-in security features that address the required security objectives including authentication, confidentiality, integrity and access control.

2.3 802.11 WLAN THREATS & ATTACKS

Although IEEE 802.11 WLANs have a number of built-in security features and have rectified potential security issues in the IEEE 802.11i amendment, there remains the risk that a WLAN may be misused and exploited by an attacker. The following section will, firstly, identify and discuss the potential security threats that WLANs may be exposed to. Secondly, known WLAN attacks are examined with detail to the method and effect of the attack on the wireless network.

2.3.1 802.11 WLAN Threats

A threat can be defined as the "potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm" (Shirley, 2000, p.169). Potential threats may be conducted via a vulnerability, which is "a flaw or weakness in a system's design, implementation or operation and management that could be exploited" (Shirley, 2000, p.189). Vulnerabilities are present on most information technology systems, however, not all these vulnerabilities result in a practical attack, nor does every attempted attack succeed. Table 2.2 displays a list of the major threats against IEEE 802.11 WLAN security features.

Some of the threats shown above are relevant to WLANs or wireless networking in general, and are inherent in the 802.11 WLAN standard. Threats range from passive eavesdropping of wireless network traffic to denial of service threats which prevent the normal usage of network resources. The threats outlined in Table 2.2 will be matched to currently known WLAN attack methodologies in the following section.

Table 2.2: Major Threats Against WLAN Security (Frankel et al., 2007, p.28).

Threat Category	**Description**
Eavesdropping	Attacker passively monitors network communications for data, including authentication credentials.
Traffic Analysis	Attacker passively monitors transmissions to identify communication patterns and participants.
Masquerading	Attacker impersonates an authorized user and gains certain unauthorised privileges.
Message Replay	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
Message Modification	Attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
Denial of Service	Attacker prevents or prohibits the normal use or management of networks or network devices.
Man-in-the-middle	Attacker actively intercepts the path of communication between two legitimate parties.

2.3.2 802.11 WLAN Attacks

In terms of computer security, an attack is defined as "an assault on systems security that derives from an intelligent threat ... to evade security services and violate the security policy of a system" (Shirley, 2000, p.12). Since the first IEEE 802.11 standard published in 1997, WLANs have suffered from a number of security threats and associated vulnerabilities. The 802.11i amendment, in particular, addressed many of these issues and was incorporated into the still current IEEE 802.11-2007 standard. However, due to the very nature of wireless communication technology, 802.11 WLANs may be monitored or attacked without physical connection to the network. Furthermore, the IEEE 802.11 standard only outlines the technology to be implemented and does not require all devices to meet specific standards. Therefore, 802.11 capable devices may not be implemented with correct security specifications creating potential security issues. Coupled with the security features not implemented by default on devices, as well as WLANs configured incorrectly by administrators, exposes WLANs making them vulnerable to practical attacks.

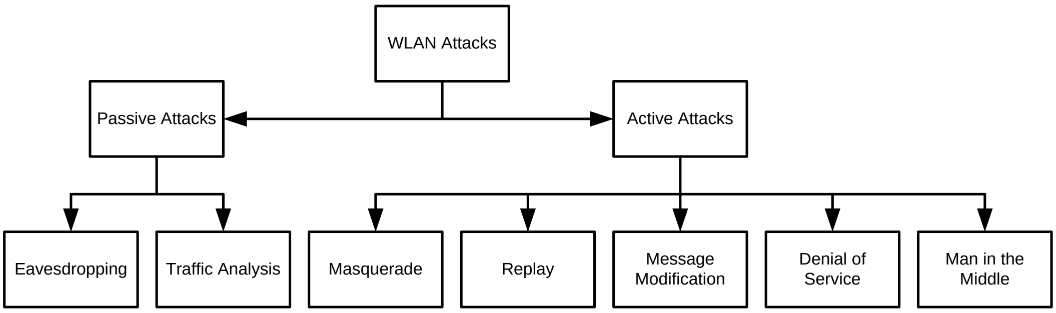

Figure 2.6: Taxonomy of WLAN Security Attacks (Karygiannis & Owens, 2002, p.3-19).

The WLAN threats displayed in Table 2.2 may be grouped into two different classes based on the method by which the attack is conducted. Figure 2.6 displays the threats to a WLAN grouped into either passive or active attack methodologies. Firstly, a passive attack can be defined as "attempts to learn or make use of information from the system but does not affect system resources" (Shirley, 2000, p.12). In a passive attack, the attacker does not interact with the WLAN, but passively listens to the network traffic. Passive attacks may incorporate eavesdropping on network traffic and also traffic analysis. A passive attack can be devastating to the security of a network as there is often no evidence or knowledge that the attack has occurred. In comparison "an active attack attempts to alter system resources or affect their operation" (Shirley, 2000, p.12). Thus, in an active attack, the attacker effectually interacts with the WLAN. Active attacks encompass replay attacks, masquerading, modification of messages, Denial of Service (DoS) and Man in the Middle (MITM) attacks.

Since the initial IEEE 802.11 standard was published, WLANs have suffered much scrutiny in terms of the security features that are incorporated into the standard. WLAN security was initially highly reliant on the WEP encryption protocol, thus WEP has had numerous security vulnerabilities discovered by researchers. One of the first research papers published regarding potential vulnerabilities in the WEP protocol was *Weaknesses in the Key Scheduling Algorithm of RC4* which discovered the use of the RC4 algorithm to be "completely insecure" (Fluhrer, Mantin & Shamir, 2001, p.1) in the mode of operation used by WEP. The attack described that the generated IVs used to initiate the WEP key could be collected and cryptanalysis performed to discover the WEP secret key. The attack was known as the FMS attack after the authors. Following the research there was further scrutiny of the WEP protocol, and further papers published which increased the speed at which IVs could be generated, therefore, increasing the speed of the cryptanalysis attack. An example is the fragmentation attack against WEP, which outlined how an attacker could send arbitrary data on an 802.11 network to increase the generation of the IVs after eavesdropping a single data packet (Bittau, 2005, p.1). Similar attacks, such as the KoreK ChopChop attack, were also developed, and allowed attackers to crack WEP encrypted networks in a quicker time frame.

Due to the discussed potential security issues in WEP, the Wi-Fi Alliance released the WPA encryption method. Shortly after the IEEE 802.11i amendment was published. Both of which provided increased security against the identified attacks against the WEP protocol. However, potential attacks have also been proposed against the WPA Personal, or WPA-Pre Shared Key (PSK), encryption method. For example, a dictionary attack may be launched against a weak PSK (Beck & Tews, 2008, p.1). Furthermore, additional attacks have been investigated in order to increase speed and reliability of WPA attacks.

There have also been a number of WLAN attacks that are not conducted against the encryption method implemented in a network. Such attacks focus on other weaknesses in the IEEE 802.11 standard. Examples include MITM, DoS and Fake Access Point (FakeAP) attacks (Frankel et al., 2007, p.28). Many of these attacks utilise the different 802.11 frames used in a WLAN to perform attacks. For example, the use of management frames to perform DoS attacks through the act of flooding the WLAN with deauthentication and disassociation frames which cause DoS attacks.

In conclusion it is evident that there are a number of threats and attacks identified and associated with the IEEE 802.11 standard wan WLANs raising the concern of potential security issues and the need for investigative technologies.

2.4 WLAN MISUSE

To understand the reason for conducting a forensic investigation and evidence acquisition on wireless networks, it must first be established why wireless technologies should be included in the digital forensic investigative process and how they may be misused with intent. There have been a number of criminal cases worldwide in which an attacker or unauthorized person has been involved in the misuse of wireless networks. Slay & Turnbull (2005, p.2-3) identified six separate cases, occurring between 2002 and 2004, which, in some manner, involved the misuse of 802.11-based wireless networks. These cases ranged from theft of intellectual property, credit card fraud and network intrusion, to using an insecure wireless signal for an anonymous internet connection. “The most interesting common theme with the cases above relates to how these offenders were caught – all were caught by a combination of bad luck, poor choice of target, their own admission, or by not obscuring their own tracks” (Slay & Turnbull, 2005, p.4). The following section will outline possibilities of how a WLAN may be misused with intent, and why such misuse occurs.

2.4.1 Taxonomy of 802.11-Based Misuse

Slay & Turnbull (2006) proposed the taxonomy of 802.11-based misuse to include technical considerations, methodology of attack, types of devices used and motivation of the misuse. The taxonomy does not include the unintentional misuse of a WLAN by authorized persons, such as an employee of an organisation using the network. Rather, the taxonomy describes the misuse based on the deliberate intent of an unauthorized party (the attacker) to commit a crime using the WLAN technology.

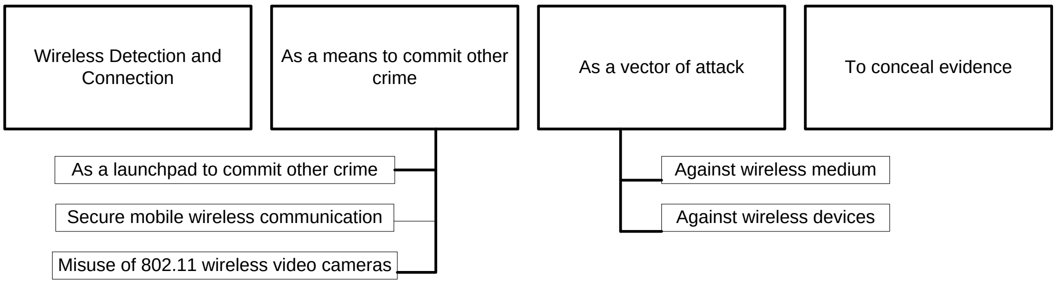
Wireless Detection and Connection
As a means to commit other crime
As a vector of attack
To conceal evidence
As a launchpad to commit other crime
Secure mobile wireless communication
Misuse of 802.11 wireless video cameras
Against wireless medium
Against wireless devices

Figure 2.7: Taxonomy of 802.11-based Misuse (Slay & Turnbull, 2006, p.124).

Figure 2.7 shows the four classifications of 802.11-based misuse; wireless detection and connection, as a means to commit other crime, as a vector of attack and to conceal evidence.

'Wireless Detection and Connection' refers to the discovery of and connection to wireless networks which allow the client an anonymous connection. Slay & Turnbull (2006) state that an unidentified connection can be the consequence of poorly configured wireless hardware, intentionally free accessible wireless connections and commercial wireless 'hotspots'. All of these aspects can result in an unnamed wireless connection where further misuse could occur, such as using the wireless network as a vector of attack or perhaps as a means to commit other crime.

'As a means to commit other crime' outlines how wireless systems can be misused to commit a crime unrelated to the network being breached. Slay & Turnbull (2006) describe three major categories when a wireless medium is used in such a scenario. Firstly, as an unidentified launchpad to commit further crime, where an attacker uses a wireless network to gain anonymous access to the internet or the internal network of the target. In such a situation the event origin can only be traced back to the wireless connection. Secondly, to establish secure wireless communication. An example of this would be wireless networks being misused to conduct secure communications using communication protocols such as VoIP (Voice over Internet Protocol) on an 802.11 wireless network. If compared to other similar forms of radio communication, such as mobile phone networks, there are known techniques and tools available to intercept communications and store the resultant evidence acquired. The third category covers the misuse of wireless video cameras which may include illegal filming of individuals or of specific areas such as restrooms.

'As a vector of attack' describes the misuse of wireless networks to gain access to network resources or to clients within the network. Slay & Turnbull (2006) detail the following two scenarios where such misuse of wireless systems may occur. Firstly, as a vector of attack against devices in the network. Wireless network devices can include access points, clients or other devices attached to the network such as printers and servers. Common types of attack include connecting to an insecure wireless network, rogue access points, MITM attacks and evil twin attacks. Secondly, as a vector of attack against the wireless medium which relates to the availability of the wireless service. Wireless networks that operate in an unlicensed radio frequency spectrum are subject to quality of service issues due to both interference and denial of service attacks. The final misuse classification refers to the ability to conceal evidence utilizing wireless communication technologies. For example, it is possible to hide potential digital evidence by using a wireless device to hide other devices such as a network attached storage unit.

The preceding information concerning wireless systems misuse substantiates the need for strategies and procedures to be set in place and reinforces the fact that there is a requirement for investigative tools and techniques to perform wireless digital forensic investigations.

2.5 WLAN FORENSICS

The origin of the word forensic comes from mid 17th Century Latin *forensis* meaning "in open court, public" from *forum* (Oxford Dictionary of English, 2e, 2003). It relates to the "application of scientific methods and techniques to the investigation of a crime" (Oxford Dictionary of English, 2e, 2003). The processes of a wireless digital forensic investigation involving network forensic methodologies will be described in the following section. The digital evidence gathered from an electronic device is subject to scrutiny, in particular regarding viability, and thus assessment is made in accordance with standards , recommending the guidelines to follow. The stated guidelines will be reviewed as well as currently available digital forensic procedure guides setting out investigation techniques recommended for conducting wireless forensic investigations.

2.5.1 Digital Forensics

There are a number of definitions and models that have been proposed for digital forensics. However, most reflect the same basic principles and overall methodology. Kent et al. (2006, p.16) state that the forensic process is comprised of collection, examination, analysis and reporting of digital evidence. In addition, the Scientific Working Group on Digital Evidence (SWGDE, 2006, pp.3-9) outline seizing, imaging, analysis and examination, and documenting and reporting as part of the digital forensic process. Furthermore, Brown (2006, p.7) defines the forensic process as collection, preservation, filtering and presentation of evidence. In all of the described scenarios it can be deduced that the gathering of digital evidence is the key area of digital forensics. The National Institute of Justice (NIJ) defines digital evidence as "information stored or transmitted in binary form that may be introduced and relied on in court" (NIJ, 2008, p.52). Which means that evidence collected must be viable, that is of a quality that can be used in a civil or criminal legal action and, thus, must comply with the standards of evidence presented in a court of law.

Given the legal requirements demanded of digital forensics, the four key domains or elements of the digital forensic investigation procedure are as follows; the identification and acquisition of digital evidence, preserving the integrity of the acquired evidence, forensic analysis or examination of acquired evidence, and the presentation and reporting of the obtained digital evidence in an appropriate manner. These four domains, and their interactions, can be seen in Figure 2.8

McKemmish (1999, p.1) defines the identification of evidence as the first step of the digital forensic process. It includes the recognition of what evidence may be present and where and how it is stored. This is especially important as digital evidence within a physical device cannot be confirmed until it is examined. Therefore the next step is the process of acquiring that evidence. After identifying the source of potential evidence, the acquisition, or collection, of it is determined by the appropriate technology to extract it. Furthermore, NIJ (2004, p.11) state that during the acquisition of the original digital evidence, the technique used needs to protect and preserve the soundness of the evidence to ensure that no change has taken place.

The preservation process of digital forensics involves safeguarding the digital data that may contain potential evidence and to ensure the integrity is protected throughout the digital forensic process (ISO/IEC 27037 Standard WD, 2009, p.5). Moreover, preserving potential evidence should be initiated after the identification of that evidence and maintained throughout the acquisition and analysis stages of digital forensics investigations. McKemmish (1999, p.1) also states that certain circumstances may cause changes to the data which is unavoidable. In such scenarios it is imperative that the least amount of change to the data occurs.

According to the ISO/IEC 27037:2009 (2009, p.6) the analysis or examination phase of a digital forensic investigation involves the use of scientifically proven methods to determine the characteristics of the acquired digital data. Kent et al. (2006, p.16), describe the analysis process as analysing the results of acquired data using legally justifiable methods and techniques. In both cases, the investigator aims to discover digital evidence in a forensically sound manner, addressing the questions for initially conducting such an investigation. The analysis phase of digital forensics is generally regarded as the major domain of digital forensics; being able to discover evidence relating to the forensic investigation.

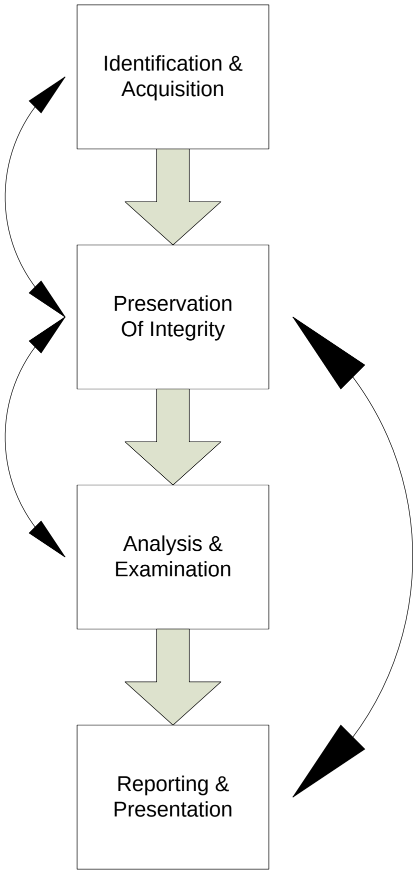

Figure 2.8: Digital Forensic Process (adapted from Brown, 2006, p.7; Kent et al., 2006, p.25).

"The presentation of digital evidence involves the actual presentation in a court of law" (McKemmish, 1999, p.2). The domain is also known as the reporting of digital evidence. The presentation of evidence attempts to convey the results that have been obtained in the digital forensic process; the analysis of digital evidence. Kent et al. (2006, p.16) outline that reporting on discovered digital evidence includes explaining what and how procedures and tools were used as well as the actions that were performed during the investigation.

2.5.2 Network Forensics

Corey, Peterman, Shearin, Greenberg & Van Bokkelen (2002, p.60) define network forensics as the process of capturing and archiving network traffic for later analysis of specific subsets. However, capturing and analysing network traffic is not the only method to gather viable potential evidence. Nikkel (2005, p.194) identifies a number of different sources that may be utilized to acquire evidence during the process of network forensics. These include analysis of IDS and firewall logs, backtracking network packets and TCP connections, collection of data from remote network services and the capture and analysis of network traffic using sniffers and Network Forensic Acquisition Tools (NFAT). "A network forensics analysis tool (NFAT) can provide a richer view of the data collected, allowing you to inspect the traffic from further up the protocol stack" (Corey et al., 2002, p.60).

A digital forensic investigation involving networks can vary in scope and complexity. There are numerous reasons for conducting investigations into electronic crime involving networking in general which range from computer intrusion to identity theft.

2.5.3 Digital Evidence

As explained earlier the purpose of conducting a digital forensic investigation is to obtain viable digital evidence from an electronic device.

> Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination (NIJ, 2008, p.ix).

According to the digital forensic procedure guidelines outlined by the NIJ, electronic devices may include computer systems, data storage devices, handheld devices, peripheral devices and computer networks. Given the nature of digital data, digital evidence has a number of unique properties that require specific procedures and techniques dictated by the four domains of digital forensics in order to secure the integrity. For example, digital evidence can be easily altered, damaged or destroyed if handled incorrectly.

The ISO/IEC 27002:2006 Standard: Information Technology – Security Techniques – Code of Practice for Information Security Management (ISO/IEC 27002, 2006, p.93) specifically outlines evidence guidelines in section 13.2.3: Collection of Evidence. The Implementation Guidance section indicates how evidence can be judged relative to its importance, which includes:

a) Admissibility of evidence: whether or not the evidence can be used in a court of law.
b) Weight of evidence: the quality and completeness of the evidence.

Furthermore, the ISO/IEC 27002:2006 standard specifically addresses evidence, or information on computer media, and outlines the following guidelines:

- Mirror images or copies of any removable media, information on hard disks or memory should be taken to ensure availability.
- A log of all actions should be kept and the process should be witnessed.
- The original media and the log should be kept secure and untouched.
- Any forensics work should only be performed on copies of the evidential material.
- The integrity of all evidential material should be protected.
- Copying of evidential material should be supervised, when, where and who should be documented as well as which tools or programs have been used.

2.5.4 Established Wireless Investigation Procedures

There are a number of procedural guides that have been documented, primarily for law enforcement, that outline the best practices to carry out digital forensic investigations involving identifying, acquiring, preserving and presenting digital evidence. "A digital investigation is a process to answer questions about the current or previous states of digital data and about previous events" (Carrier, 2006, p.58).

The NIJ *Electronic Crime Scene Investigation: A Guide for First Responders* (NIJ, 2008, p.vii) is intended to assist law enforcement and other first responders to recognise, collect and safeguard electronic evidence. Therefore, the guide is aimed at providing the first responders to a crime scene with the information and processes needed to conduct a digital forensic investigation of the scene. In terms of wireless investigation procedures, NIJ (2008, p.12) identifies wireless networking as a potential source of evidence, including wireless APs, wireless network servers, wireless cards and Universal Serial Bus (USB) devices as well as directional antennas used with wireless devices. NIJ (2008, p.12) identifies the possible evidence contents including log files, event logs and MAC or IP addresses. It also points out that wireless network equipment may be associated with computer intrusion investigations. Although wireless networking is identified and discussed in the First Responders guide, there is no specifically designated procedure for acquiring or preserving digital evidence involving wireless devices.

A second document produced by the NIJ, titled *Investigations Involving the Internet and Computer Networks* (NIJ, 2007a), discusses wireless networking during investigations of network intrusion and denial of service attacks. NIJ (2007a, p.59) expressly outline the following information to be collected during a wireless network investigation: The SSID broadcasting the wireless signal, if Dynamic Host Configuration Protocol (DHCP) was configured and maintaining logs, if WEP was enabled and any other log files containing information on wireless connections. However, there is no reference or steps on how to acquire or preserve the potential evidence. Such detailed information is needed when performing a wireless investigation as the methods and procedures are different when compared to traditional computer forensics. However, NIJ (2007a, p.59) does state that network investigations are technically complex and likely to require the assistance of specialized experts in the field.

The Association of Chief Police Officers' (ACPO, n.d.) produce the *Good Practice Guide for Computer-Based Electronic Evidence* with information relating to investigators, first responders, evidence recovery and external consulting witnesses. The ACPO (n.d., p.16) outlines recommendations when an investigation involves wireless networks including, using a wireless network detector to determine if a wireless network is in operation, isolate the wireless network by unplugging the wired link (if applicable), collect, photograph and document the discovered devices according to normal digital forensic principles. It also reiterates that "due to the potential complexity of technical crime scenes, specialist advice should be sought when planning the digital evidence aspect of the forensic strategy" (ACPO, n.d., p.15).

SWGDE (2006) produces the *Best Practices for Computer Forensics* procedure guide. The guide has no reference to conducting forensic investigations involving wireless devices; rather they provide guidelines for conducting traditional computer forensic investigations.

Although some wireless based information has been identified in most of the above discussed procedural guides, there is no specific information given on how to acquire, analyse or present digital evidence from wireless sources. Nevertheless, advancements have been made in general procedural guides since initial publications. A similar review of procedural guides by Turnbull & Slay state that:

> The development and maintenance of procedural guides that rely on interaction with technology is difficult, given the rate of change in the industry, and there is a constant need to update and adapt such works to ensure they are current (Turnbull & Slay, 2007, p.4503).

They go on to say that the only example that discusses wireless devices at all was the NIJ First Responders Guide. However, since the review a revised second edition of the guide has been released encompassing more comprehensive and up-to-date information. It is especially important to continue to address issues where there is no available information with reference to conducting a wireless digital forensic investigation. This is enforced by the increasing potentiality for attackers to exploit and misuse WLANs pointing to a call for a defined means and set of procedures to combat misuse.

2.6 WLAN SOURCES OF EVIDENCE

The resultant outcome from the process of digital forensics is digital evidence. Due to the unique nature of WLANs and wireless networking technology the sources of evidence in a WLAN environment differ greatly from that of a traditional computer forensic investigation. Turnbull & Slay (2008) group the possible sources of evidence from WLANs into either *post-mortem* or 'live' areas. Post-mortem sources include potential evidence from 802.11 capable devices and embedded wireless devices. Live sources include wireless network traffic interception and capturing of the traffic from the wireless communication spectrum. The following section will discuss each possible source of evidence in a WLAN, including 802.11 capable devices, wireless network devices and the wireless communications spectrum. Different types of wireless networking tools are also examined on the potential use in wireless forensics, including network discovery and packet capture tools as well as wireless intrusion detection systems.

2.6.1 802.11 Capable Devices

The identification and acquisition of electronic devices capable of 802.11 WLAN communication are a potential *post-mortem* source of evidence and may yield prospective evidence to assist with the digital forensic investigation. Such examples include personal computers, laptops, smartphones and PDAs. Turnbull & Slay (2008, p.1359) state that the type of wireless networking information stored and how that information can be extracted is dependent on the type of operating system used and how it is configured by the user. For example, the task of examining a personal computer is conducted via the process of computer forensics. Computer forensics is defined as "the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable" (McKemmish, 1999, p.1). Although very similar to the definition of digital forensics, computer forensics involves conducting digital forensic investigation on a computer system. Such practice may entail identifying and acquiring the device and obtaining a forensic copy of the computer's hard disk or volatile memory. The forensic copy may then be analysed to establish if any digital evidence exists. Digital evidence may include wireless network artefacts that are present on the host operating system. The reason for the operating system to store such information is to add ubiquity to the WLAN technology, storing wireless network data so the user does not have to enter the details every time they connect to a wireless network.

Microsoft Windows XP stores a list of preferred networks, which a user has selected to save when previously connecting to a wireless network. Table 2.3 displays the pertinent registry keys that may hold information regarding wireless network artefacts.

Table 2.3: Windows Preferred Networks Registry Entry (compiled from Turnbull & Slay, 2008, p.1359-1340 & Carvey, 2005, p.205).

Registry Location	**Information Available**
HKEY_LOCAL_MACHINE\Software\Microsoft\WZCSVC\Parameters\Interface	SSID of network, MAC address.
HKEY_LOCAL_MACHINE\System\Current\ControlSet\Services\TCPIP\Interfaces\GUID	Network settings for the network interface (IP address, DNS server).

Similar to Windows based operating systems, Apple Mac OS X also store the preferred list of wireless networks. According to Turnbull & Slay (2008, p.1360) the OS X operating system stores the list of preferred network in the following file:

/Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist
/Library/Keychains/System.keychain

System preferences regarding open wireless networks are stored in the first file location. The second file location holds information pertaining to encrypted 802.11-based wireless networks, including SSID and key required to establish network connectivity (Turnbull & Slay, 2008, p.1360).

Other potential information may also be obtained from a forensic copy of a computer’s hard disk. For example, the operating systems ‘computer name’ and the MAC address of wireless Network Interface Card (NIC). Such information can be used to trace an attacker’s computer to other data found from network forensics including network device logs. Furthermore, conducting computer forensics on an attacker’s computer may yield additional information regarding the device and wireless hardware used. Physical examination of the attacker’s computer may discover the MAC address of the device’s wireless NIC. It is common practice for manufacturers to list the MAC address on a sticker on the base of a laptop computer or the wireless adaptor itself. Also, the computer name of a client may be collected by the forensic examination of a system’s hard disk. A computer name could be used in the same way as a MAC address to tie a device to network logs, such as DHCP logs of distributed IP addresses to specific wireless devices.

2.6.2 Networked Devices

Another potential ‘post-mortem’ source of evidence from a WLAN is the device that is offering the wireless communication service. A common example would be a wireless AP. Turnbull & Slay (2008, p.1358) state that the possible information that may be extracted from an AP includes SSID naming convention, encryption type implemented, DCHP details of IP address distribution, MAC address filtering details and possibly log files. However, “the mechanics of the extraction of such information is dependent on the device, as there is no universal interface” (Turnbull & Slay, 2008, p.1358). Such investigation of network devices may be a lot easier to accomplish if the investigation is being conducted by the party who owns the wireless device. For example, if a wireless breach occurred in a corporate network the organisation would have access to the device, via a username and password to facilitate inspection of the wireless device. They would also have details regarding the type of information stored by the devices in the network such as log files.

2.6.3 Wireless Communications Spectrum

A further likely source of digital evidence from a WLAN is the actual network traffic that is being sent and received between WLAN devices. It is a form of ‘live’ evidence from a WLAN, as the network traffic needs to be collected in real-time. As stated previously, network forensics is the process of capturing and archiving network traffic for later analysis. Although such a technique was first adopted in wired network architectures, the same methodology may also be implemented in a wireless network environment. “Captured network traffic can be abstractly described as the preserved communication between multiple nodes on a network” (Nikkel, 2005, p.196).

Table 2.4: Advantages and disadvantages of the collection of wireless traffic as digital forensics evidence source (Turnbull & Slay, 2007, p. 4505).

Advantages	Disadvantages
Will provide forensic investigators with a network topography of 802.11 wireless devices.	The legality of such network interception depends on the investigators, local, state and federal law and may require a warrant.
Alert forensic investigators to the existence of multiple wireless networks, or movement of devices between networks.	The capture of wireless traffic during forensic seizure will require new processes and technology.
May provide forensic investigators with evidence that is unavailable through other means.	The capture of wireless traffic may give no benefit to investigators, and will require more analysis.

Turnbull & Slay (2007) say that the information able to be extracted from wireless devices from network traffic is amply sufficient to identify and classify live devices. These include the networks SSID, use of encryption, communication channel, MAC address of the AP and approximate geographic location of devices. In addition, "captured network traffic is a particularly compelling form of evidence because it can be used to show all of the offender's actions, like a videotape of a convenience store robbery" (Casey, 2004, p.28). Table 2.4 displays the advantages and disadvantages of the collection of wireless traffic as a source of evidence.

2.6.3.1 Wireless network discovery tools

There are two different methodologies that wireless network discovery tools use to detect, monitor and log a WLAN device, one being active scanning and the other passive scanning. Both methods gather information pertaining to the WLAN's AP by capturing and decoding a beacon frame which contains network information including SSID, BSS Identification (BSSID) and the network encryption implemented. Most of these tools were originally developed for non-forensic applications, such as wardriving, network monitoring, network spectrum analysis and network management.

Vladimirov, Gavrilrnko & Mikhailovsky (2004) state that the active scanning methodology for wireless network discovery involves broadcasting a probe request frame and waiting for responses from available wireless networks. Use of the active scanning method can retrieve information including the WLAN's ESS Identification (ESSID), BSSID, operation channel, signal strength and the presence of network encryption. An example of an active wireless scanner is NetStumbler, or Network Stumbler, which is a licence-free Windows tool that can detect WLANs using 802.11a, b or g (Milner, 2004). There is also a portable version of the NetStumbler tool, MiniStumbler, designed for Windows Mobile devices. Although both tools have not been updated since 2004 (version 0.4.0), Milner (2010) has stated that a new release of NetStumbler is currently being developed, adding usability on Windows Vista and 7, and other additional features such as advanced Global Positioning System (GPS) support and integration with Kismet drones. Currently, NetStumbler has the ability to actively probe WLANs for network information, including SSID, encryption type implemented, AP MAC address and AP signal strength. Another similar Windows based tool is inSSIDer by MetaGeek (2010) which has the means to actively scan and identify 802.11 WLANs and provide information on the SSID, BSSID, signal strength, communications channel and encryption type implemented.

In contrast, Vladimirov, Gavrilrnko & Mikhailovsky (2004) then maintain that passive scanning methodology utilizes the most practical wireless network discovery tools to discover wireless devices by detecting, capturing and analysing wireless traffic. Passive scanning based wireless network detection is deemed a superior method because any wireless based device may be discovered, that is the ability to detect clients connected to a WLAN, whereas active scanning is only able to identify APs. Passive scanning wireless network monitors may also have the ability to reveal hidden or cloaked WLANs. There are a number of wireless network discovery tools which utilize passive scanning to detect and monitor WLANs, including Kismet, KisMAC, airodump-ng and AirPCap. All of these tools have the ability to perform wireless network discovery even though their principle function involves another goal of wireless packet capture.

Table 2.5: Active Scanning vs Passive Scanning Methodologies: Key Differences.

Active Scanning	**Passive Scanning**
Actively sends probe request frames to perform wireless network discovery.	Passively intercepts wireless network traffic to perform wireless network discovery.
Does not intercept or collect any wireless network traffic.	Capability to intercept and collect wireless network traffic.
Capability to provide WLAN AP information such as SSID, BSSID, signal strength and other network properties.	Capability to provide WLAN AP information, as well as client STA details.

In summary, and in terms of forensic capabilities, there is a wide difference between active and passive scanning methodologies as shown in Table 2.5. Active scanners, such as NetStumbler and inSSIDer, currently do not have the ability to capture wireless packets compared to passive scanning which can both detect WLANs and capture wireless network traffic.

2.6.3.2 Wireless network packet capture tools

Wireless network traffic may be monitored and captured by utilizing a wireless network sniffer or a wireless NFAT. According to Shirley (2000, p.162 & 192), sniffing is defined as passive wiretapping, when the network traffic flow is only observed in order to gain knowledge of information that it contains. In comparison, active wiretapping alters the network traffic. Packet sniffers are designed to monitor network traffic and capture packets on wired or wireless networks. According to Kent et al. (2006), a NIC normally only accepts incoming network packets that are specifically directed to it, but when a NIC is placed in monitor mode all incoming packets can be seen regardless of their intended destinations. Monitor mode is also referred to as raw or Radio Frequency Monitor (RFMON) mode. Table 2.6 shows an overview of wireless packet capture tools.

Table 2.6: Wireless Network Packet Capture Tools: Capability Overview.

Tool	**Capability**
Kismet	Wireless network detector, sniffer and IDS capabilities. Multi-platform (Linux, OS X). Extensive filtering and logging capabilities.
Wireshark	Wireless network sniffer. Supports 802.11 frame, as well as a great many other network protocol capture and analysis. Extensive filtering, live analysis and logging capabilities. Various included tools to merge, divide and manipulate packet capture files.
AirPCap	Specialised hardware device to provide ability to intercept and collect wireless network traffic from Windows hosts.
KisMAC	Wireless network detector and sniffer. Active and passive scanning methodologies. OS X platform only.
Airodump-ng	Wireless network detector and sniffer. Simple user interface with traffic filtering capabilities. Multi-platform (Linux, OS X).

According to Kershaw (2010), Kismet is an open source 802.11 layer2 wireless network detector, sniffer, and intrusion detection system which uses a NIC in monitor mode to sniff 802.11a, b, g and n based WLAN traffic. Kismet also has abilities beyond wireless network detection such as sniffing wireless traffic and additional IDS functionalities. Currently, Kismet may be run on most popular operating systems including Linux and UNIX variations, Microsoft Windows and Apple OS X.

Wireshark is an open source network protocol analyser, providing capabilities to allow the capture and analysis of network traffic. Wireshark has built-in support for the 802.11 WLAN standard and is available for use on popular OSs including Linux, OS X and Windows based systems.

Another tool, produced by CACE Technologies (2010), is the AirPCap wireless USB device which supports full 802.11 WLAN passive packet capture on a Windows platform, Wireshark integration, multichannel monitoring, and packet transmission in selected models. According to Meghanathan, Allam & Moore (2009), full 802.11 capture using AirPCap can capture the control frames (ACK, RTS, CTS), management frames (Beacon, Probe Requests and Responses, Authentication) and data frames of 802.11 WLAN network traffic.

KisMAC (n.d.) is another wireless network tool that utilizes passive sniffing methodologies and monitor mode wireless NICs, developed specifically for the Apple Mac OS X operating system and associated hardware in such devices. Features of the KisMAC application include displaying the WLAN client's MAC address, IP address and signal strength, revealing hidden SSIDs, support for 802.11b and g, as well as packet capture (pcap) file import or export.

Another tool designed specifically for wireless packet capture is airodump, being part of the aircrack-ng suite of wireless tools. Airodump-ng (2010) also utilizes wireless NICs in monitor mode to discover WLANs and associated clients. Airodump is a command line (CLI) application that is able to list AP, BSSID, SSID, signal power and encryption implementation as well as detailed client information including MAC address and packet capture. Moreover, airodump is extremely adaptive for use in different scenarios by the application of extensive filters and command line switches. For example, wireless packet sniffing can be filtered by BSSID, SSID or the channel used. Such information can be very helpful when isolating which devices are included in the scanning and packet capture process.

2.6.3.3 Network packet analysis

As previously discussed the analysis phase of digital forensics involves examination of the gathered data and isolating the potential evidence from the entire data set. Wireless network traffic is collected and stored in a pcap file format. Wireless network traffic is initially captured in the 802.11 frame format. However, after decryption of traffic, the resultant packet capture is similar to that of wired network traffic and contains higher level network protocol packets, such as TCP packets.

In an open network that is not protected using a form of network encryption, packet analysis is considerably easier due to the fact that the network traffic does not first need to be decrypted in order to be analysed. However, such a scenario provides no security from eavesdropping attacks which may also capture and view network traffic. In comparison, the use of encryption on network traffic scrambles the packet data to provide confidentiality to members of the network. The original WEP encryption is able to be decrypted if knowledge of the secret key is known. No other variables are needed.

Although WPA decryption is achievable, with knowledge of the PSK or certificate used, there are a number of other factors that affect the ability to conduct decryption. Chen, Yao & Wang (2010, p.168) state that WPA encryption traffic may be decrypted, to some extent, using the 4-way handshake packets generated to establish encryption between the communicating AP and STA. Without the 4-way handshake data, encryption variables used during WPA implementation are unavailable and decryption of acquired network traffic packets cannot be achieved. It should also be noted that any traffic collected before the 4-way handshake is not able to be decrypted either. Although the use of WPA hopes to ensure security objectives are maintained, it may have a negative effect on the ability to perform forensic investigation on the wireless traffic collected. Currently, there are a number of tools available that have the means to decrypt both WEP and WPA encrypted traffic. Kismet is one of these tools and has the ability to decrypt WEP encrypted traffic in real-time (Kershaw, 2010). Airdecap-ng, part of the aircrack-ng suite of tools, also has the ability to decrypt WEP and WPA PSK-based encrypted traffic from packet capture files (aircrack-ng, 2010). In addition, Wireshark also is capable of decrypting both WEP and WPA PSK-based encrypted traffic.

Although not specifically designed for network forensic analysis of captured traffic, there are a number of applications and tools available for conducting analysis of acquired network traffic. Arguably, the most popular network protocol analyser tool, Wireshark, has the ability to process packet capture files and apply a vast variety of filters to locate specific packets.

2.6.4 Intrusion Detection System as Source of Evidence

“Although the main aim of Intrusion Detection Systems (IDSs) is to detect intrusions to prompt evasive measures, a further aim can be to supply evidence in criminal and civil legal proceedings” (Sommer, 1999, p.2477). Depending on the type of IDS implemented there is the possibility that there may be potential evidence gathered and stored by the IDS, including basic event characteristics, such as date and time, source and destination network addresses and protocol used (Kent et al., 2006, p.66). Application data may also be collected, such as username and filename applied within the application.

There have been a number of papers that propose network forensics systems, for both wired and wireless networks, could be based on using an Intrusion Detection System. Sommer (1999, p.2477-2487) proposes the use of an IDS as a source of evidence for network forensics and lists enhancements regarding redesigning an IDS output as a form of reliable digital evidence. Kahai, Srinivasan and Pendse (2005, pp. 153,163) propose a forensic profiling system, based on the use of an IDS, to enhance the data gathered and the possibility of potential digital evidence from a network intrusion event. Yim, Lim, Yun, Lim, Yi and Lim (2008, p.197) also propose the use of a forensic profiling system for WLANs based on an IDS to detect and log possible intrusions for potential evidence.

It can, therefore, be seen that the use of an IDS system as a source of evidence in a WLAN has a number of benefits for forensic purposes. For example, an IDS will detect attacks or intrusions and generate an alert from the information gathered. The generated alert is then examined against the network packet capture, thereby providing details of possible evidence and isolating data from a full set of acquired network traffic. Since wireless network packet captures can comprise of hundreds of megabytes of data, the ability of an IDS to separate the possible evidence from a large packet capture file is an advantage to forensic analysis.

2.7 INTRUSION DETECTION SYSTEMS

It has been discussed that intrusion detection systems can be used in the process of conducting forensic investigation and evidence acquisition in WLANs. Scarfone & Mell (2007, p.1) define intrusion detection as the process of monitoring the events occurring in a computer system or network and analysing them for possible incidents which are in violation of the system's policies. In comparison, "Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents" (Scarfone & Mell, 2007, p.1). The following section will discuss the background of intrusion detection, types of IDSs and associated attack detection methodologies. Finally, wireless-based IDSs are investigated for functionality and availability of currently available systems.

2.7.1 Intrusion Detection Background

"Originally, systems administrators performed intrusion detection by sitting in front of a console and monitoring user activities" (Kremmerer & Vigna, 2002, p.27). The method was manually conducted was not scalable and consumed administrative time but, nonetheless, was effective during the period. In the 1970's and 1980's intrusion detection involved analysis of audit logs that system administrators reviewed for evidence of unusual or malicious behaviour. Again the method still relied on manual work to analyse the recorded log files. "In the early '90s, researchers developed real-time intrusion detection systems that reviewed audit data as it was produced" (Kremmerer & Vigna, 2002, p.27). The advance in technology created the first IDS solution that modern systems are now based on.

2.7.2 Intrusion Detection System Overview

According to Scarfone & Mell (2007, p.iv) an Intrusion Detection System (IDS) is software that automates the intrusion detection process, compared to an Intrusion

Prevention System (IPS) which is software that has all the capabilities of an intrusion detection system and also attempts to stop possible incidents.

Scarfone & Mell (2007, p.1) state that there are four types of IDS technologies: Host-based, Network-based, Network Behaviour Analysis and Wireless-based. Host-based IDSs monitor a single host machine and the events occurring within that host for suspicious activity. In comparison, network-based IDSs monitor network traffic for network segments or devices and analyses the network and application protocol activity for suspicious activity. Network Behaviour Analysis IDSs examine network traffic for threats that generate unusual traffic flows. Examples include the detection of DoS attacks, some malware and security policy violations. Finally, wireless-based IDSs monitor and analyse wireless network traffic to identify suspicious activity.

In addition to the different types of IDS technology, there are also different types of implemented detection methods to detect intrusions. The three major detection methods are signature detection, anomaly detection and stateful protocol analysis methodologies. According to Scarfone & Mell (2007, p.18), signature detection is achieved by matching a pattern that corresponds to a known threat. Therefore signature-based detection methods use known signatures to compare against observed events. Signature-based detection is also known as misuse detection. An example of signature-based detection is an e-mail with a "Free pictures!" and an attachment file "freepics.exe" which are characteristics of a known type of malware. In comparison, anomaly detection uses models of "normal behaviour" to map against observed events (Kemmerer & Vigna, 2002, p.28). A common example of anomaly detection is if a user logs into the network in the middle of the night, compared to normal network activity which involves users logging in during working hours. The last detection method, stateful protocol analysis, relies on predetermined profiles of benign protocol activity against observed events to identify deviations (Scarfone & Mell, 2007, p.19). Stateful protocol analysis is sometimes also known as deep packet inspection.

2.7.3 Wireless Intrusion Detection Systems

Wireless-based IDSs monitor wireless network traffic and analyse wireless networking protocols to identify suspicious activity involving the protocols themselves (Scarfone & Mell, 2007, p.2-6). It is important to state that a wireless IDS cannot identify suspicious activity in higher layer protocols, such as TCP and User Datagram Protocol (UDP) or the application data that the wireless network is transporting.

According to Yang, Xie & Sun (2004, p.554), a Wireless Intrusion Detection System (WIDS) may either have a centralised or decentralised network architecture. Such variant network architecture is needed because in wireless networks "no central point exists from which to monitor all network traffic" (Yang, Xie & Sun, 2004, p.555) due to the fact that wireless stations are independent nodes. A centralised WIDS is comprised of several individual sensors which collect and forward all 802.11 data collected to a central system. The central system stores and processes all of the 802.11 traffic that is received from the wireless sensors. In comparison, decentralised wireless intrusion involves a single device that performs the collection and processing of 802.11 data. An example of a decentralised WIDS is a single sensor configured to perform intrusion detection functions on a specific segment of the wireless network. When an IDS system identifies an intrusion, an alert is usually raised to notify an administrator that some form of intrusion has occurred.

It should also be mentioned that many of the WIDS systems available perform additional functions compared to traditional wired IDS, where the only goal is to detect and/or prevent attack. This is due to the nature of WLAN networking technology; hence, many available systems also provide the ability to perform network discovery, network packet capture, wireless spectrum analysis and infrastructure management. Although additional features may provide solutions to other unrelated requirements, it may hinder IDS development in primary applications owing to the concentration of development moving to other aspects of the application.

2.7.3.1 Existing WIDS systems

There are currently a number of products that are specifically designed as wireless IDSs to detect intrusion and/or prevent the attack from continuing. Currently, available commercial solutions include AirMagnet and AirDefense, and open-source solutions include Kismet and Snort-wireless.

AirMagnet, founded in 2001, is a part of Fluke Networks and offer a range of wireless management solutions including IDS/IPS management systems (Fluke Corporation, 2010). The AirMagnet range of IDS/IPS products includes AirMagnet Enterprise and AirMagnet WiFi Analyzer. AirMagnet Enterprise is comprised of a centralised server and distributed wireless nodes providing a distributed WIDS system. In comparison, the AirMagnet WiFi Analyzer is a mobile station, usually a laptop, which is available in an Express and a Pro version. The express version performs basic WLAN monitoring capabilities similar to other Wireless discovery and monitoring tools. However, AirMagnet Pro contains all the functionality of the AirMagnet Enterprise product. Capabilities include 802.11n support (with appropriate wireless NIC), classification and location techniques for unauthorised (rogue) devices and a range of attack detection including MDK3 AMOK MODE, 802.11n DoS and Karma attacks. Berghel & Uecker (2004a, p.19) describe the AirMagnet wireless IDS as feature rich and the “best-of-breed” wireless monitoring and scanning tool. However, the AirMagnet range of products is relatively expensive to purchase and licence. AirMagent Enterprise is approximately NZD$10,000 and comprises a total of 3 sensors.

Motorola (2010) produces a range of commercial solutions for WLAN security, compliance, infrastructure management and network assurance under the AirDefense range of products. In addition, Motorola (2010) state that AirDefense provides built-in forensic analysis capabilities for devices, threats, associations, traffic, signal and location trends.

According to Kershaw (2010), Kismet include wireless IDS functionality for layer 2 and layer 3 wireless attacks which is accomplished by either fingerprint analysis (specific single-packet attacks) and trends analysis (disassociation flood, unusual probes). Kismet is an extremely configurable application with complete control of all functionality available to the user, such as channel hopping features and a distributed architecture (Murray, 2009, p.7). The Kismet architecture consists of a Kismet server, client and drone. Kismet servers are configured to be the centralised server allowing connections from any available packet capture device. The Kismet client provides a graphical user interface (GUI) for the administrator to review the data that the Kismet server is collecting, while a Kismet drone is a remote dumb sensor that sniffs data and forwards it to the Kismet server. Distribution of drones to cover a WLAN with a central server creates a distributed WLAN IDS. The IDS alerts provided by the Kismet server application can be seen in Table 2.7. Although there are a total of 22 alerts defined in Kismet, many are outdated and not applicable to modern WLANs.

Table 2.7: Kismet IDS Alerts (compiled from Kershaw, 2010).

Alert	Description
APSPOOF	When a beacon or probe response contains an invalid MAC address of a predefined SSID.
BSSTIMESTAMP	Invalid or out-of-sequence timestamps indicate AP spoofing.
CHANCHANGE	A previously detected AP which has changed channels may indicate AP spoofing.
DEAUTHFLOOD	Denial of service attack, conducted by attacker spoofing disassociate and deauthenticate packets on the network.
DISASSOCTRAFFIC	Client which is disassociated from a network immediately begins exchanging data. May indicate a spoofed client.
DHCPNAMECHANGE/ DHCPOSCHANGE	DHCP hostname and operating system type may be in DHCP discover packets. If values change for a client, it may indicate a client spoofing attack.

Due to the nature of the Kismet application it may be run on various hardware devices from regular desktop PCs to small embedded devices. One popular example is the ability to run Kismet (especially the drone application) on the open-source wireless device firmware, OpenWRT. A wireless AP coupled with the OpenWRT firmware and a cross compiled Kismet drone package can provide a distributed, centrally managed wireless IDS system. Furthermore, Kismet also has the ability to integrate with other IDS systems by forwarding captured traffic to other compatible IDSs such as Snort. However, only WEP encrypted network traffic may be forwarded by Kismet because of the inability to decrypt WPA encrypted network traffic in real time. Overall, the Kismet application has extensive flexibility due to the open-source code and the variety of methods available to implement the Kismet application.

Another open source wireless IDS, Snort-wireless is based on the well known Snort application, which incorporates 802.11 specific rules for detecting WLAN intrusions including MAC address spoofing attacks and DoS attacks (Lockhart, 2005). The Snort-wireless project was a great advancement in the detection of 802.11-based attacks due to the close relationship of the detection method used by the Snort IDS. However, the project is now defunct and has not been updated since 2005 (Murray, 2009, p.8). Since the application has not been upgraded or maintained for some time it lacks the adaptations needed to counter new attacks and is not concurrent with specifications outlined in the latest IEEE 802.11 standard and amendments.

2.8 PROBLEMS AND ISSUES

From the literature reviewed there have been a number of issues presented that are specific in the realm of conducting digital forensic investigations in WLANs. The apparent problems and issues discovered will be outlined in order to identify important aspects of the chosen research area where further research is needed.

Wireless networking, by its particular inherent qualities, is a security threat mainly due to the lack of physical borders that are defined on the network. Thus, an unauthorised party is able to monitor a WLAN without physically connecting to it and in many scenarios such an attack may be accomplished at a reasonable distance from the target WLAN. In comparison, in a wired LAN, an unauthorised party would have to physically connect a device to a network port to monitor or access the targeted network. Furthermore, a number of security threats specific to WLANs have been identified (Section 2.3.1), ranging from eavesdropping to denial of service attacks. To further complicate the issue of security both 802.11 legacy and RSN based networks have been shown to suffer from a number of potential security attacks. Moreover, the attacks discussed are realistically feasible and can be implemented using hardware and software that is available to regular consumers. All of these identified points may lead to a WLAN being attacked and exploited. WLAN 802.11-based misuse has been outlined and discussed (Section 2.4) and a number of scenarios substantiate the fact that intentional misuse from an unauthorised party can, and does, arise. Such misuse ranges from providing an anonymous internet connection to attacks against wireless devices or the wireless medium itself. The issues of security and misuse highlight the predicament of problems including insufficient security of a wireless network, potential of wireless attacks and also the misuse of a wireless network. Each problem area reinforces the need to be prepared to execute digital forensic investigations on 802.11 WLANs if, or when, required.

Currently, in terms of conducting digital forensic investigations on WLANs, limited information from reputable procedural guides (Section 2.5.4) is available to forensic investigators. Without such guidelines available there exist issues which restrict the work of digital forensic investigators in being able to conduct a forensic investigation involving wireless networks. There have however, been a number of academic research papers addressing the need for technical information in order to conduct wireless forensic examination including performing digital forensics on wireless networks to obtain viable digital evidence. The literature was reviewed to identify potential sources of evidence obtainable from a WLAN (Section 2.6). Sources of evidence included 802.11 capable devices, network devices and the wireless spectrum used in 802.11 WLANs. Even though such research enhances the ability to conduct digital forensics in WLANs there remain many puzzles and further research is still needed. For example, if evidence was to be extracted from a WLAN via acquisition of 802.11 frames (sniffing) from the wireless spectrum, is the evidence credible given the particular levels of reliability needed of digital evidence in the ramifications of a court of law? The available tools (Section 2.6.3.2) for conducting such acquisitions are not specifically designed for performing digital forensics and have not been tested for reliability and best practice principles when performing such an investigation. Furthermore, collection of network traffic is a type of live evidence which involves specific challenges to acquire and preserve data for later use in digital forensic procedures. In addition, architectures for live evidence collection need to be proposed and tested to ensure that digital forensic principles are achieved to enable acquisition and preservation of potential digital evidence.

Intrusion detection systems (Section 2.6.4) were also identified as a potential source of evidence to aid in WLAN investigations. From the literature reviewed a number of WIDS were considered (Section 2.7.3) and which could be implemented in an existing WLAN. However, in terms of conducting an digital forensic investigation, these systems have not yet been specifically tested or given requirements of operation or system implementation.

The discussed problems and issues demonstrate the need for further research to be undertaken in the field of digital forensics in WLANs in order to establish guidelines to investigation techniques and best practices. Furthermore, research also needs to be conducted regarding the principle domains of digital forensics including acquisition, preservation of integrity, analysis and reporting of potential digital evidence in WLANs.

2.9 CONCLUSION

The literature review conducted in Chapter 2 provides an overview of the current state of knowledge and of the context of the thesis. It first established the IEEE 802.11 standard and amendments of WLAN based communications technology followed by a review of the security features, attacks and misuse. The process of digital forensics and investigation provided fundamental knowledge to then lead on to a review of the potential sources of evidence from WLANs. Methods of acquisition and analysis of digital evidence as well as the operation and use of an Intrusion Detection System in WLANs were examined to establish the potentiality of obtaining digital evidence from a WLAN. The problems and issues apparent in conducting digital forensic investigations in WLANs were identified as a basis to forming research questions.

The literature reviewed and discussed, therefore, introduces specific areas where there is a definite need for further research. In particular, the security issues which have been raised and the apparent misuse of WLANs further support the perceived need to conduct such an investigation. The current state of knowledge also identified crucial factors that will assist in the design perspectives and developments of a feasible research methodology. It has therefore, been determined that the proposed research will focus on advancing the body of knowledge surrounding wireless digital forensic principles in WLANs. Specifically, the research will aim to acquire wireless network traffic as a source of evidence while also incorporating intrusion detection systems to provide further information about possible attacks.

Chapter 3 will therefore firstly undertake a review of similar studies relevant to the chosen area of research and together with the literature knowledge, the main research question and associated sub-questions will be derived. Undoubtedly, there will be limitations to the proposed project but any potential restrictions will be identified early at the pre-testing stage of the project so as to negate or explain any foreseen negative impacts in the results. The formations for the project have been established.

Chapter Three

RESEARCH METHODOLOGY

3.0 INTRODUCTION

In Chapter 3, the main research objectives are to formulate a research question and develop an appropriate methodology establishing a framework for the proposed research. Wireless network traffic is a compelling source of evidence as it provides ample information of the activity in a WLAN and the data communicated between electronic devices. There are a number of issues that surround the topic of acquisition and preservation of wireless network traffic and it would seem that an investigation in this field of capturing evidential trails would be of value.

A number of similar studies in the chosen research field will first be sourced and fully evaluated in Section 3.1 so as to learn from the experience of other researchers working within the same domain of study. In conjunction with the readings from Chapter 2, these additional facts will be pivotal to forming the research question and hypothesis to be tested. Section 3.2 will outline the main research question and secondary questions with associated hypotheses based on all of the gathered information.

Sections 3.3 and 3.4 concentrate on establishing a practicable research model of the proposed system architecture and the associated hardware and software requirements. The data requirements in Section 3.4 will outline the generation, collection, analysis and reporting methodologies needed to conduct the research. Finally, the expected outcomes will be covered in Section 3.5 and in Section 3.6, the limitations of the research will be discussed to identify early restrictions that may apply to the project.

3.1 REVIEW OF SIMILAR STUDIES

In order to develop the methodology for this research, six independent research studies have been sourced and reviewed. There have been a number of references of evidence identified in Chapter 2 to facilitate the process of forensic investigation in a wireless network environment. The following research studies have been selected for relevance and similarity to the chosen research area, methodology used and detailed information regarding forensic investigation of wireless networks.

The first study by Casey (2004) examines network traffic as a source of evidence and discusses the techniques, guidelines and recommendations of using network traffic to assist forensic investigation. The second study by Ngobeni & Venter (2009) outlines the theoretical system architecture for a Wireless Forensic Readiness Model (WFRM) which constantly monitors a WLAN to acquire and preserve wireless network traffic for later examination and analysis. The third study by Sommer (1999) investigates the use of Intrusion Detection Systems (IDS) as a source of potential evidence. Different types of IDS systems are identified and evaluated for their ability to provide admissible evidence with recommendations then given to improve the role of IDS systems in supplying viable digital evidence.

The fourth study by Murray (2009) examines the use of Kismet as a distributed wireless IDS implementing wireless drones on OpenWRT embedded Linux APs which are centrally managed with the Kismet server application. The fifth study by Pradeep Reddy, Sharma and Paulraj (2008) conducted research into the design and application of a multi-channel Wi-Fi sniffer and the performance ability of the device. The final study by Yim et al. (2008) implements a WLAN Forensic Profiling System to detect Denial of Service attacks in a WLAN and log the gathered evidence of the attack.

3.1.1 Network Traffic as a Source of Evidence

Casey (2004) conducted a research study into the use of captured network traffic as a source of digital evidence in the article *Network traffic as a source of evidence: tools strengths, weaknesses, and future needs*. The paper discusses the use of various open source and commercial tools in the context of the overall digital investigation process involving the collection, documentation, preservation, examination and analysis phases of digital forensics (Casey, 2004, p.28). Although this research encompasses all varieties of network traffic, the principles of the study can also be applied to wireless network traffic.

"Network traffic presents a number of challenges as a source of evidence" (Casey, 2004, p.29). This statement is particularly significant as in most cases there is only one chance to capture network traffic and the consequences of inadequate evidence collection systems result in unrecoverable losses of potential evidence. "Additionally, networks comminute data before transmitting them" (Casey, 2004, p.29). It is therefore necessary to piece together packets from network traffic to obtain data in its original form. Combined with the numerous network protocols available this contributes additional complexity to an already complicated source of evidence.

When collecting digital evidence, the selected hardware and software should be well suited to the task to ensure collection of a full data set, documentation of any losses and establishment of the integrity of evidence collected (Casey, 2004, p.37). Therefore, specific hardware and software is needed when capturing network traffic and, in this case, Linux proved to be the desired operating system of choice from informal academic testing.

This is due to better performance, scalability and security which prevents malicious interference and a stable platform to collect, store and preserve digital evidence. Furthermore, “when collecting network traffic, the de facto standard is to store the data in a Tcpdump file with a ‘dmp’ extension” (Casey, 2004, p.39). The dmp extension is the same a cap or pcap extension implemented under the libpcap or winpcap Application Programming Interface (API).

Casey (2004, p.29) defines the examination phase of digital forensics as the process of extracting and preparing data for later analysis. Techniques to assist examination of network traffic include flow reconstruction, protocol decoding, data reduction and keyword searching (Casey, 2004, pp.31-36). Flow reconstruction involves the reconstruction of network packets into a single flow of network packets. The concept of flow reconstruction of network traffic is displayed in Figure 3.1. Protocol decoding entails extracting specific important items from the acquired network traffic. For example, the process of decoding File Transfer Protocol (FTP) commands from FTP packets (Casey, 2004, p.31). Data reduction involves the use of filtering on the acquired network traffic to reduce the amount of data for analysis. For example, performing network traffic filtering to identify web based traffic by using port number 80, or, by using other protocol, destination and source addresses to filter the captured network traffic into a reduced form. Keyword searching utilises search parameters that are run against the acquired network traffic in order to isolate a specific keyword in the packet capture.

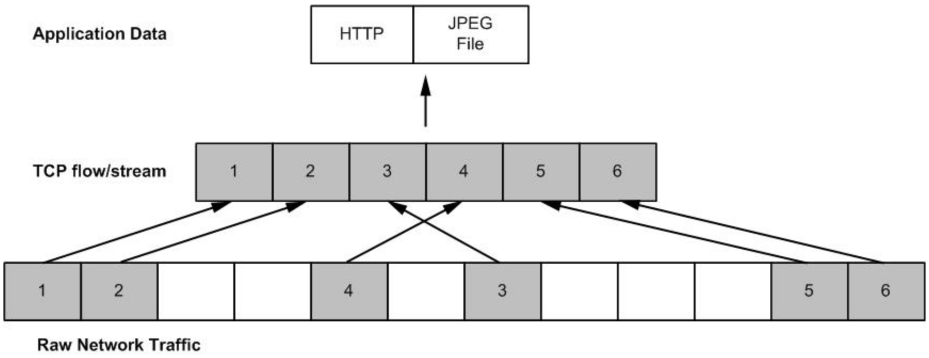

Figure 3.1: Conceptual representation of packets in network traffic relating to single flow being extracted to obtain data carried by networking protocols (Casey, 2004, p.30).

The analysis phase involves assessment, experimentation, correlation and validation of available evidence to gain an understanding and draw a conclusion regarding the incident. Casey (2004, p.41) outlines a number of findings from the conducted research. In terms of available tools, open-source tools such as tcpflow and Etheral (now known as Wireshark) are useful for basic network examination. However, they are not designed specifically for evidence processing whereas, NetInterceptor and NetDetector do have such means providing more powerful examination and analysis capabilities. In conclusion, a number of recommendations have been proposed by the author setting out the basic requirements of the tools needed to process network traffic as evidence. Table 3.1 sets out the recommendations of Casey (2004, p.41).

Table 3.1: Recommendations for Network Traffic Tools (Casey, 2004, p.41).

Recommendations	**Comments**
Tcpdump Format	When acquiring or analysing network traffic, use applications and tools which support Tcpdump file format.
Data Reduction	Implement various methods to locate or reduce amount of data to capture or analyse.
Documentation	Record audit trail of all digital evidence, examiner actions, system performance and packet loss.
Integrity	Calculate MD5 hash value of packet capture evidence file.
Read-only Data	Provide read-only access during collection and examination of evidence.
Complete Collection	Ensure the network traffic capture collected is a full data set and minimise data losses.
Security	Ensure secure remote access and administration of systems and tools.

3.1.2 The Design of a Wireless Forensic Readiness Model

Ngobeni & Venter (2009) describe their Wireless Forensic Readiness Model (WFRM) and compare it to the digital forensic process outlined in previous research. Forensic readiness is defined as decreasing the effort and time to perform a digital forensic investigation while continuing to maintain the accepted level of digital evidence. “The principal concept addressed by the WFRM is that it monitors wireless network traffic from various Access Points (APs). The monitored traffic is logged in a log file, and then preserved to maintain its integrity” (Ngobeni & Venter, 2009, p.7). The proposed WFRM therefore, consists of the monitoring and then logging of wireless network traffic, preservation of the logged network traffic, followed by the analysis of the acquired network. The reporting of the information or data obtained from the forensic process conducted on the wireless network can then be made. The process used is similar to the digital forensic process (Section 2.5.1) previously discussed. However, the authors also base the forensic process implemented in the WFRM on popular forensic tools such as

EnCase and Forensic Toolkit in an attempt to acquire and preserve digital evidence in a sound manner.

Figure 3.2 displays the proposed WFRM by Ngobeni & Venter (2009, p.7), in the form of a block diagram illustration, outlining the proposed life cycle of the wireless forensic methodology.

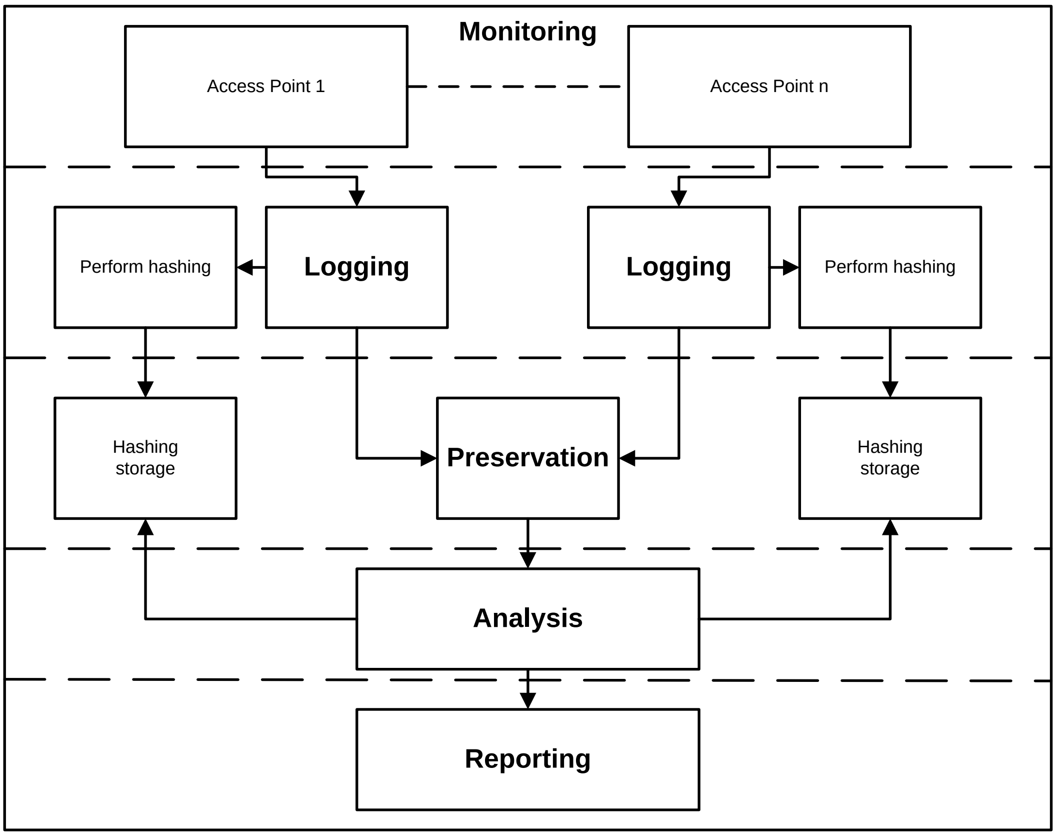

Figure 3.2: WFRM Block Diagram (Ngobeni & Venter, 2009, p.7).

The monitoring in the WFRM is to be conducted on each of the APs in the WLAN. Thus, the AP must be able to acquire wireless network traffic. However, the authors do not suggest how this traffic should be collected, but it can be assumed that the monitored network traffic would be collected in packet capture format. A Capture Unit is proposed to log all the monitored network traffic into split files of 1 megabyte (Ngobeni & Venter, 2009, p.8). The traffic log file is then combined into a block comprised of multiple logs and transferred to a permanent storage space described as the Evidence Server (ES). The transportation of the log files is necessary because APs have very limited storage areas that cannot contain large amounts of data. The ES acts as the central storage area for the data collected from the APs in block form and proceeds to preserve the data by assigning an Message Digest algorithm 5 (MD5) hash of the data. Hashing the data preserves the integrity of the captured network traffic and ensures the data stored on the ES has not been altered. From here, a digital investigator is able to conduct the analysis and will then be in a position to report on the acquired network traffic.

The proposed WFRM has a number of advantages and disadvantages in its implementation. The evidence collected is forensically ready and forensically sound, therefore reducing the time involved for the investigators to identify, acquire and preserve digital evidence (Ngobeni & Venter, 2009, p.14). Disadvantages include the amount of data that needs to be stored and the associated costs to implement this storage facility as well as the legal technicalities involved in capturing network traffic data. Furthermore, the authors identify that future research in the area of evidence admissibility requirements also needs to be addressed in the process of conducting wireless forensic investigations.

3.1.3 Intrusion Detection System as Source of Evidence

Sommer (1999) conducted research to address the problem: "What is required to turn the output of an IDS into legally reliable evidence?" (Sommer, 1999, p.2477). Currently IDSs are not suited for evidence handling. For example, IDSs are not designed or implemented to correctly collect or store potential evidence, nor maintain the integrity of the potential evidence collected.

Sommer (1999, p.2479) groups the types of IDSs into a conventional taxonomy divided into either post-event audit trailing or real-time monitoring. Post-event auditing involves the analysis of logs and audit trails, while real-time monitoring constantly monitors network traffic, or on host or network devices. From an evidential point of view data, or information that is preserved after the event has occurred, is needed for forensic investigation. In terms of IDSs such evidence tends to include various types of logs including system, audit, application, network management logs, as well as network traffic capture which is classed as *primary data* (Sommer, 1999, p.2479). Primary data is then processed into a form that is easier to analyse and understand and is then known as *derived data*.

From his research Sommer (1999, p.2486-2487) offered a number of conclusions in regard to redesigning IDSs as sources of evidence. The value of an IDS as a source of evidence depends on the extent of the timeliness and accuracy of the information obtained (Sommer, 1999, p.2486). Since the main goal of an IDS is to prompt or identify computer intrusion attacks, additions may need to be made to the tool to aid in forensic evidence acquisition. Furthermore, even though digital investigation may identify the perpetrator or an incident, the evidence extracted may still not be admissible in court (Sommer, 1999, p.2486). For example, if IDS logs identify a suspect based on a device address (such as IP or MAC address), the evidence may not be admissible due to the fact that IDS systems are not specifically designed to collect and preserve evidence, thus creating issues with obtained evidence and its use in a court of law.

To complicate the situation, “single streams of evidence are unlikely to be adequate to convince a court” (Sommer, 1999, p.2486). Therefore the evidence gathered from an IDS will provide more weight if collaborated by a separate, but related steam of evidence. For example, if IDS logs identify and log a network perimeter breach, a secondary stream of evidence may be firewall logs or server audit logs where collaboration can be achieved through timestamps and Internet Protocol (IP) or Media Access Control (MAC) device addresses. Sommer (1999, p.2786) also states that if evidence is used from an IDS, such as logs, the prosecutor must be prepared to disclose complete details of the tool used and how it was configured and operated. In the case of networking monitoring tools, disclosure of local network topography may be needed. Another recommendation is that logged evidence should be handled according to digital evidence guidelines. Evidence needs to maintain its integrity and “the raw log should always be available” (Sommer, 1999, p.2487). “Where an exhibit is built from derived data (as in a chart or spreadsheet) the raw data has to be available for disclosure” (Sommer, 1999, p.2487). This involves storing potential evidence that has been gathered and ensuring preservation and integrity of the data gathered. Finally, there needs to be a complete chain of custody of evidence from source to court (Sommer, 1999, p.2487).

3.1.4 An Inexpensive Wireless IDS using Kismet and OpenWRT

Murray (2009) proposed the use of an open source distributed wireless IDS platform as an alternative for medium to small enterprises employing commercial products such as AirMagnet and AirDefense. This is a much needed solution due to the high cost of similar proprietary systems, including the investment in equipment and associated staff training. Murray (2009, p.9-10) outlined the use of the Kismet application combined with the open source wireless router firmware OpenWRT. A distributed wireless IDS architecture was thus created using a Kismet server, as a centralised management system, and Kismet drones as the distributed wireless IDS sensors. The Kismet drones are installed and configured on the APs that are running OpenWRT which forwards the traffic collected to the central Kismet server for collection and later analysis. Figure 3.3 displays the system architecture of the proposed distributed Wireless IDS (WIDS) system.

Murray (2009) produced a highly technical and practical paper of his research outlining the various methods to configure an appropriate wireless AP with the OpenWRT firmware and Kismet drone application. In the article the Linksys WRT54G Version 1.1 is used as the configured AP. The WRT54G is an inexpensive, open-source based wireless AP that communicates using 802.11b and g (Murray, 2009, p.7). However, the WRT54G is limited to 802.11b and g and is not capable of communication using the newest 802.11n standard amendment. Furthermore, both the OpenWRT firmware Operating System (OS) and Kismet application are constantly being updated, thus changes to the capabilities of the software and configuration are also needed in order to implement a WIDS system based on Kismet and OpenWRT.

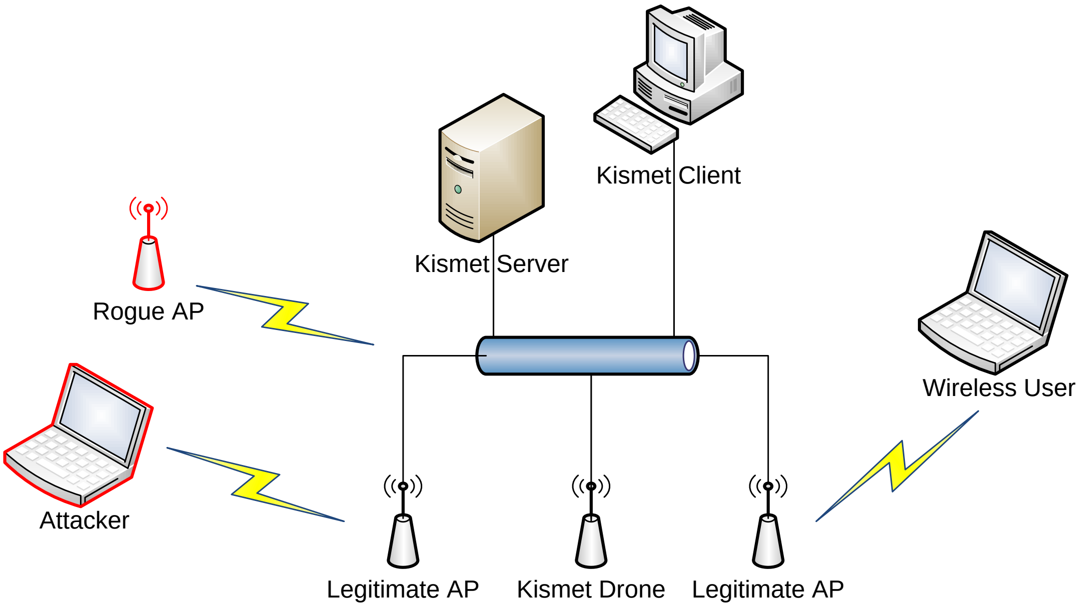

Figure 3.3: OpenWRT and Kismet Centralised Distributed WIDS Architecture (Murray, 2009, p.9).

3.1.5 Multi Channel Wi-Fi Sniffer

Reddy, Sharma and Paulraj (2008) conducted research regarding sniffing multiple channels in the 2.4GHz and 5GHz wireless spectrum simultaneously implemented in the Multi Channel Sniffer (MCS). The aim of the research was to provide intelligent support and detection of threats in open wireless networks. Such capabilities are achieved because the device is able to sniff all wireless channels simultaneously so there is no chance of missing packets while performing channel hopping.

Reddy, Sharma and Paulraj (2008, p.1) outline a system architecture consisting of a host system and target system. The host system is a personal computer running Linux with an Ethernet interface and a sniffer application. The target system, on the other hand, is a single device comprised of multiple Single Board Computers (SBC), each containing 4 Atheros mini Peripheral Component Interconnect (PCI) wireless adapters with external antennas (Reddy, Sharma and Paulraj, 2008, p.2). The host and target system are connected via a 100Mbps Ethernet connection. The main software specifications for the MCS SBC sniffer includes the SnapGear embedded Linux OS, WLAN driver and wireless sniffer application.

To test the capabilities of the MCS, Reddy, Sharma and Paulraj (2008, p.4) conducted a number of experiments to assess the packet capture abilities of the implemented system. Experiments were conducted multiple times under the same conditions in a Radio Frequency (RF) shielded environment. Three traffic generators were used to flood the wireless network with traffic allowing the MCS to sniff the generated packets to assess the wireless network packet capture capabilities of the implemented system (Reddy, Sharma and Paulraj, 2008, p.4). The rates of the tested generated packets were approximately 2200 and 3700 packets/sec (PPS) in a secured network. 6000 packets/sec were tested in an open network.

Table 3.2: Performance Results of MCS: Base Implementation (Reddy, Sharma and Paulraj, 2008, p.4).

	~2200PPS	**~3700PPS**	**~6000PPS**
1 Card/SBC	100%	100%	98%
2 Card/SBC	100%	92%	80%
3 Card/SBC	100%	78%	44%
4 Card/SBC	100%	54%	28%

Table 3.3: Performance Results of MCS: Optimised Implementation (Reddy, Sharma and Paulraj, 2008, p.5).

	~2200PPS	**~3700PPS**	**~6000PPS**
1 Card/SBC	100%	100%	100%
2 Card/SBC	100%	100%	99%
3 Card/SBC	100%	99%	99%
4 Card/SBC	100%	98%	95%

Table 3.2 displays the base implementation results from the experimental testing of the MCS architecture which was able to capture a full data set (100% of all generated traffic) at the rate of 2200PPS using up to four active wireless adapters. However, as the packet generation rate increases the loss of packets also greatly increases. With four wireless adapters running and a rate of 6000PPS the MCS was only able to acquire 28% of all generated traffic. Due to the low percentage of packet capture results achieved with the base implementation, optimised implementation was performed in an attempt to increase the packet capture rates of the MCS. Table 3.3 displays the optimised implementation results from the experimental testing. Included in the optimisations were: the use of User Datagram Protocol (UDP) instead of Transmission Control Protocol (TCP) from sending packets from target to host, aggregation of packets being sent from target to host and the use of an intermediate character driver to handle packets captured by the wireless adapter

(Reddy, Sharma and Paulraj, 2008, p.5). All of the optimisations help in providing a more efficient system design to gather packets and forward them to the host system. The results obtained using the optimised implementation, at a rate of 6000PPS and all four wireless adapters running, the MCS was able to capture 95% of all packets generated, a greatly improved increase from 28% when using the base implementation.

3.1.6 The Evidence Collection of DoS Attack in WLAN

The research of Yim et al. (2008) propose the use of a WLAN Forensic Profiling System comprised of a forensic client and a forensic server using IDS methodologies to detect Denial of Service (DoS) attacks in a WLAN. The forensic server acts as a central management system to the Forensic Profiling System and contains database profiles of known attacks, an analysis engine to determine attacks being conducted, and a database of collected evidence that has been identified. Figure 3.4 displays the Forensic Profiling System architecture.

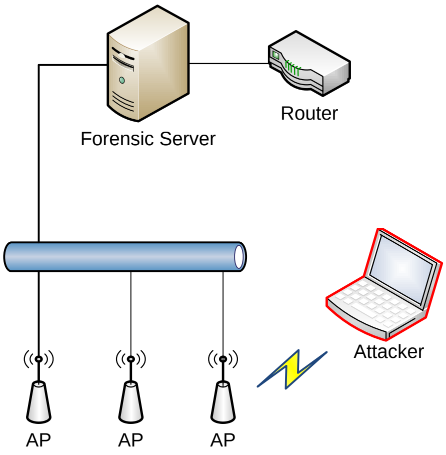

Figure 3.4: Forensic Profiling System Architecture (Yim et al., 2008, p.199).

The forensic server contains a collected evidence database, an analysis engine and a forensic profile database. The collected evidence database preserves collected evidence and saves log files regarding confirmed DoS attacks (Yim et al., 2008, p.200). The collected evidence ties an attacker by the MAC address of the wireless Network Interface Card (NIC) used in the DoS attack. The analysis engine determines whether a DoS attack is occurring by monitoring network traffic and identifying specific forged packets. The forensic profile database contains WLAN DoS attack descriptors which the analysis engine matches against network traffic being monitored. There are a total of 5 alerts including deauthentication, disassociation, authentication, association and duration DoS attacks. Yim et al. (2008, p.200) outline 4 types of DoS attack descriptors that use the 802.11 management frame to implement the DoS attacks, in the form of deauthentication, disassociation, authentication and association attacks. Table 3.4 (Casey, 2004) identifies the type of 802.11 management frames that may be used to conduct a DoS attack against the WLAN. Yim et al. (2008, p.202) also outline a DoS duration attack which is conducted by manipulating the duration field of 802.11 control frames.

Table 3.4: Denial of Service Attacks using Management Frame Field (Casey, 2004, p.41).

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

Evidence is collected from the evidence database which contains alert messages and the associated collected evidence from the attacks. The collected evidence is in the form of network traffic acquired using libpcap as the source of original data. 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 recreate the DoS attacks against the WLAN the following 2 applications were used: void11 and aireplay-ng (Yim et al., 2008, p.203). The AP used to acquire the packet capture evidence is a Cisco-Linksys WRT54G v7. Table 3.5 displays the efficiency of the WLAN Forensic Profiling System during the first minute of the WLAN DoS attack. According to Yim et al. (2008, p.203) the average collecting rate during testing was 65.9%. Therefore, the WLAN Forensic Profiling System proved to be able to capture 65.9% of all DoS packets being flooded on the WLAN. However, it also means that 34.1% of the attackers injected packets were not collected during testing.

Table 3.5: Efficiency of WLAN Forensic Profiling System (Yim at al., 2008, p.204).

Time (seconds)	10	20	30	40	50
WLAN Forensic Profiling System	987	789	891	668	879
DoS Attack Packets	1119	1192	1200	1122	1115
Collecting Rate	0.882	0.661	0.724	0.595	0.788

3.2 THE RESEARCH QUESTION AND HYPOTHESIS

The literature review (Chapter 2) has provided a firm foundation of written knowledge regarding the chosen research area of aiding evidence acquisition and preservation in the realm of conducting digital forensic investigation in 802.11 WLANs. A vast diversity of literature has been covered ranging from IEEE 802.11 based WLAN technology including standardization, security features, attacks and misuse. The process of digital forensics was then examined and specific literature reviewed regarding digital forensic processes in WLANs. Additionally, the preceding review of similar research studies (Section 3.1) has given a varying background into the use of network traffic and IDSs as a source of evidence in a digital forensic investigation. Specifically, the studies also provided an insight of the implementation of such technologies in wireless networks. All of these similar studies have provided further information into the realm of conducting digital forensic investigations in WLANs.

The development of a research question was constructed based on the literature reviewed in Chapter 2, and the review of similar research studies in Section 3.2 has discovered that the use of wireless network traffic is a potential source of evidence that may be acquired from a WLAN. Furthermore, it has also been discovered that wireless network traffic is a compelling source of evidence as it provides ample information of the activity in a WLAN such as active APs and Stations (STA) and data being communicated between such devices. However, there are still a number of issues that surround the topic of acquisition and preservation of wireless network traffic as a source of digital evidence. Such issues include the method of collection of evidence and the requirements to ensure that potential evidence is acquired and preserved according to previously outlined digital forensic principles.

Table 3.6 displays the main research question and the associated hypothesis which has been developed from the information discussed thus far.

Table 3.6: Main Research Question and Associated Hypothesis.

Main Question: *What are the capabilities of a design system to acquire and preserve wireless network traffic as viable evidential trails from 802.11 WLANs?*

Asserted Main Hypothesis:

That a system designed to acquire and preserve wireless network traffic is capable of providing viable evidential trails together with ample information to support digital forensic investigations in which WLANs are involved.

Furthermore, a number of related secondary questions have also been developed. The secondary questions have been devised in order to set out and answer various linked components of the main research question and are set out in Table 3.7.

Table 3.7: Secondary Research Questions.

Secondary Question 1: *What are the hardware and software requirements for the successful acquisition of wireless network traffic as digital evidence for forensic purposes?*
Secondary Question 2: *What are the capabilities of the proposed system design to acquire and preserve a full data set of wireless network traffic?*
Secondary Question 3: *What are the capabilities of the system design to provide digital evidence from WLAN attacks?*
Secondary Question 4: *What is the effect of monitoring multiple 802.11 WLAN channels simultaneously in terms of digital evidence acquired?*
Secondary Question 5: *What are the methodologies, techniques and tools used to conduct digital forensic examination and analysis of the acquired data from wireless network traffic?*

Hypotheses have also been developed for each of the secondary questions which have been proposed. Because of the difficulty in composing a succinct hypothesis for each secondary question, a brief synopsis has been given to articulate the reasoning behind each of the informed hypotheses. Table 3.8 displays the hypotheses for each of the secondary research questions presented in Table 3.7.

Table 3.8: Secondary Research Questions Associated Hypotheses.

Hypothesis 1: That the hardware configurations used will have the capability to collect and process network traffic, including fast Central Processor (CPU) power, high Random Access Memory (RAM) availability and fast Local Area Network (LAN) links between the system components. The software requirements will effectively acquire and preserve wireless network traffic using a wireless sniffer based application.
Hypothesis 2: That the proposed system will not be capable of acquiring a full data set of WLAN traffic due to the proposed method of monitoring a WLAN with an external device. Nevertheless, enough data can still be acquired to determine and reconstruct certain events, such as an attack against the WLAN. Furthermore, the preservation and integrity of the acquired evidence will be able to be maintained.
Hypothesis 3: That digital evidence from recreated WLAN attacks is possible by acquiring and preserving wireless network traffic between devices of the WLAN. The IDS system will also provide additional digital evidence of the attacks conducted. In addition, the collected evidence will provide details of the type of attack conducted and digital evidence to aid in digital forensic investigation.
Hypothesis 4: That multiple 802.11 WLAN channels can be monitored to provide additional evidence for events occurring on different channels. However, the performance and acquisition capability of the system may decrease.
Hypothesis 5: That examination and analysis of the acquired wireless network traffic can follow similar methodologies and techniques to that of wired network traffic. Also, that previously used tools and methods for wired network traffic can also be utilised.

In order to attempt to answer the proposed research questions, validate the asserted hypotheses and conduct research testing in an organised manner a data map was developed. Figure 3.5 presents the research data map outlining the main research question, secondary research questions and the links to the associated research testing phases. Furthermore, each testing phase is also linked to the associated point of data collection achieved from testing. Finally, the findings gathered from the research testing phases and related data collected will be used to aid in determining the asserted hypotheses.

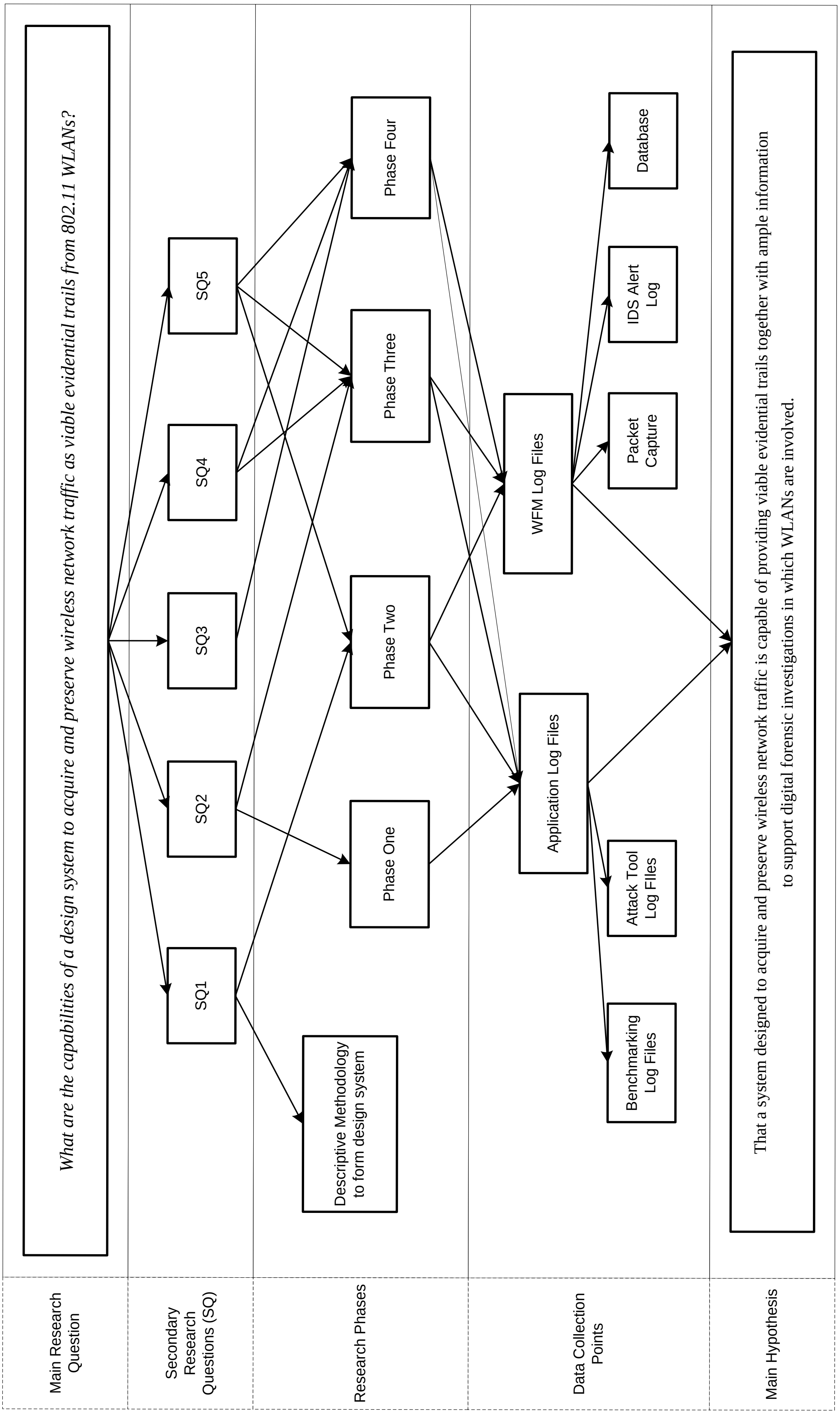
Main Research Question
Secondary Research Questions (SQ)
Research Phases
Data Collection Points
Main Hypothesis
What are the capabilities of a design system to acquire and preserve wireless network traffic as viable evidential trails from 802.11 WLANs?
SQ1
SQ2
SQ3
SQ4
SQ5
Descriptive Methodology to form design system
Phase One
Phase Two
Phase Three
Phase Four
Application Log Files
WFM Log Files
Benchmarking Log Files
Attack Tool Log FIles
Packet Capture
IDS Alert Log
Database
That a system designed to acquire and preserve wireless network traffic is capable of providing viable evidential trails together with ample information to support digital forensic investigations in which WLANs are involved.

Figure 3.5: Research Data Map.

3.3 THE RESEARCH MODEL

The aim of this research is to advise on robust architectures and system designs for the acquisition and preservation of digital evidence from 802.11 WLANs. The particular digital evidence of importance to this research is in the form of wireless network traffic or 802.11 frames. A theoretical research model is proposed using a design science approach in order to establish a framework for the research to be conducted. Descriptive methodology will be used to conduct fact-finding enquiries to establish the state of affairs in the proposed research area (Kothari, 2004, p.3). From this the system architecture and the components needed to construct the system design will be derived.

A design science approach will be adopted to form the system design. Simon (1981) describes design science as a statement of "how things ought to be" and a "theory for design and action" (pp.132-133). Design theory gives explicit prescriptions (guidelines or principles) for constructing an artefact (Gregor, 2002, p.14). Design science lies in acquired knowledge that can be used to design artefacts (in this case, digital evidence acquisition and preservation in WLANs) and a prescription for a generic class of problem (van Aken, 2004). The intention of the research is to implement a Wireless Forensic Model (WFM) system architecture to acquire and preserve wireless network traffic. The goal is to attempt to obtain and store potential digital evidence that will aid digital forensic investigation in WLANs by providing viable digital evidence. It is proposed that the WFM be implemented and reviewed to determine the capabilities of the model and its ability to provide digital evidence of an acceptable standard from wireless network traffic. The implemented WFM will passively monitor a WLAN acquiring the wireless network traffic between devices. The proposed theoretical research model described is illustrated in Figure 3.6.

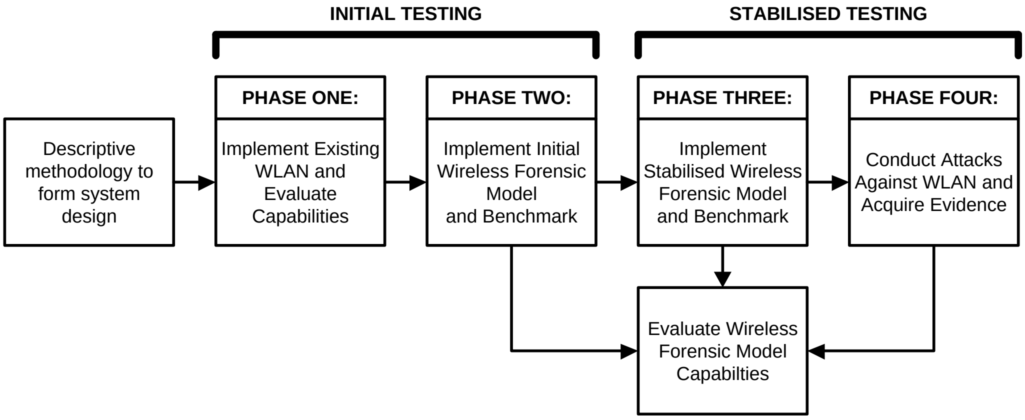
INITIAL TESTING
STABILISED TESTING
Descriptive methodology to form system design
PHASE ONE:
Implement Existing WLAN and Evaluate Capabilities
PHASE TWO:
Implement Initial Wireless Forensic Model and Benchmark
PHASE THREE:
Implement Stabilised Wireless Forensic Model and Benchmark
PHASE FOUR:
Conduct Attacks Against WLAN and Acquire Evidence
Evaluate Wireless Forensic Model Capabilties

Figure 3.6: Theoretical Research Model.

Descriptive methodology entails outlining the system design relating to the architecture and components needed to later be implemented into a practical system. The software and hardware components and associated configurations will also be described and discussed in order to present a proposal for the intended system.

Initial testing will be conducted on the proposed system which may necessitate the system to be modified several times in response to learning. Outcomes from initial testing will also dictate which components in the WFM need to be modified in order to achieve a stable and reliable system architecture. Possible components that are likely to be changed during initial testing include both software and hardware solutions.

Initial testing will involve two phases. Phase One of testing is to implement the WLAN and perform benchmark testing to determine the capabilities of the existing infrastructure. Such information includes the bandwidth and maximum packet per second (PPS) capabilities of the network. The testing of the existing WLAN capabilities is important as it provides a baseline of the maximum amount of network traffic that the testbed WLAN is capable of transmitting providing a maximum measurement of data available for acquisition by the proposed WFM. Therefore, with information such as maximum PPS transfer rate, the WFM can be tested using the obtained rates and later evaluated for the ability to acquire a full data set. Although other researchers have performed similar methodologies of benchmark testing under the different IEEE 802.11 standards, it is critical to ensure that the test network is functioning correctly. Furthermore, with the existing WLAN capabilities having been determined, the findings of wireless network traffic acquisition by the WFM are assured to be accurate.

Phase Two of initial testing involves the implementation and benchmarking of the proposed WFM. The implementation will entail establishing a hardware and software solution to acquire wireless network traffic and preserve the collected evidence in a centralised server. Subsequent to the initial implementation benchmarking of the initial WFM will involve testing different PPS rates using the same methodologies from Phase One.

After the proposed system design is stabilised, further testing will be conducted to review the ability of the system to acquire and preserve wireless network traffic. The ultimate goal is obtaining evidentiary trails to reconstruct WLAN events, such as attacks conducted against the WLAN. Therefore, the testing at the end of the initial stage is not the limit of the research. The tests are to inform different solutions to any identified problem areas encountered so far.

Stabilised testing also involves two phases. Phase Three draws on the information gained during initial testing to form a stabilised WFM design. At this stage the system design is likely to have been altered as a response to any discovered issues during initial testing. Stabilised testing will involve using the same testing methodologies used in initial testing, where benchmarking is conducted to determine the capabilities of the developed WFM. The results from stabilised benchmark testing will then be analysed and assessed in order to verify the capabilities of the final system design, as well as the ability to acquire and preserve wireless network traffic to be used as a source of digital evidence.

Phase Four of testing will involve recreating specific attacks against the WLAN infrastructure and the capabilities of the stabilised WFM system design to obtain evidentiary trails of the attacks from acquired wireless network traffic. It is proposed that multiple different attacks will be conducted to present a variety of scenarios where evidence collection may help determine the source of the attack or provide details of the type of attack and targeted devices. The effect of each attack is to be recorded in terms of evidential trails, the potential for comprehensive data collection and compliance with forensic principles.

3.3.1 Proposed System Architecture

The proposed system architecture will closely follow previous theoretical and practical solutions discussed in the selected similar studies (Section 3.2). The solution to acquire wireless traffic as a source of evidence in a WLAN requires the placement of wireless drones, or sensors, which monitor the WLAN and collect wireless traffic (802.11 frames) that is transmitted between APs and STAs in the WLAN.

The WFM is designed to allow implementation of the system into an existing WLAN, as the system contains external components which are additional components to the already existing WLAN infrastructure. The components of the WFM include wireless drone(s) and a Forensic Server. A wireless drone is to be distributed into the existing WLAN system architecture, one for each separate AP, to monitor the wireless traffic on the network. The wireless drones then forward collected wireless traffic to the centralised Forensic Server to perform data preservation. Replicating the research design of the Multi-Channel Sniffer (Pradeep Reddy, Sharma and Paulraj, 2008) the wireless drone to be implemented in the WFM will also contain multiple wireless adaptors. The design will allow the wireless drone to monitor the channel of the existing WLAN, while also monitoring other multiple channels simultaneously. It is not a goal of the research to monitor all 802.11 channels, rather it is to monitor the channel in which the existing WLAN resides and to hop between the other channels available. The purpose of the design is to aid in the detection of WLAN attacks which occur on channels what the existing WLAN is not using. For example, Fake Access Point (FakeAP) attacks can occur on any channel defined under the 802.11 standard.

Figure 3.7 displays the proposed system design of the WFM introduced into the existing WLAN infrastructure. The legitimate AP and wireless user are authorised members of the existing WLAN infrastructure, while the attacker and rogue AP are unauthorised parties attempting to attack the WLAN.

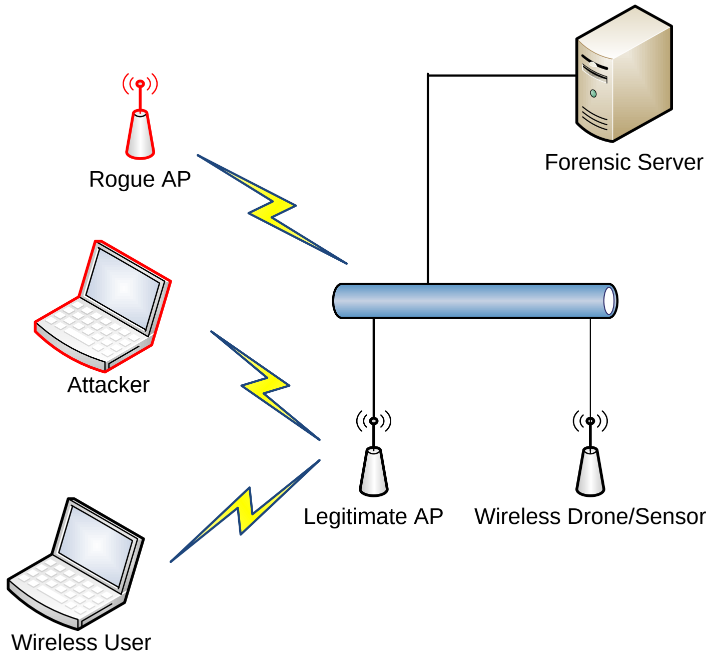

Figure 3.7: Proposed 802.11 WLAN Wireless Forensic Model Architecture Design.

The proposed system architecture will be implemented into a testing environment consisting of three main entities. The first component of the testing environment is the WFM, comprised of a Forensic Server and Wireless Drone. The second component of the testing environment is the existing WLAN network infrastructure which is comprised of APs and STAs which actively communicate together. Therefore, the existing network is comprised of a stationary legitimate AP and mobile client STAs, such as a laptop. The third component of the testing environment is the attacker’s computer and associated WLAN attack tools. The software and hardware specifications and configurations to be used in the proposed research model will now be outlined and discussed in the following sub-sections.

3.3.2 System Components

The research testing will involve the implementation of three main components: the WFM, the existing WLAN network and the Attacker components. Each component is different regarding design, configuration and intended task, therefore, each component to be implemented will be outlined and described separately.

3.3.2.1 Wireless forensic model configuration

The proposed software and hardware configuration to be used for the WFM has been developed from the literature review (Chapter 2) in combination with the similar studies reviewed (Section 3.1). The choice of software configuration has been carried out prior to the hardware configurations in order to match the desired software to compatible hardware.

SOFTWARE CONFIGURATION: Currently there is no application specifically designed to perform wireless packet sniffing to aid in conducting evidence acquisition in a WLAN. Therefore, the choice of wireless packet sniffing software has been based on the previously discussed literature regarding wireless network packet capture tools (Section 2.6.3.2). Of the available tools, the Kismet application has been chosen as the desired software application for the foundation of the WFM software configuration for a number of reasons. The application is an open source wireless sniffer which provides high availability of the software and also reduces potential issues with proprietary licences and cost. Moreover, Kismet has the built-in ability to provide a centralised distributed wireless IDS and wireless network monitoring system. Kismet was first released in late 2001 and given a total rewrite of the core Kismet code in 2009 (Kershaw, 2009, pp. 5, 13). The new design of the Kismet application rectified a number of usability and configuration issues as well as better remote capture, error handling, IDS capabilities and the ability to use application plug-ins. Furthermore, Kershaw (2009, p.13) states that the old code “grew” from initial development, while the new code is specifically designed for the intended purpose of the application. Therefore, it is proposed that a ‘newcore’ version of Kismet will be used.

In order to create a distributed WFM it is proposed that the Kismet drone application will be run on independent wireless routers with wireless chipsets that support Radio Frequency Monitor (RFMON) mode, thus creating a wireless drone. It is proposed that the wireless router’s firmware will be upgraded from the default Original Equipment Manufacturer (OEM) firmware to OpenWRT embedded Linux distribution. OpenWRT (2010) is the preferred embedded Linux OS with a fully writable filesystem and package management capabilities to enable full customisation. Furthermore, OpenWRT is open source allowing high availability, has a large development and user community and a number of compatible wireless devices.

In terms of the Forensic Server, the software configuration chosen includes Ubuntu Linux as the OS and the Kismet Server application to collect and preserve wireless network traffic from the wireless drones. Ubuntu is an open source Linux distribution with the required software packages available to run the Kismet Server application and collect network traffic.

HARDWARE CONFIGURATION: Since the application of choice is Kismet, the hardware device chosen for the wireless drone must have the ability to run the Kismet (drone mode) application. Therefore, the wireless drone hardware must have an Ethernet port to transport packets back to the Forensic Server and a compatible wireless chipset to allow monitor mode. Additionally, the device must have enough RAM and CPU power to allow the capture of 802.11 frames at a high packet per second rate. A popular method for producing a wireless drone was identified in previous similar studies (Section 3.1.4) which involves using a wireless router as a wireless drone. OpenWRT was chosen as the software to run the wireless drone, so therefore, the device chosen must be able to run the OpenWRT embedded OS. However, it is difficult to source an available wireless router with suitable capabilities such as a high powered CPU and RAM as well as Gibabyte Ethernet. For these reasons the selected device for the wireless drone has been based on the Multi-Channel Sniffer (Pradeep Reddy, Sharma and Paulraj, 2008) and the use of a SBC and mini-PCI wireless adapters with external antennas.

The Forensic Server is also required to run the Kismet application (server and client mode) to collect wireless traffic forwarded by the wireless drone, and be able to preserve the data gathered in accordance with digital forensic principles. It has been proposed that the server will run the Ubuntu OS, and the hardware configuration requirements are a Personal Computer (PC) with adequate hardware to process network traffic. Furthermore, it is proposed that the Forensic Server will also contain a Gigabyte Ethernet adapter to collect data being forwarded from the wireless drone.

3.3.2.2 Existing WLAN configuration

As previously stated, in order to perform testing of the proposed WFM an existing WLAN infrastructure needs to be implemented that can be constantly monitored by the WFM. The selected IEEE 802.11 standard chosen for the research testing phase will be an 802.11g based WLAN. As stated earlier, the existing WLAN infrastructure will be comprised of a single AP and single client STA. It is proposed to use a consumer based wireless AP, while the client STA will be a laptop computer with a wireless network adapter.

A further element of the existing WLAN infrastructure is the IEEE 802.11 built-in security features that are to be implemented. It is proposed that the single method of security to be used in the existing WLAN is the Wi-Fi Protected Access version 2 Pre Shared Key (WPA-PSK2) network encryption protocol as it offers a higher level of security for IEEE 802.11 based WLANs.

3.3.2.3 Attacker’s configuration

The final component of the proposed system design is the attacker. The attacker conducts specific attacks against the WLAN which will generate data to be collected by the WFM. It is proposed that the attacker will run the Backtrack Linux OS installed on a laptop computer with a wireless network adaptor to conduct DoS and FakeAP attacks against the existing WLAN. Backtrack is the desired OS as it provides a number of built-in penetration testing tools for conducting security audits of WLANs, as well as wireless drivers that are patched for 802.11 frame injection.

3.4 DATA REQUIREMENTS

During the proposed testing phases there are a number of requirements for different aspects of data handling. It has been established that a WLAN will be implemented in a laboratory testing environment consisting of an AP and a single STA. The proposed WFM system design will then be added to the testing environment and attempt to acquire and preserve wireless network traffic as a source of digital evidence. To evaluate the ability and performance of the WFM various tests will be conducted where data is actively generated between devices in the existing WLAN which is subsequently collected by the WFM. The data that is collected will then be analysed and the results reported in Chapter 4.

The data requirements that need to be addressed in the research testing phases fall into three main categories: data generation, data collection and data reporting and analysis. Each of the three data requirement categories will be discussed to ensure viable data is generated, collected, reported and analysed correctly.

3.4.1 Data Generation

The process of data generation is an important aspect in the proposed research testing. In order to evaluate the proposed system design, data must be generated using correct methods so as to provide accurate results. All four phases of research testing require data generation to create network traffic on the existing WLAN, either between the AP and client STA, or by the unauthorised attacker.

Phase One entails benchmarking the existing WLAN, that is, measuring the capabilities of wireless communication between devices. It is proposed that the implemented WLAN architecture will be benchmarked using two tools: iPerf and Multi-Generater (MGEN) application. iPerf is a popular application used to measure bandwidth TCP and UDP bandwidth performance, which will be used to generate data between the AP and client STA and discover the throughput capabilities of the existing WLAN. MGEN is an open source software application produced and maintained by the United

States Naval Research Laboratory, designed to perform IP network performance testing using either TCP or UDP network traffic protocols (Naval Research Laboratory, 2010). MGEN is the desired application because it allows full user control over network traffic generation and logging functionality between the nodes on the WLAN. The main purpose of the MGEN benchmark testing is to establish the maximum PPS capabilities of the existing WLAN. The main reason for not using iPerf for packet per second testing is that MGEN provides additional functionality, such as extensive logging to ensure correct data generation is achieved.

During Phases Two and Three it is proposed that the MGEN application will be used again to test the performance and ability of the implemented WFM by flooding the existing WLAN with network traffic. The results from Phase One will be used to establish the correct PPS rates that the existing WLAN is capable of maintaining, therefore providing a baseline performance evaluation. The baseline results will then be used as inputs to benchmark testing of the WFM. For example, if the existing WLAN is capable of, say, 3700PPS, benchmarking of the WFM will involve generation of network traffic at 3700PPS. The MGEN application will be used to generate data, at the defined baseline performance, between AP and STA on the existing WLAN which will be collected by the WFM.

Aside from benchmark testing, Phase Three will also involve other specific tests to determine certain performance aspects of the stabilised WFM implementation. The iPerf tool will again be used to generate network traffic in order to perform bandwidth measurement between the Forensic Server and wireless drone components.

Phase Four involves recreation of attacks against the existing WLAN to assess the ability of the WFM to collect evidentiary trails. As previously discussed, the attacker’s configuration (Section 3.3.2.3) involves the use of attack tools that are built into the Backtrack 4 OS. The aircrack-ng suite (aireplay-ng and airbase-ng) and mdk3 tools are proposed to recreate two DoS, and two FakeAP attacks. Data generation will be initiated on the attacker’s computer, forging 802.11 frames which are subsequently injected to the existing WLAN. Table 3.9 displays the tool used and the associated attack.

Table 3.9: WLAN Attack Tools.

Tool	Associated Attack Mode
Aireplay-ng	Deauthentication Attack – deauthentication frame flood DoS attack.
Mdk3	Authentication Attack – authentication frame flood DoS attack
Mdk3	Beacon Flood Mode – forges fake beacon frames to show fake APs
Airbase-ng	FakeAP attack tool

3.4.2 Data Collection

The process and methods of data collection is an exceptionally crucial part of the data requirements. The data that is generated by the previously described methods (see Section 3.4.1) is subsequently collected in various log files. The main collection point of data is provided by the WFM, which acquires and preserves the wireless network traffic communicated between devices on the WLAN. However, other areas of data collection are needed, including MGEN application log files and application standard output from the bandwidth and attack tools.

During Phase One of testing, the points of data collection include the application output of the iPerf tool, which reports the bandwidth results, including the total size of data sent over the wireless network link and time taken to conduct the test. Data generation guidelines state that the MGEN application is to be used to benchmark the existing WLAN to discover the maximum PPS rate achievable. Data collection during MGEN benchmark testing will encompass activating the logging function of the application to create a log of every sent and received packet, thus providing a record of the exact number of packets sent across the WLAN and a timestamp for each packet logged.

As stated, Phase Two will benchmark the initial WFM by performing data generation using MGEN to create network traffic streams at specific PPS rates. Phase Two relies on two main branches of data collection. Firstly, the MGEN applications logs to determine the network traffic generated, and secondly, the various log files produced by the WFM from the Kismet server application residing on the Forensic Server. As stated, the log files produced by the WFM are the foremost source of data collected during the testing phases. Since the Kismet application is proposed as the software backbone of the WFM system design, the log files produced by the Kismet server application are the main source of collected data. There are a total of 3 log files proposed to be implemented. Firstly, the packet capture log file which contains the collected wireless network traffic in libpcap format. A database of discovered devices is also prescribed, which identifies unique WLANs and devices based on the wireless network traffic processed by the Kismet server. The database provides extensive information regarding each WLAN or wireless device discovered, for example, the time first seen and specific WLAN capability information, such as network encryption method used and channel of operation. Lastly, a text based IDS alert log file which contains intrusion alerts. Table 3.10 displays the proposed Kismet log files to be implemented in the WFM with a brief description of the information collected.

In order to determine the capabilities of the WFM, the MGEN application log files will be compared to the packet capture log file to establish the total number of generated network traffic packets acquired.

Table 3.10: Kismet Log File Types.

Log File Type	**Description**
Packet Capture (pcap)	Wireless network traffic capture log file, saved in libpcap format.
Database of Discovered Devices (netxml)	XML based database of discovered devices based on wireless network traffic processed by Kismet server.
IDS Alert Log (alert)	Text based log file of raised intrusion alerts based on Kismet intrusion alert rules.

Phase Three, the stabilised benchmark testing of the WFM, will follow similar data collection requirements as described in Phase Two. The packet capture log file will again be compared to the MGEN application log files to establish the total number of generated network traffic acquired by the WFM. Additionally, iPerf application output will be collected when performing the bandwidth test between the wireless drone and Forensic Server. Furthermore, an additional test will be conducted using the 'top' command in the Linux OS, in order to collect the CPU and RAM usage of the WFM components.

The recreation of attacks and subsequent acquisition of evidentiary trails in Phase Four requires a number of individual data collection areas. Again, the Kismet log files will be collected as previously described to assess the acquisition capabilities of the WFM system design. Each attack will be recreated with the tools proposed in Table 3.8. According to the proposed tools documentation, each attack will be conducted with the 'verbose' option to provide additional output, such as total number of frames injected and timestamps of injected frame. The application output of each tool will be collected to compare to the packet capture logs collected by the WFM to establish the acquisition capabilities of the system design.

In summary, the main points of data collection include the WFM log files produced by the Kismet application, as well as various application logs such as MGEN log files and the application standard output from the other various tools proposed.

3.4.3 Data Reporting, Analysis & Presentation

Subsequent to performing data generation and collection during the various testing phases, the information gained will be reported, analysed and presented in order to clearly convey the findings achieved.

Data reporting is needed to convey the findings from each separate research testing phase. The various points outlined by the data collection requirements will be examined and aggregated data produced will be clearly reported in a table format. It is proposed that there will be various important points of interest that need to be reported. For example, during benchmark testing the total number of frames generated by each test and the total number of frames subsequently acquired by the WFM will be important aspects to report, displaying the wireless network traffic acquisition capabilities of the system design. In addition, percentage results will also be calculated to provide an overview of the capabilities. Data analysis will be carried out in order to examine the findings that have been previously reported. The data analysis procedures as shown in Table 3.11 are exceptionally important as it examines the reported data and analyses various important aspects in relation to the goals of the different research testing phases.

Table 3.11: Data Analysis Procedures.

Data Analysis Procedures	Description
PCAP manipulation	Splitting and merging of packet capture log files based on time or WLAN properties.
PCAP examination	Filtering and manipulation of packet capture log files to reduce data set.
PCAP analysis	Forensic and statistical analysis of packet capture log files to determine system capabilities.

As wireless network traffic capture is the main source of data generated during the testing phase, data analysis will process the packet capture log files (pcap) which have been collected from the WFM. In order to analyse the packet capture log files the Wireshark application will be used. Specific wireless network traffic filters that are built into Wireshark will be used to filter the entire packet capture log file and identify the wireless network traffic that has been generated using the various methods previously outlined. For example, to analyse the acquired wireless network traffic from the WFM collected during benchmark testing, Wireshark filters can be used on the packet capture log file to filter the acquired network traffic that was generated by the MGEN application. Examples of possible Wireshark filters include filtering the packet capture log file based on Service Set Identifier (SSID), Basic Service Set Identifier (BSSID), source and destination MAC addresses and 802.11 frame type to name a few. Another example of data analysis based on Wireshark filtering methodologies is analysis of the recreated attacks conducted in Phase Four of testing. In order to analyse the acquired wireless network traffic from the WFM, the packet capture log file collected from the aireplay-ng deauthentication attack can be filtered to discover the frames injected by the attacker using the following Wireshark filter:

```
wlan.fc.type_subtype == 0x0c && wlan.sa == 00:11:22:33:44:55
```

The Wireshark filter will identify all the 802.11 deauthentication frames originating from a specific MAC address (in the example, 00:11:22:33:44:55), such as the attacker's wireless adapters MAC address.

Aside from analysis of the WFM log files, other methods of data analysis will be conducted to examine additional data collection sources. The MGEN application log files and application standard output from the various tools, proposed for use during testing, will be conducted using a standard text editor application, such as 'gedit' provided by the Ubuntu Linux OS. Data analysis of the collected data will be conducted manually, although in some situations the method of line numbering (provided by the application) will be used to analyse certain aspects, such as number of network packets generated by the MGEN application and stored in the collected log file.

Finally, the data that has been reported and analysed will be clearly displayed to present the findings. Various graphing techniques are proposed so that the findings are presented in a visual medium to easily convey the results to the reader.

3.5 EXPECTED OUTCOMES

The expected outcomes of the proposed research methodology will be outlined and discussed briefly in regards to each of the testing phases proposed in the research model design (see Table 3.4).

Phase One of testing involves implementing the existing WLAN components including the AP and client STA. After establishing devices and configurations, the connection between devices will be subsequently benchmarked to discover the capabilities of the existing WLAN infrastructure. It is expected that the bandwidth and packet per second tests will show similar results that other researchers have achieved using the 802.11g standard WLAN (see Section 3.1.5). Such results can be expected due to the use of similar wireless devices operating on the same 802.11 standard, therefore aligning with previously tested packet transmission rates. For example, the packet per second capability rates of the existing WLAN is expected to be approximately 3700PPS, the maximum packet test rates achieved in an encrypted WLAN environment.

Phase Two of testing involves implementing and subsequent benchmark testing of the WFM system design. The implementation of the WFM components will require significant trial and error of varying configurations. However, it is expected that the system architecture will be formed using the hardware and software configurations described (see Section 3.3.2.1). After implementation of the WFM, it is expected that the benchmark testing will also follow similar patterns to previous results achieved by the MCS Base Implementation (see Figure 3.2) running 2 wireless adapters, as prescribed in the hardware configuration for the wireless drone.

Phase Three of testing involves alteration of the WFM based on findings from initial testing, then the subsequent benchmarking of the stabilised model. Improvements will be made to both of the WFM components, the wireless drone and Forensic Server. It is expected that the subsequent benchmark testing will produce slightly better results, including performance and reliability, due to refinement in the hardware and software configurations.

Phase Four of testing involves the recreation of attacks against the WLAN and the associated evidence acquisition by the WFM. The WFM is expected to be capable of acquiring and preserving the wireless network traffic generated by the recreated WLAN attacks. Therefore, the evidentiary trails acquired to determine that an attack has taken place and digital evidence to link an attack to a specific wireless device.

3.6 LIMITATIONS OF RESEARCH METHODOLOGY

The research methodology that has been proposed poses a number of limitations which will be outlined and discussed so that constraints in the proposed research may be recognised. It is important to identify such limitations in order to correctly evaluate the results obtained and to determine if, or where, further areas of research are needed in the scope of performing digital forensic investigation in WLANs.

The first main limitation of the proposed research is that there are numerous configurations in which 802.11 WLAN system architectures may be implemented. Such configurations include the use of any four of the main IEEE 802.11 standards available, 802.11a, b, g and n. Each 802.11 WLAN standard has particular differences in the operation, implementation and capabilities of the means to provide wireless networking communication between compatible devices. These differences vary in the security features available, network bandwidth capabilities and the radio frequency used for wireless communication. For example, the operation and implementation of 802.11a and 802.11b are completely different system designs due to operating on different radio spectrums (5GHz and 2.4GHz respectively) and the network speeds they are able to provide (54Mbps and 11Mbps respectively). Another example is the use of 802.11 security features that may be implemented in a WLAN, ranging from the original Wired Equivalent protocol (WEP) to 802.11i amendment specifications and the introduction of WPA. Furthermore, differences vary between the available 802.11 hardware devices that may be used and the capabilities of such devices.

In the proposed research testing methodology a single existing WLAN configuration is proposed to be tested using the WFM. The proposed existing WLAN entity will only operate using the 802.11g standard, and will be used due the maturity of the mode of operation, widespread usage and the availability of compatible devices and software. Additionally, only one network encryption protocol is proposed to be used in the WLAN being monitored (WPA2-PSK). A single WLAN configuration has been chosen because of the inability to conduct testing on all of the available network configurations and of the differences discussed in WLAN system architecture also show that it is unrealistic at this time to propose testing on all of the possible variations that may be implemented. Therefore, the testing of a single existing 802.11 WLAN in the research conducted will evaluate the implemented WFM in a single scenario only. Differences in existing 802.11 WLAN configurations will need to be addressed in extended research to further test the capabilities and performance of the proposed WFM.

Another limitation of the proposed research testing methodology is the environment in which the testing will be conducted. Previous research in the capability of wireless sniffing applications has usually been conducted in a RF shielded environment (see Section 3.1.5). However, an RF shielded environment will not be available for the testing of the WFM and therefore the possibility of RF interference could potentially cause discrepancies in the results gathered. However, RF interference (especially in the 2.4GHz frequency) is always a likelihood in any WLAN infrastructure, so the lack of a shielded environment could conceivably provide more accurate ‘real world’ results.

A further limitation of the proposed research testing methodology is the restriction of the types of attacks to be conducted against the wireless medium. There are numerous 802.11 WLAN attack methods and associated tools that provide the ability for an attacker to compromise a WLAN. Such attacks range from technical attacks on 802.11 security features defined by the 802.11 standard, to attacks against the implementation of the 802.11 standard. Due to the wide range of possible attacks available, only two main types of attacks are proposed to be conducted against the existing WLAN infrastructure: Denial of Service and FakeAP attacks.

During the research testing phase only one software configuration has been chosen; the Kismet application. Full commercial wireless IDSs will not be evaluated due to the costs involved. Therefore, products such as AirMagnet Enterprise and Motorola AirDefense have been eliminated from the research testing phase. The exclusion of such products creates research testing limitations when all possible system architectures are not able to be tested for the capability of conducting digital forensic investigations in a WLAN.

3.7 CONCLUSION

Chapter 3 focussed on developing the research methodology to conduct testing in the chosen research area of acquiring and preserving wireless network traffic from a WLAN. Similar previous studies were reviewed to learn from previous associated methodologies. The tools and recommendations presented by other researchers were also studied to aid in development of testing methodologies. The additional information gained from the review of similar studies, coupled with the comprehensive literature review in Chapter 2, was used to develop the research questions, as well as the predicted hypotheses for each question. The proposed research model was then outlined, providing a logical progression of testing phases to be conducted. A descriptive methodology was employed to form the proposed system design, consisting of the system architecture and components. Furthermore, the proposed data requirements, expected outcomes and limitations of the proposed research methodology were detailed and discussed.

Chapter 3 has thus presented an overview of the chosen research methodology. The research data map (see Figure 3.5) provided a graphical chart of the main and secondary research questions, linking each question to a specific phase of testing and the associated data collection point. The proposed phases of testing presented in Figure 3.6 outlines the phases of research testing needed to address the research questions. The model provides the goals of each phase of testing, involving implementing the system design in a testing environment. Following each separate phase of testing the associated data will be gathered and evaluated. It is anticipated that the challenge of building and stabilising the forensic model and then launching attacks against the implemented system to test its capabilities will be challenging.

Chapter Four

RESEARCH FINDINGS

4.0 INTRODUCTION

Chapter 3 has formulated the research questions based on the problems and issues pertinent to digital forensic procedures in Wireless Local Area Networks (WLANs). From this, the research methodology was then established. Furthermore, expected outcomes were discussed, as well as identified limitations of the proposed research methodology.

Chapter 4 will now report the research findings from the system design and testing phases proposed in Chapter 3. Firstly, variations made to the proposed data requirements established in the research methodology will first be addressed in Section 4.1. Then, in order to clearly articulate the research findings, various techniques will be used. The outcomes from each independent but consecutive four phases of testing will be reported and analysed to evaluate the implemented system design and determine the capabilities of the Wireless Forensic Model (WFM). The summarised data from each phase will be presented in tabled format in Section 4.2 (initial testing findings) and Section 4.3 (stabilised testing findings). The results of the stabilised benchmark testing and recreated attacks will show the success rate of the system design. At the close of the chapter, in Section 4.4, the research findings will also be displayed visually in a graphic format.

4.1 VARIATIONS IN DATA REQUIREMENTS

A number of variations to the originally proposed research methodology in data requirements (Section 3.4) have been made. It is important to identify these variations prior to the reporting of the findings from the research testing phases. Any differences between the proposed methodology and the final methodology used during the testing phase of the research are therefore set out in the following sub sections.

4.1.1 Data Generation & Collection

During the course of performing the research testing phases, a number of challenges arose which subsequently prompted changes being made in the proposed techniques for data generation and collection.

The first change involved the use of the Multi-Generator (MGEN) application to generate data on the existing WLAN. During the initial testing phases it was found that MGEN was not specifically designed to perform network packet testing in 802.11 WLANs. The data generated by MGEN, is instead, specifically designed for Internet Protocol (IP) based networks and generates Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets. The generated packets are then encapsulated within an 802.11 data frame and transported over the WLAN. Further research then discovered that there were no tools specifically designed to generate wireless network traffic, and so the MGEN application continued to be used as the main data generation tool of choice. Instead, it became necessary to make appropriate changes regarding the methodology of testing. The MGEN tests had revealed that every data packet sent by MGEN was encapsulated into an 802.11 data frame. It also had an associated acknowledgement frame generated by the client Station (STA) destined for the Access Point (AP). An acknowledgement frame is generated by the client STA to ensure the data transmission is received correctly from the AP. Thus, twice the amount of network traffic is generated on the existing WLAN as every data frame is also presumed to have an associated acknowledgement frame. Therefore, the WFM was also now collecting acknowledgement frames and, as such, would be included in the benchmark testing of the WFM as well as in the statistical findings from testing.

A second discovery was the absolute need for time management of all components in the system architecture. Time is an exceptionally important aspect for both the final requirements of the WFM and for testing purposes. In order for correct analysis of the gathered data to be carried out, timing on the WFM and existing WLAN components had to be synchronised. To accomplish correct time management, the Forensic Server was configured as a Network Time Protocol (NTP) server which maintained the correct date and time by synchronising with an Internet based NTP server. The Forensic Server then provided the NTP service to authorised devices on the local network. During testing, the wireless drone, existing WLAN AP and client STA were all configured to periodically synchronise with the Forensic Server. Therefore, all testing components had the same date and time settings to allow for collected data to be easily examined.

The final variation from the proposed methodology was the inclusion of a test to establish the effect of the Denial of Service (DoS) attacks performed against the WLAN. So that the test could be conducted, the ping application was initiated on the client STA, pinging the AP every second throughout the duration of the attacks. The inclusion of the "ping test" was primarily to assess whether the attacks could potentially disrupt a WLAN, reinforcing the need to acquire evidence from wireless networks if such a scenario occurred.

4.1.2 Data Reporting, Analysis & Presentation

In response to testing, only one variation was made to the proposed methodology of data analysis and reporting. The addition of the development of Forensic Profiles for each of the recreated WLAN attacks was now to be included. Forensic Profiles of attacks were then developed by performing an attack against the existing WLAN and initiating a local network packet capture on the attacker's system. The packet capture file was subsequently analysed to determine the 802.11 frames used to perform the attack, and a Forensic Profile outlined in order to map the gathered evidence to the conducted attack. The process of developing Forensic Profiles was necessary as the associated documentation of the attack tools used did not specify which 802.11 frames were used to conduct the attack, nor how many frames were generated during a specified duration of the attack. Each Forensic profile is discussed in the associated findings section.

4.2 INITIAL TESTING FINDINGS

Initial testing of the project was proposed as it was anticipated that difficulties may occur in the implementation of the hardware and software configurations to be used during the research testing phase. The main goal of initial testing was to assess the implementation of the proposed system design of the WFM and its ability to acquire and preserve wireless network traffic as a form of digital evidence.

In order to ultimately evaluate the capabilities of the WFM it was essential firstly to perform initial testing on the existing WLAN infrastructure in which the readiness model was to be installed. Therefore, Phase One involved initial testing of the existing WLAN consisting of an AP and associated STA. Following this, the WLAN was then subjected to a range of benchmark testing to ensure the capabilities of the network, such as bandwidth and maximum packet per second generation rates.

Once the initial testing of the existing WLAN had been shown to be in order, Phase Two of initial testing, this time incorporating the WFM, was then conducted. The WFM components were implemented into the existing WLAN and data generated using the same methodologies to the initial testing of the existing WLAN. Different hardware and software configurations were examined and tested to develop a stabilised design, which could be used and relied on, for the final stage of the research testing.

4.2.1 Phase One: Evaluation of Existing WLAN Capabilities

Phase One, the first stage of initial testing, involved implementing the existing WLAN with an AP and an associated client STA and performing benchmark testing to evaluate the capabilities of the network.

The AP used was a wireless router, manufactured by TP-Link, model TL-WR1043ND. Due to the difficulties in performing benchmark testing on a wireless router with standard firmware, the AP firmware was upgraded to a custom compiled OpenWRT firmware image. The image was built using the OpenWRT source code from the development branch (trunk revision 22321) designed specifically for software development use and testing. Included in the custom compiled firmware were the MGEN and iPerf applications, both used for wireless networking benchmark testing. The latest release at time of testing, MGEN (version 5.01b) and iPerf (version 2.0.5) were used. Furthermore, the wireless networking stacks and drivers were also included in the custom firmware and configured to operate using the 802.11g standard. The AP was also configured with Wi-Fi Protected Access version 2 (WPA2) network encryption and the Pre Shared Key (PSK) option.

The client STA implemented in the existing WLAN, the laptop computer, was an Apple MacBook, model 5-2, with built-in AirPort Extreme wireless adaptor. The Apple laptop was also installed with the necessary applications to perform wireless benchmark testing, MGEN (version 5.01b) and iPerf (version 2.4.0). MGEN was compiled from source code for the OS X operation system, while iPerf was installed using DarwinPorts (a system for running open source applications on OS X). The full hardware and software specifications for the existing WLAN client STA and AP is displayed in Appendix A.

Table 4.1: iPerf Bandwidth Results of the Existing WLAN.

	Data Transferred (Mbytes)	**Bandwidth (Mbyte/sec)**
Test 1	190	26.5
Test 2	190	26.6
Test 3	190	26.6
Test 4	190	26.5
Test 5	190	26.5
AVERAGE	**190**	**26.54**

The iPerf application was first used to perform a bandwidth test on the existing WLAN between AP and client STA to ensure the wireless network was operating at optimal speeds. The iPerf application was used with default settings, and a ten second test conducted with five separate runs to evaluate the bandwidth of the existing WLAN. The findings of the iPerf bandwidth test are displayed in Table 4.1.

After the available bandwidth of the existing WLAN was tested and accepted to be normal for an 802.11g network with the specified network encryption method, the MGEN application was used to test the packet per second (PPS) capability of the wireless network. As previously outlined in Data Requirements (Section 3.4.1) of the research methodology, it was proposed that several PPS rates were to be used during the testing phase of the research. The outlined rates were set at 2200, 3700 and 6000PPS. In order to ensure that the proposed data generation rates were able to be achieved, the three rates were tested on the existing WLAN infrastructure. MGEN uses script files to drive the packet generation between the MGEN server and client. In the existing WLAN architecture, the AP is the MGEN server while the client STA is the MGEN client. Several MGEN scripts were authored to generate network traffic from the MGEN server at 2200, 3700 and 6000PPS rates. Furthermore, a MGEN script was also implemented on the client STA to listen and record a log file of the generated packets which were received. It was discovered that a MGEN server and client are both needed to ensure that correct packet generation takes place. The MGEN server and client were also both required for later analysis to establish correct PPS rates and time taken to conduct the test. An example of the MGEN scripts used is displayed in Appendix A.

Table 4.2: MGEN 2200 Packet Per Second Results of the Existing WLAN.

	Total Number of Generated Packets	**Test Duration (seconds)**	**Aggregated PPS Rate**
Test 1	128344	59.75	2147.95
Test 2	129269	59.91	2157.72
Test 3	128853	60.18	2141.29
Test 4	129117	59.84	2157.85
Test 5	129128	59.82	2158.59
AVERAGE	**128942.2**	**59.90**	**2152.68**

Tables 4.2, 4.3 and 4.4 show the respective results of the benchmark capabilities of the existing WLAN infrastructure in terms of maximum PPS rates. Each test was run 5 separate times for a period of 1 minute to ensure a consistent result. The associated tables display the number of network packets generated by the MGEN application, the test duration and calculated PPS rate from the gathered data. The full tabulated results are displayed in Appendix A.

Table 4.3: MGEN 3700 Packet Per Second Results of the Existing WLAN.

	Total Number of Generated Packets	**Test Duration (seconds)**	**Aggregated PPS Rate**
Test 1	220022	59.75	3682.57
Test 2	219792	59.75	3678.38
Test 3	219825	59.82	3674.59
Test 4	220642	59.91	3682.60
Test 5	221781	59.89	3703.30
AVERAGE	**220412.4**	**59.82**	**3684.29**

Table 4.4: MGEN 6000 Packet Per Second Results of the Existing WLAN.

	Total Number of Generated Packets	**Test Duration (seconds)**	**Aggregated PPS Rate**
Test 1	356478	93.30	3820.69
Test 2	357800	92.08	3885.54
Test 3	357360	89.25	4004.03
Test 4	357051	90.84	3930.51
Test 5	356867	92.85	3843.41
AVERAGE	**357111.2**	**91.66**	**3896.84**

4.2.2 Phase Two: Benchmark Initial Wireless Forensic Model

After the existing WLAN was implemented and benchmarked, Phase Two of the initial testing began by implementing the WFM components into the test system so that further testing could be conducted. Benchmarking of the WFM was carried out using the MGEN application and the PPS generation rates of 2200PPS and 3700PPS discovered in the initial evaluation of the existing WLAN.

As anticipated, numerous hardware and software configurations were trialled during the initial testing phase of the WFM. When implementing the forensic server and wireless drone components of the WFM, the initial model had to be informally tested. Such testing involved various configuration changes to both the wireless drone and forensic server, such as changes in the Kismet configuration files to achieve connection between server and drone. Also many filtering, log files and Kismet source options were investigated to determine effect and usefulness. During the informal testing, the system was also trialled on the ability to acquire traffic generated by the MGEN application.

The Forensic Server was first installed and configured with Ubuntu Desktop 10.04. The latest stable release of Kismet (version 2010-01-R1) was then installed from source code as well as the associated dependencies, such as the libpcap library for network traffic capture. Security is an important aspect of the WFM so, for that reason, Kismet was installed using the Set User Identification (SUID) technique to allow the application to run with an unprivileged user. Kismet was then configured (using the kismet.conf configuration file) to accept incoming network connections from the wireless drone. Other additions were also made to retain specific log file types, to save logs every 15 seconds to a specific location, filter traffic based on AP Basic Service Set Identifier (BSSID) value and configure Intrusion Detection System (IDS) alert rules. As time management is especially important for network traffic capture and performing digital evidence acquisition, NTP was also installed. It was configured to periodically update the system time from internet NTP servers (nz.pool.ntp.org) and to allow local network devices to synchronise time with the Forensic Server. Furthermore, a firewall was established with the iptables application, allowing incoming network traffic on ports 3501 and 123 for Kismet drone and NTP traffic.

The first step of implementing the wireless drone component into the WFM was to choose a specific hardware device. It was proposed that OpenWRT embedded Linux would be the desired firmware of choice running on a type of Single Board Computer (SBC). Research was conducted to find a suitable device which led to the RouterStation Pro produced by Ubiquiti Networks. The RouterStation Pro features Gigabit Ethernet, 680Mhz Central Processing Unit (CPU), 128MB Random Access Memory (RAM) and is designed specifically for OpenWRT firmware. The device also supports the use of up to 3 mini-PCI wireless cards.

The next stage of implementing the wireless drone involved the compiling and installing of a custom OpenWRT firmware image. In the early stages of compiling the firmware image from the development source code, the OpenWRT application repositories only included Kismet version 2009-06-R2, an old version in terms of Kismet-newcore. Since release, numerous changes through constant development had been made to Kismet and so it was decided to attempt to compile the same version for the wireless drone as had been previously installed on the Forensic Server (2010-01-R1). Therefore, Kismet was cross compiled using the OpenWRT build environment for specific use on a wireless router with a MIPS processor. The initial Makefile (see Appendix A) used to include the Kismet drone with the OpenWRT build environment proved exceptionally difficult to compile without programming errors that would cause the Kismet application to malfunction. However, during later testing, another Makefile authored by members of the OpenWRT community was added to the application repositories. The second Makefile contained a number of changes needed to port the Kismet application to a different computing platform and could thus be compiled without any programming errors.

Although Kismet was now compiling correctly there were still a number of issues including the use of correct wireless networking frameworks and drivers and the ability for Kismet to operate with the specified software. For example, if Kismet is compiled without mac80211 support, it is unable to create a virtual wireless interface in monitor mode and support packet capture from that interface. After initial research and testing, including many OpenWRT firmware builds, a preliminary testing build was finally decided on. The OpenWRT version used in initial testing was subversion revision 22414. The full specifications of software and hardware configurations for both the forensic server and wireless drone are in Appendix B.

In order to maintain forensic integrity of the collected data from benchmark testing, the three Kismet log files produced from each test conducted were hashed using the Message Digest algorithm 5 (MD5) to assign a unique cryptographic hash value to the log files. The MD5SUM application, which is a built-in tool provided with Ubuntu Linux (and almost all Linux based distributions), was used to calculate the hash value which was recorded in a separate database file containing file name, modification date, size and the corresponding hash value. Furthermore, all the log files that were produced and hashed were moved to an external storage medium which was made read-only after copying the various files to the storage device. Duplicate copies of the log files were also maintained by creating two separate hard drive partitions, each storing a single copy of the acquired data. Although automation of the described process to maintain the integrity of collected data would have been desirable, the process was conducted manually for each test conducted.

The final stage of initial benchmark testing of the WFM in Phase Two was subsequently conducted to assess two scenarios: first, the performance and second, the packet capture capabilities of the proposed system. In each testing scenario different wireless adapters and the associated wireless driver were trialled in the wireless drone. The testing involved a similar methodology that was used when evaluating the existing WLAN maximum packet per second capabilities in Phase One. The existing WLAN AP was configured to use the MGEN application to generate network traffic at the rates of 2200PPS and 3700PPS discovered in Phase One. Also, the laptop was again configured to be the MGEN client to receive and record log files of the testing conducted. The duration of the test was now increased to 5 minutes, run at a total of 5 times for each selected rate to achieve a more consistent result. Furthermore, the test was also conducted with a single wireless adapter running and then again with both wireless adapters running. Performing both these tests allowed for the later evaluation of the WFM running either the single or dual wireless adaptors which was to be later implemented for the stabilised testing. The following two sections outline the performance results of the WFM using two different wireless drone configurations each with different wireless adapters and associated wireless drivers installed in the device. The full tabulated results as well as the full hardware and software specifications from Phase Two of testing are in Appendix B.

4.2.2.1 Drone configuration one

Drone Configuration One involved the use of two Mikrotik R52N wireless adapters in the RouterStation Pro device. At the outset the R52N wireless adapter was chosen as it provided all of the major IEEE 802.11 wireless standards: 802.11a, b, g and n. Moreover, the adapters also offered Multiple Input Multiple Output (MIMO) technology, dual antenna connectors and ath9k driver support under the mac80211 Linux wireless networking stack. The ath9k driver is essentially used to provide 802.11n support on Linux based systems. However, the configuration used during testing put the wireless adapter in 802.11g mode. The results of the MGEN packet per second testing can be seen in Table 4.5.

Table 4.5: Data and Acknowledgement Frame Acquisition Performance of WFM Drone Configuration One.

Frame Type	Number of Adapters	2200PPS	3700PPS
Data Frame Acquisition	1	100.73%	98.09%
	2	100.81%	88.96%
Acknowledgement Frame Acquisition	1	99.94%	96.63%
	2	99.35%	78.41%

4.2.2.2 Drone configuration two

Drone Configuration Two involved the use of two Ubiquiti XtremeRange2 wireless adapters in the RouterStation Pro device. The XR2 wireless adapter was chosen as it is recognised as one of the most sensitive and powerful wireless adapters available. In addition, the XR2 is specifically designed to operate using Linux madwifi drivers which are now ported into the mac80211 framework. The XR2 offers antenna connector and ath5k driver support under the mac80211 Linux wireless networking stack. The results of the MGEN PPS testing can be seen in Table 4.6.

Table 4.6: Data and Acknowledgement Frame Acquisition Performance of WFM Drone Configuration Two.

Frame Type	**Number of Adapters**	**2200PPS**	**3700PPS**
Data Frame Acquisition	1	99.88%	94.54%
	2	104.69%	93.21%
Acknowledgement Frame Acquisition	1	99.72%	57.96%
	2	99.97%	55.32%

4.2.3 Initial Testing Data Analysis

The purpose of the initial testing phase of the research was to implement and benchmark both the existing WLAN infrastructure and the WFM components used to monitor the WLAN. The data analysis then undertaken is used to identify and examine the results obtained from the initial testing phases in order to establish a stabilised WFM system design.

The results from performing benchmark testing of the existing WLAN in Phase One determined that the network was operating at an acceptable level in terms of bandwidth and at the lower rates of PPS capabilities. The bandwidth testing showed the existing WLAN was capable of an average of 26.54Mbps, which is normal for an 802.11g based WLAN with encryption enabled. In terms of the achievable PPS rate, the existing WLAN was capable of maintaining a constant flow of packet generation at 2200PPS and 3700PPS. However, when the rate was increased to 6000PPS, the existing WLAN was only capable of achieving approximately 3900PPS. In an encrypted WLAN the 6000PPS rate is unachievable due to the increased overhead of encrypting each 802.11 data frame which the MGEN generated UDP packet is encapsulated within. Another point of interest is that the MGEN application was unable to achieve the exact PPS rates and the exact duration times that were specified in the MGEN scripts. For example, even though a rate of 2200PPS over a period of 60 seconds was specified, MGEN generated packets at an average rate of 2153PPS over a 59.90 second interval. It demonstrates that the MGEN packet generation rates are approximate only and do not provide precise results. Therefore, correct procedures need to be taken when conducting such testing; for example retaining logs produced by the MGEN application to determine the correct amount of packets generated as well as the time taken to conduct the test. Both tests conducted in Phase One have produced results indicating that a stable WLAN testing environment was configured, where additional tests could then be conducted on the initial WFM implementation. Furthermore, baseline PPS capabilities were discovered providing the acceptable packet generation rates for later phases of testing.

The proposed data requirements for data analysis were used to perform examination of the data collected by the WFM from initial testing. Wireshark was used to perform packet capture analysis on the Kismet packet capture log file, while the ‘gedit’ application was used to analyse the various other text based log files produced. Each Kismet log file that was produced was hashed with a unique MD5 value and multiple copies stored on an external hard disk which was write protected after the data was copied onto the device. Furthermore, a database of stored log files was maintained containing the file name, date modified, size and unique hash value. During data analysis, each log file was checked by comparing the unique hash value of the file to the database of collected evidence, and analysis performed on the file from the write protected storage medium. The methods used to ensure forensic integrity proved effective in preserving and providing viable digital evidence.

Phase Two of testing involved implementation and benchmark testing of the initial WFM design. The most notable findings from initial testing of the WFM show that different configurations of the wireless drone component are an important contributing factor to the overall performance of the WFM and the network traffic acquisition capabilities. The Forensic Server, however, was more than capable of collecting the data being forwarded from the wireless drones. The high power of the computer, including CPU power and RAM available, meant that the Forensic Server was also able to preserve all the data being forwarded. The CPU load was periodically checked which averaged to approximately 50% load. As discussed the wireless drone was implemented with two different configurations and subsequently benchmarked. The benchmarking results of the WFM indicate the total percentage of generated data collected. The results are divided into two sections of frame acquisition performance: the data frames generated by the MGEN application, and the acknowledgement frames. The results are further divided into either single or dual wireless adapters which are in use at the time of testing.

Unfortunately, there were discrepancies with the aggregated findings of the collected data from the WFM. The discrepancies include multiple times where more than 100% of the generated network traffic was collected by the WFM. For example, Drone Configuration One at 2200PPS with a single and dual wireless adapter acquired more than 100% of the generated data frames produced by the MGEN application. The results, again, indicate the apparent issues with only approximate network packet generation results being achieved. The issue was identified to occur when network packets were sent multiple times by the MGEN server due to transmission errors and a duplicate packet was resent. Thus, the WFM collected both versions of the same packet, increasing the percentage of data frames acquired.

Nevertheless, in terms of data acquisition capabilities of the generated MGEN traffic, both drone configurations were capable of acquiring a very high percentage of the generated traffic with single and dual radios at 2200PPS. However, with an increased PPS speed, neither of the drone configurations was able to obtain a constantly high percentage level acquisition rate. At 3700PPS with dual radios, Drone Configuration One acquired approximately 89% of generated data, while Drone Configuration Two was able to acquire approximately 93% (see Tables 4.5 and 4.6 respectively). In terms of acknowledgement frame acquisition, again the performance at 2200PPS was very high for both configurations (in the region of 99% for both) with single and dual adapters. However, once more at 3700PPS with dual adapters, Drone Configuration One was only able to achieve approximately 78% and Drone Configuration Two achieved even less at approximately 55% at the same rate. Therefore, although the data acquisition rates were high overall, neither drone configurations were able to achieve a high percentage collection rate of acknowledgement frames.

Theoretically, the acknowledgement frame is sent after every data frame. Nevertheless, there is no way of confirming that the acknowledgement frames are actually being sent by the AP, whereas, it is possible to state how many data frames are generated by MGEN by using it's logging function. The percentage results of acknowledgement frame acquisition rates were calculated by the number of acknowledgement frames acquired divided by the number of data frames recorded in the MGEN logs. The method is based on the theory that each generated MGEN frame has an accompanying acknowledgement frame. In terms of data acquisition, Drone Configuration Two was able to obtain a slightly higher percentage. However, Drone Configuration One was able to acquire a higher percentage of acquisition when acknowledgement frames were included in the calculation.

Aside from the results obtained in initial testing of the WFM, there were also other aspects discovered during the course of benchmark testing. Firstly, it was discovered that the wireless drone experienced an extremely high CPU load when the Kismet drone application was collecting wireless network traffic. The 680MHz CPU was at 99-100% load during each of the MGEN tests, regardless of the different PPS rates used. Therefore, initial testing showed that implementation of a higher powered CPU could lead to higher acquisition percentage results.

A second factor discovered during initial testing of the WFM, was the acquisition of corrupt beacon frames being captured under the mac80211 framework and ath9k driver when using the R52N wireless adapter (Drone Configuration One). The XR2 wireless adapter, again using the mac80211 framework but changing to the ath5k driver, did not have the same issue with corrupt beacon frames. The identified problem was exceptionally important in terms of acquisition of wireless network traffic by the WFM. If corrupt beacon frames are being acquired, there is obviously a concern with the monitor mode functionality of the driver in use. Issues may then ensue with the potential evidence acquired by the WFM. An example of a corrupt beacon frame is shown in Figure 4.1. The example has been extracted from a Kismet netxml log file collected during initial testing of the WFM capabilities. The correlating packet capture log file also contained the corresponding corrupt beacon frame packet.

```
<SSID first-time="Wed Aug 25 22:19:23 2010" last-time="Wed Aug 25 22:19:23 2010">
            <type>Beacon</type>
            <max-rate>48.000000</max-rate>
            <packets>1</packets>
            <beaconrate>10</beaconrate>
            <encryption>WPA+TKIP</encryption>
            <encryption>WPA+AES-CCM</encryption>
            <essid cloaked="false">tplink1043\025\323</essid>
            </SSID>
<BSSID>00:27:19:FE:40:88</BSSID>
```

Figure 4.1: Example of Corrupt Beacon Frame Acquired by WFM Drone Configuration One using mac80211 ath9k wireless driver.

As shown in Figure 4.1, the acquired beacon frame has a corrupt 802.11 frame header resulting in incorrect information displayed about the WLAN. The revealing detail is the ‘essid’ field which shows “tplink1043\025\323” when the actual beacon frame should contain “tplink1043ap”, being the correct AP Service Set Identifier (SSID).

Drone Configuration One, and the use of the Mikrotik R52N wireless adapter and ath9k driver, were discarded for use in the final stabilised wireless drone configuration mainly due to the corrupt beacon frame issue. It was disappointing because the Mikrotik wireless adapters performed better in terms of collecting a full data set of wireless network traffic when both data and acknowledgement frames were counted. However, due to the absolute need for reliability and correctness of acquired evidence for potential forensic purposes, such issues cannot be apparent in the stabilised system. Had it not been for the corrupt beacon frame issue, the stabilised wireless drone configuration would probably have been based on one Mikrotik R52N and one Ubiquiti XR2 wireless adapter.

4.3 STABILISED TESTING FINDINGS

Initial testing during Phase One and Two revealed a number of conclusions from the data analysis and provided a reasonable ground on which to base the final stabilised system design of the WFM. The implementation and subsequent testing of the stabilised WFM is now outlined in the following sections. Firstly, in Phase Three, the WFM system configuration is discussed and benchmark testing conducted. The testing methodologies are again drawn from initial testing results and analysis. Finally, in Phase Four, the stabilised WFM is evaluated according to the ability to collect evidence of recreated attacks conducted against the existing WLAN infrastructure.

4.3.1 Phase Three: Benchmark Stabilised Wireless Forensic Model

One of the most significant factors discovered during initial testing was the importance of which wireless drone configuration was to be used. In contrast, no major changes were needed for the Forensic Server when once it was implemented and tested. However, the wireless drone did require reconfiguration based on the results obtained from initial testing. One area which proved especially important was the difference in capabilities of the wireless adapters used in the wireless drone. The optimal system configuration discovered from the initial WFM benchmarking was to use one Mikrotik R52N and one Ubiquiti XR2. Initial testing data collected showed the Mikrotik wireless adapter was capable of a high packet per second acquisition rate. Ultimately though, it was decided not to pursue with that particular configuration due to the instability of the ath9k driver used by the Mikrotik wireless adapter.

Aside from manipulation of the wireless adapters, a number of other software configurations were also made to the wireless drone. The OpenWRT version was upgraded (to revision 22414), as well as the associated mac80211 wireless networking stack and ath5k wireless drivers. The RouterStation Pro CPU was also overclocked to 800MHz (from manufacture specifications) as a high CPU load was recorded during initial benchmarking of the WFM. Lastly, the Kismet drone application was upgraded to version 2010-07-R1 which included numerous fixes for the drone to server communication protocol. The Kismet version on the Forensic Server was also upgraded to version 2010-07-R1 to match the new drone Kismet version. The final stabilised system configuration of the wireless drone and forensic server can be seen in Appendix C.

The first test conducted in benchmarking the stabilised WFM was to measure the bandwidth between the wireless drone and Forensic Server. The same methodology that was used to measure the bandwidth of the existing WLAN was conducted using the iPerf application. Table 4.7 reports the iPerf bandwidth results of the Gigabyte Ethernet LAN link between the Forensic Server and wireless drone.

Another test conducted in order to evaluate the capabilities of the stabilised WFM system configuration followed the same methodology as outlined and applied during initial testing. The AP, in the existing WLAN, generated network traffic to the client STA using the MGEN application at the same packet per second rates previously outlined. The same MGEN scripts were used on both AP and client STA. However, one change was made to the stabilised testing configuration. Instead of simply powering on the second wireless adapter, it was included in the Kismet configuration file to perform hopping on all channels in the 2.4GHz radio frequency channels, though not including the channel which the first wireless adaptor is locked onto. This meant that the first adaptor was permanently monitoring channel 10 (for which the existing WLAN AP is configured) while the second wireless adapter hops channels 1, 2, 3, 4, 5, 6, 7, 8, 9 and 11. The final results of stabilised testing of the WFM is displayed in Table 4.8 which show the percentage of UDP data packets and acknowledgement frames acquired by the stabilised WFM at 2200 and 3700 packet per second rates. The full tabulated results from Phase Three of testing is displayed in Appendix C.

Table 4.7: iPerf Bandwidth Results of WFM Ethernet Connection.

	Data Transferred (Mbytes)	**Bandwidth (Mbyte/sec)**
Test 1	341	286
Test 2	341	286
Test 3	341	286
Test 4	341	286
Test 5	344	288
AVERAGE	**341.6**	**286.4**

Table 4.8: Data and Acknowledgement Frame Acquisition Performance of the Stabilised WFM.

Frame Type	**Number of Adapters**	**2200PPS**	**3700PPS**
Data Frame Acquisition	1	100.23%	92.19%
	2	99.70%	90.35%
Acknowledgement Frame Acquisition	1	99.99%	56.43%
	2	99.40%	49.97%

An additional test was conducted to determine the performance of the Kismet drone application running on the wireless drone, by utilising the ‘top’ command to provide the CPU and RAM usage. The performance test was conducted during the MGEN stabilised benchmarking testing at 2200PPS, 3700PPS and when MGEN was not actively generating data but Kismet was still gathering non-MGEN frames. The tests were performed, first with a single wireless adapter running, and secondly, with both wireless adapters running and were also carried out 3 separate times to ensure consistent results were obtained. Table 4.9 displays the aggregated findings of the wireless drone performance testing, showing the CPU and RAM usage of the Kismet drone application.

Table 4.9: Wireless Drone System Performance: CPU & RAM Usage.

		Kismet Running	**2200PPS**	**3700PPS**
Single Radio	CPU Usage:	0.33%	74%	99.33%
	RAM Usage:	5%	5%	5%
Dual Radio	CPU Usage:	4.67%	83.67%	100%
	RAM Usage:	8%	8%	8%

4.3.2 Phase Four: Evidence Collection of Recreated Attacks

Phase Four involved the recreation of specific attacks against the existing WLAN infrastructure, and subsequent acquisition and preservation by the stabilised WFM of the wireless network traffic created. The goal of this phase of testing was to evaluate the capabilities of the WFM to obtain evidence of the different types of attacks conducted and to what extent that evidence was able to be acquired. Furthermore, if the evidence acquired provided enough information to determine than an attack had been conducted.

Two different types of attacks were proposed against the existing WLAN: Denial of Service and FakeAP attacks. In order to reproduce the attacks, a new component was introduced into the system architecture in the form of an attacker equipped with a laptop and an external wireless adaptor. The laptop used for the replicated WLAN attacks is an Asus EEE PC Laptop (model 900HD) running the Backtrack 4 R1 Linux OS. As specified in the research methodology, Backtrack was used as it is pre-installed with a variety of penetration testing tools as well as numerous tools specifically used for conducting WLAN attacks. Each of the recreated attacks and associated methodologies are described together with the findings and are reported in sub-sections 4.3.2.1 and 4.3.2.2 respectively for DoS and FakeAP attacks conducted. The hardware and software specifications of the introduced attacker's device are located in Appendix D. Furthermore, the full tabulated results from both types of recreated attacks from Phase Four of testing are also located in Appendix D.

4.3.2.1 WFM evidence collection of denial of service attacks

A series of testing with variations of software and hardware configurations were made to the originally proposed WFM. The earlier testing was performed to evaluate the WFM and to assess its ability to acquire and preserve 802.11 frames as a source of potential evidence in a WLAN. Now, in the final phase of testing, two separate DoS attacks were conducted for the research: a deauthentication attack using aireplay-ng and an authentication attack using mdk3. In order to establish a profile for each DoS attack, both were conducted on the attacker's computer. A local packet capture session was initiated using Wireshark to capture the frames generated by the attacker. The packet capture file was subsequently analysed to establish the frame types used by each attack tool to orchestrate a DoS attack in a WLAN. The purpose of identifying the types of frames used and the associated forensic profile for each recreated attack was an important aspect of the testing as it provided a profile to search and discover evidence in the WFM packet capture and log files. Each DoS attack profile is displayed in Table 4.10.

Table 4.10: Forensic Profiles of Denial of Service Attacks.

Type of DoS Attack	Injected Frame Type	Wireshark Filter
Aireplay-ng Deauthetication DoS Attack	802.11 WLAN Management Frame - Deauthentication	wlan.fc.type_subtype == 0x0c
Mdk3 Authentication DoS Attack	802.11 WLAN Management Frame - Authentication	wlan.fc.type_subtype == 0x0b

After establishing the forensic profiles of each attack to be recreated, the final phase of the research testing then took place. Due to the differences in performing data generation using the attack tools, different methods were used to establish the type and amount of frames being injected by the attacker. When aireplay-ng was used to perform a deauthentication attack, the application output was used as the baseline for the amount of frames generated. Each DoS attack generates a total of 128 frames, 64 sent to the AP and 64 sent to the client STA. The aireplay-ng attack was run a total of 572 times which equates to an approximate duration of 5 minutes for each test run, generating a total of 73,216 frames for each test conducted. The Kismet server was also configured to detect IDS alerts from the processed wireless network traffic. Specifically, for the DoS attacks, the configuration of Kismet alerts was not altered from the default settings. The data collected by the WFM during the recreated attacks was analysed and statistical data produced by using Wireshark and performing the filter function on the collected packet capture file. Furthermore, the Kismet alert file was also examined to identify alerts associated with the attacks being conducted.

In addition to the DoS attack being recreated, another test was conducted between the AP and client STA to establish the effect of the recreated DoS attack. The ping application was applied to verify the success of the attack as WLAN DoS attacks attempt to deny service to WLAN devices. The ping application was initiated on the client STA laptop, pinging the AP every second for the duration of the DoS attack. The findings of the aireplay-ng deauthentication attack are displayed in Table 4.11. It shows the number of DoS frames generated by the attacker and the number and percentage of the DoS frames acquired by the WFM. The findings from the ping test are displayed in Table 4.12 which shows the number of pings sent from client STA to the AP and the correlated number of successful pings and calculated percentage of packet loss sustained by the WLAN.

Table 4.11: Aireplay-ng Deauthentication DoS Attack: Acquisition Performance Results of Stabilised WFM.

	Total Number of Generated DoS Frames	**Total Number of Acquired DoS Frames**	**Percentage of Acquired DoS Frames**
Test 1	73216	72216	98.63%
Test 2	73216	72316	98.77%
Test 3	73216	71935	98.25%
Test 4	73216	72156	98.55%
Test 5	73216	72487	99.00%
AVERAGE	**73216**	**72222**	**98.64%**

Table 4.12: Effect of Aireplay-ng Deauthentication DoS Attack on the Existing WLAN.

	Total Number of Pings Sent	**Total Number of Successful Pings**	**Percentage Packet Loss**
Test 1	310	16	94.84%
Test 2	310	17	94.52%
Test 3	310	13	95.81%
Test 4	310	19	93.87%
Test 5	310	13	95.81%
AVERAGE	**310**	**15.6**	**94.97%**

As stated, the second Denial of Service attack conducted against the WLAN was an authentication DoS attack using the mdk3 tool. The Forensic Profile investigation showed that the mdk3 attack operates in a similar manner to the Aircrack-ng attack, by flooding authentication frames creating a DoS attack against the WLAN. The same methodologies were undertaken as per the previous attack; by performing the DoS attack against the WLAN for approximately 5 minutes. Again, the test was conducted 5 times to ensure consistent results were obtained. Due to the design of the mdk3 application it was difficult to establish the number of authentication frames injected into the WLAN. Therefore, Wireshark was used to perform a local packet capture when conducting the test to establish the number of frames generated. The packet capture was then analysed using filters to determine the amount of frames that were sent, allowing for the correct analysis of the data collected by the WFM. The ping test was used again to determine the severity of the DoS attack. Table 4.13 displays the acquisition performance results of the mdk3 authentication DoS attack and Table 4.14 displays the effect of the attack using the ping test between client STA and AP.

Table 4.13: Mdk3 Authentication DoS Attack: Acquisition Performance Results of Stabilised WFM.

	Total Number of Generated DoS Frames	**Total Number of Acquired DoS Frames**	**Percentage of Acquired DoS Frames**
Test 1	300346	299108	99.59%
Test 2	300233	299952	99.91%
Test 3	300131	299944	99.94%
Test 4	300526	300439	99.97%
Test 5	300218	299923	99.90%
AVERAGE	**300290.8**	**299873.2**	**99.86%**

Table 4.14: Effect of Mdk3 Authentication DoS Attack on the Existing WLAN.

	Total Number of Pings Sent	**Total Number of Successful Pings**	**Percentage Packet Loss**
Test 1	309	34	89.00%
Test 2	306	28	90.85%
Test 3	306	29	90.52%
Test 4	305	42	86.23%
Test 5	307	29	90.55%
AVERAGE	**306.6**	**32.4**	**89.43%**

4.3.2.2 WFM evidence collection of FakeAP attacks

The second type of WLAN attacks recreated were FakeAP based attacks against the existing WLAN infrastructure. As discussed in the literature review, FakeAP attacks involve the attacker establishing AP functionality and enticing WLAN devices to associate with the fake AP instead of the legitimate one. Again, two separate attacks were recreated: a beacon flood attack using mdk3 and a FakeAP infrastructure using airbase-ng.

A Forensic Profile was also established for each FakeAP attack to provide information regarding how the attacks are conducted by the applications. The same method used to establish the DoS attack profiles was once more used to establish Forensic Profiles. The FakeAP attacks were conducted on the attacker's computer and a local packet capture initiated using the Wireshark application. The packet capture file was subsequently analysed to determine the types of frames used to conduct the attack, which was to be used later to analyse the packet capture log files collected by the WFM. The Forensic Profiles for the two recreated FakeAP attacks using the mdk3 and airbase-ng tools are displayed in Table 4.15.

Table 4.15: Forensic Profiles of FakeAP Attacks.

	Injected Frame Type	**Wireshark Filter**
Mdk3 Beacon Flood Mode Attack	802.11 WLAN Management Frame - Beacon	wlan.fc.type_subtype == 0x08
Airbase-ng FakeAP Attack	802.11 WLAN Management Frame – Beacon and Probe Response	wlan.fc.type_subtype == 0x08 && wlan.fc.type_subtype == 0x05

In order to recreate a FakeAP attack against the existing WLAN, the mdk3 application was used again in beacon flood mode which forges 802.11 beacon frames based on user input. As discussed previously, beacon frames are used in 802.11 WLANs to advertise the availability of an AP to allow client STAs to connect and communicate in the WLAN. Although the mdk3 beacon flood mode attack is not specifically a FakeAP attack, which encourages a user to connect to the fake AP instead of the legitimate AP, it creates a FakeAP attack which does not allow a client STA to connect to it. However, the attack does recreate the same principles that would be used in such an attack. The mdk3 beacon flood mode attack against the existing WLAN was conducted on the attacker's computer targeted against the existing WLAN by broadcasting the same network SSID value. Mdk3 was configured to inject spoofed beacon frames with the SSID value set as "tplink1043ap", the SSID of the existing WLAN. Furthermore, the spoofed beacon frames were set to identify WPA2-PSK as the network encryption and to use channel 4 to communicate the forged beacon frames. As the AP is configured for channel 10, channel 4 was used for the beacon flood attack to demonstrate the capabilities of the wireless drone dual radio configuration. Theoretically, if the WFM was able to acquire a portion of the FakeAP attack, the dual radio configuration would demonstrate capabilities of detecting attacks conducted on a different channel than the existing WLAN uses. In order for the WFM to detect FakeAP attacks, the Kismet FakeAP alert was configured with the unique SSID and BSSID (network name and MAC address) of the existing WLAN. Therefore, if a device is offering the 802.11 wireless service, with the same SSID but a different BSSID, an alert is raised. The alert was configured to allow one alert per second, for a total of 60 per minute. As per previous testing methodologies, the FakeAP attacks were conducted over a 5 minute duration, performed 5 times to ensure consistent results were achieved. Table 4.16 shows the findings of the mdk3 beacon flood mode attack including the number of FakeAP beacon frames generated and the number and percentage of FakeAP beacon frames acquired by the WFM.

Table 4.16: Mdk3 Beacon Flood FakeAP Attack: Acquisition Performance Results of Stabilised WFM.

	Total Number of Generated FakeAP Frames	**Total Number of Acquired FakeAP Frames**	**Percentage of Acquired FakeAP Frames**
Test 1	37260	24963	67.00%
Test 2	37168	24896	66.98%
Test 3	37332	24987	66.91%
Test 4	37400	25084	67.07%
Test 5	37320	24758	66.34%
AVERAGE	**37296**	**24935.8**	**66.86%**

Table 4.17 displays the findings relating to the capabilities of the Kismet IDS used by the WFM. The number of FakeAP beacon frames which were generated are displayed in comparison to the total number of possible IDS alerts and the total number of alerts generated by the Kismet IDS.

Table 4.17: Mdk3 Beacon Flood FakeAP Attack: Generated Alerts by Kismet IDS.

	Total Number of Generated FakeAP Frames	**Total Number of Possible Alerts**	**Total Number of Alerts Generated**
Test 1	18630	300	120
Test 2	18584	300	120
Test 3	18666	300	120
Test 4	18700	300	120
Test 5	18660	300	120
AVERAGE	**18648**	**300**	**120**

As stated, the second FakeAP attack conducted against the existing WLAN was achieved by using the airbase-ng tool. The Forensic Profile investigation showed that the airbase-ng attack creates an AP service and attempts to respond to probe requests made by client STAs to join the FakeAP WLAN. Similar to the operation of the mdk3 beacon flood attack, airbase-ng forges 802.11 beacon frames as well as targeted probe request frames. The airbase-ng attack was run using the Man in the Middle (MITM) attack options which creates a virtual wireless adaptor running a fake software based AP which lures client STAs to connect. Thus, the attack allows an attacker to intercept communication from the client through a wireless network and then forward traffic to the originally intended destination. A number of other options were selected when conducting the airbase-ng FakeAP attack, including saving a packet capture log of all forged frames injected into the WLAN. The log file was then examined for data analysis to compare data generation to the acquisition capabilities of the WFM. Another option selected involved spoofing the FakeAP MAC address to 00:11:22:33:44:55. The findings of the airbase-ng FakeAP attack is reported in Table 4.18 which displays the number of FakeAP frames which were generated and the number and percentage of FakeAP frames which was acquired by the WFM.

Table 4.18: Airbase-ng FakeAP Attack: Acquisition Performance Results of Stabilised WFM.

	Total Number of Generated FakeAP Frames	**Total Number of Acquired FakeAP Frames**	**Percentage of Acquired FakeAP Frames**
Test 1	6250	3870	61.92%
Test 2	6412	3954	61.67%
Test 3	6288	3898	61.99%
Test 4	6412	3937	61.40%
Test 5	6304	4033	63.98%
AVERAGE	**6333.2**	**3938.4**	**62.19%**

The wireless drone component is an important aspect of the WFM. The research methodology proposed that the wireless drone would be equipped with dual wireless adapters in order to detect WLAN attacks occurring on different channels available under the 802.11 standard. The packet capture log file collected by the WFM from the recreated FakeAP attacks were filtered using Wireshark to identify the acquisition channel, that is, the channel which the Kismet application was monitoring when the frame was collected. Table 4.19 shows the results of the FakeAP attacks conducted with the mdk3 and airbase-ng tools indicating the channel from which the attack frames were collected. Since the existing WLAN was configured to operate using the 802.11g standard a total of 11 channels are available. Table 4.19 presents the average frame count acquisition of the WFM of the FakeAP attacks for each of the channels that the wireless drone monitors.

Table 4.19: Mdk3 and Airbase-ng FakeAP Attack Findings: WFM Aggregated Channel Based Acquisition Results.

	Mdk3 Fake AP Attack: Channel Based Frame Count	**Airbase-ng Fake AP Attack: Channel Based Frame Count**
Channel 1	1629.8	231.8
Channel 2	1505.8	239.4
Channel 3	613.6	67.2
Channel 4	35.8	3.4
Channel 5	78	10.8
Channel 6	71.2	0.4
Channel 7	26.6	1.2
Channel 8	641	24.8
Channel 9	1090.8	141.4
Channel 10	18632.4	3121.8
Channel 11	609.4	96.2
Total Frame Count	**24934.4**	**3938.4**

4.3.3 Stabilised Testing Data Analysis

The findings from Phase Two; that is benchmarking of the initial WFM model, provided insight into the capabilities of the system design. The findings were reported and analysed and changes were subsequently made to improve the performance and reliability of the system to acquire wireless network traffic as a source of forensic evidence. Stabilised testing was then a twofold process. It involved Phase Three of testing which was the initial implementation and benchmarking of the WFM, while Phase Four involved the recreation of WLAN attacks against the network and the acquisition of potential evidence by the WFM.

The first test conducted involved performing a bandwidth test between the Forensic Server and wireless drone. The average bandwidth of the network connection between the WFM components was 286.4Mbps (see Table 4.7). The bandwidth test of the existing WLAN achieved an average of 26.54Mbps (see Table 4.1). Therefore, the findings show that the wireless network traffic acquired by the wireless drone has more than enough bandwidth to forward the data collected to the Forensic Server for preservation.

The further results reported during Phase Three have shown the capabilities of the stabilised WFM in terms of acquisition of a full data set of wireless network traffic generated on the existing WLAN. These results (see Table 4.8) show that around 100% of the data generated at 2200PPS was able to be acquired by WFM. However, at the higher rate of 3700PPS the WFM was only able to acquire approximately 92% of the generated data with one wireless adapter running, and approximately 90% with dual wireless adapters running. Similar results of acknowledgement frame acquisition by the WFM were achieved at 2200PPS, with approximately 100% able to be acquired. However, at 3700PPS the WFM was only able to acquire approximately 56% and 50% of acknowledgement frames using the single and dual wireless adapters respectively. The findings were very close to the results obtained for Drone Configuration Two, being due to using the same configuration of two Ubiquiti XR2 wireless adapters in the wireless drone.

A performance test was also conducted on the wireless drone component of the WFM, calculating the amount of CPU and RAM that the Kismet drone application was using during benchmark testing. The Forensic Server was not tested, as initial testing indicated that the server was running well below maximum capacity in terms of CPU and RAM used by the Kismet server application. Furthermore, due to the ease of upgrading the specific platform of the Forensic Server, performance measurements were considered superfluous. In terms of the wireless drone performance, RAM was discovered to be of little importance to the capabilities of wireless network traffic acquisition, using 5 Megabytes (MB) and 8 MB with single and dual wireless adapters respectively. However, CPU usage was discovered to be extremely important, which increased dramatically with an increase of wireless network traffic being collected. At 2200PPS, the CPU usage of the Kismet drone application was approximately 74% and 84% for single and dual wireless adapters respectively, while at 3700PPS the CPU usage increased to 99% and 100% respectively.

Phase Four of testing involved the recreation of attacks against the existing WLAN infrastructure. Two separate types of attacks were conducted including DoS and FakeAP attacks. The purpose of performing data analysis relating to the recreated attacks is to analyse the capabilities of the WFM to detect and acquire evidence in attack situations.

The first DoS attack used was a deauthentication attack using the aireplay-ng tool. A Forensic Profile of the aireplay-ng deauthentication attack was outlined (Table 4.10) and found to operate by flooding the WLAN with 802.11 deauthentication management frames. The attack sends 73,216 deauthentication frames for each of the 5 tests for 5 minute durations. On average the WFM was capable of acquiring 72,222 frames used in the aireplay-ng attack, equating to an average of 99% of attack frame acquisition (see Table 4.11). In contrast to the MGEN tests conducted with 2200PPS and 3700PPS, the aireplay-ng attack was analysed showing that only approximately 128PPS was generated by the attack tool. Therefore, the WFM should be more than capable of acquiring a high percentage of the conducted attack, close to 100% acquisition. However, the findings show that it is still difficult for the model to acquire a perfect 100% of the wireless network traffic created on a WLAN.

As previously discussed, a ping test was also conducted for the duration of the aireplay-ng DoS attack. The goal of the additional test was to identify the effect the attack had on the existing WLAN infrastructure in terms of network communication disruption between AP and client STA. The findings of the ping test showed that the average number of pings sent from client STA to AP was 310, with an average of 15.6 successful pings (see Table 4.12). The findings equate to a 95% packet loss between AP and client STA and shows that only 5% of the generated network traffic by the ping test reached the intended destination. It can therefore be confirmed, that the aireplay-ng DoS attack is able to disrupt WLAN communication thus resulting in an effective DoS attack.

The second DoS attack used was an authentication flood attack using the mdk3 tool. A Forensic Profile, also developed for the mdk3 authentication flood attack, discovered that the attack operated by flooding the WLAN with 802.11 authentication management frames (Table 4.13). The recreated attack was run 5 times for 5 minute intervals, resulting in an average of 300,290.8 authentication frames injected per test conducted. The WFM was capable of acquiring an average of 299,873.2 authentication frames, which equates to a 99.86% average (see Table 4.13). Again, the mdk3 authentication flood attack had a much lower packet per second rate than the MGEN benchmarking tests, calculated to be approximately 1000PPS. The ping test was once more conducted to determine the effectiveness of the DoS attack. The findings of the ping test show that the average number of pings sent was 306.6, with 32.4 successfully sent packets. The results show that the mdk3 authentication flood DoS attack caused the existing WLAN network 89% packet loss (see Table 4.14). Although the packet loss percentage was lower than the aireplay-ng deauthentication attack, 89% packet loss still represents major disruption to WLAN communication, and again, an effective DoS attack.

There were a number of interesting findings made during data analysis of the DoS attacks using the Wireshark application. Firstly, the aireplay-ng DoS attack forges all 802.11 deauthentication frames with a sequence number starting at a zero value, while the mdk3 DoS attack used 0 as the sequence number for every forged frame. Another important aspect of the findings was that both the aireplay-ng and mdk3 tools forge all 802.11 frames which do not include the actual MAC address of the wireless adapter used by the attacker. Instead, the tools use the command line user input to forge the 802.11 frames with information such as source and destination MAC addresses. For example, the aireplay-ng deauthentication attack requires the MAC addresses of the client and AP of the target WLAN, and forges deauthetnication frames with the entered values. Thus, the deauthentication frames injected into the WLAN have the legitimate MAC addresses of both devices being attacked. In terms of the intrusion detection capabilities provided by the Kismet IDS for the WFM, neither DoS attacks generated any alerts regarding the attacks conducted. There are, however, two separate alert rules specifically for detecting DoS attacks. Given the description of the IDS alerts from the Kismet documentation, the aireplay-ng deathentication attack would have matched the 'DEAUTHCODEINVALID' rule.

Phase Four of testing also involved the recreation of FakeAP attacks against the existing WLAN infrastructure. The first FakeAP attack was conducted using the mdk3 application and the beacon flood mode attack. A Forensic Profile was developed which discovered that the mdk3 beacon flood attack forges 802.11 management beacon frames (see Table 4.15) based on the user input to the application. The findings show that over the 5 minute duration of the 5 tests conducted, an average of 37,296 forged beacon frames was generated by the attacker. The WFM was able to acquire an average of 24,935.8 frames. Therefore, the WFM was able to acquire an average of 66.86% of the generated FakeAP attack frames from the 5 tests conducted (see Table 4.16).

The second FakeAP attack conducted against the existing WLAN was recreated using the airbase-ng tool. Again, a Forensic Profile was developed using the previously outlined methodologies. The airbase-ng tool was discovered to forge both 802.11 beacon and probe response frames (see Table 4.15). The average number of FakeAP frames injected by the attacker was 6333.2 over the 5 tests conducted. The WFM was able to acquire an average of 3938.4 of the FakeAP frames, calculating to an average acquisition rate of 62.19% (see Table 4.18). Again the PPS rate of both FakeAP attacks were calculated to compare to the previous results obtained. The mdk3 attack was used with the default frame injection rate (50 per second) which generated an average of approximately 124 frames per second. The airbase-ng attack was also used with default frame injection speeds and generated an average of approximately 21 frames per second. Both results show that the FakeAP attacks conducted have a very low frame per second rate when compared to the MGEN tests previously conducted.

The FakeAP IDS alert, provided by the built-in Kismet alert rules, was configured to report any discovered AP service advertising the same SSID as the existing WLAN with a different BSSID (AP MAC address). In terms of the IDS capabilities of the WFM an average of 120 alerts per test conducted was achieved during the mdk3 beacon flood attack. However, due to the operation of the airbase-ng tool, no IDS alerts were triggered for the second FakeAP attack. Furthermore, even though the alert was configured to raise an alert every 1 second, with a maximum of 60 per second, each test only achieved an average of 120 alerts per 5 minute test (see Table 4.17). According to the configured alert, a total of 300 alerts should have been triggered.

The Kismet packet capture logs acquired from both FakeAP attacks were also analysed to determine the frame acquisition channel. As specified previously, the wireless drone operates one wireless adapter set to statically monitor channel 10, while the second wireless adapter hops among the ten remaining channels. The findings of the packet capture analysis showed that the 74.73% of the FakeAP attack frames generated by the md3 tool were collected by the static wireless adapter monitoring channel 10 (see Table 4.19). The second FakeAP attack conducted using the airbase-ng tool was also analysed, which discovered 79.27% of the generated FakeAP frames were also acquired by the first wireless adapter monitoring channel 10. Therefore, the addition of the second wireless adapter, specifically designed to acquire wireless network traffic from the remaining channels available, was only capable of collecting approximately 23% of the total number of FakeAP attack frames from both FakeAP attacks conducted.

4.4 PRESENTATION OF FINDINGS

Sections 4.2 and 4.3 reported and subsequently analysed the findings from both the initial and stabilised testing phases of the research conducted. The findings that have been reported will now be graphically presented. The purpose is to interpret the data gathered from the different phases of initial and stabilised testing and to convey the results in a visual manner.

Phase One involved evaluating the existing WLAN capabilities using various benchmarking testing methodologies. The findings from the MGEN benchmark testing of the existing WLAN component of the proposed system architecture is displayed in Figure 4.2, presenting the average PPS rate for each specified packet generation rate of 2200, 3700 and 6000PPS (see Tables 4.2, 4.3 and 4.4). Figure 4.2 visually shows the maximum packet transmission rate per second of the implemented WLAN, which is seen to be approximately 4000PPS based on the data presented.

Phase Two, the initial implementation and benchmark testing of the WFM, has no graphical presentation, as the findings from Phase Three provide better represent the wireless network traffic acquisition capabilities of the stabilised WFM.

Phase Three involved benchmarking the stabilised WFM using the MGEN application to generate network traffic at specific the PPS rates, of 2200PPS and 3700PPS. Furthermore, at each PPS rate the WFM was tested with either single or dual wireless adapters operating in the wireless drone component of the WFM. Figures 4.3, 4.4, 4.5 and 4.6 present the findings of the WFM benchmarking testing. The presented data is sourced from the packet capture logs from the Kismet application which were collected during the benchmarking process. Each figure displays the number of packets logged by the MGEN client as well as the total number of packets acquired by the WFM without any packet capture filtering applied to the acquired data. Each figure also displays the number of MGEN UDP packets and acknowledgement frames acquired by the WFM. Figures 4.3 and 4.4 present the findings of the stabilised WFM benchmark testing at 2200PPS with a single wireless adapter operating and a dual radio respectively, while Figures 4.5 and 4.6 present the findings of the stabilised WFM benchmark testing at 3700PPS with a single wireless adapter operating and with dual wireless adapters operating respectively.

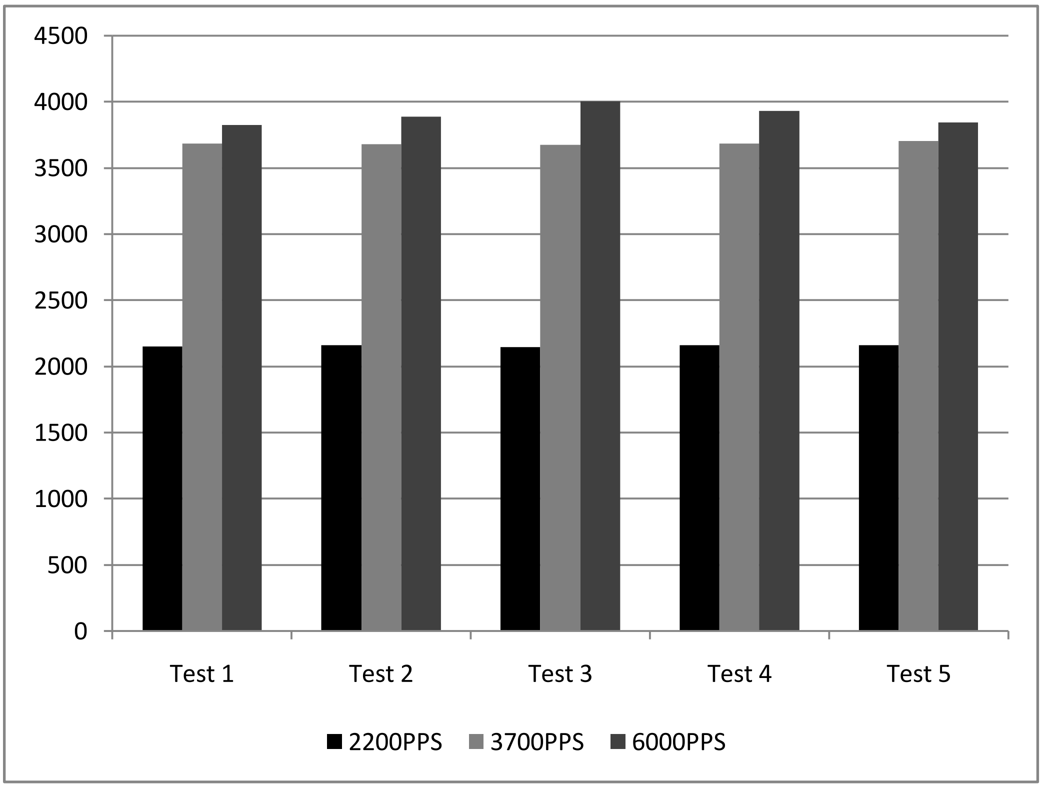

Figure 4.2: MGEN Benchmark Results of Existing WLAN Capabilities: Showing Number of Packets Generated at 2200, 3700 and 6000PPS.

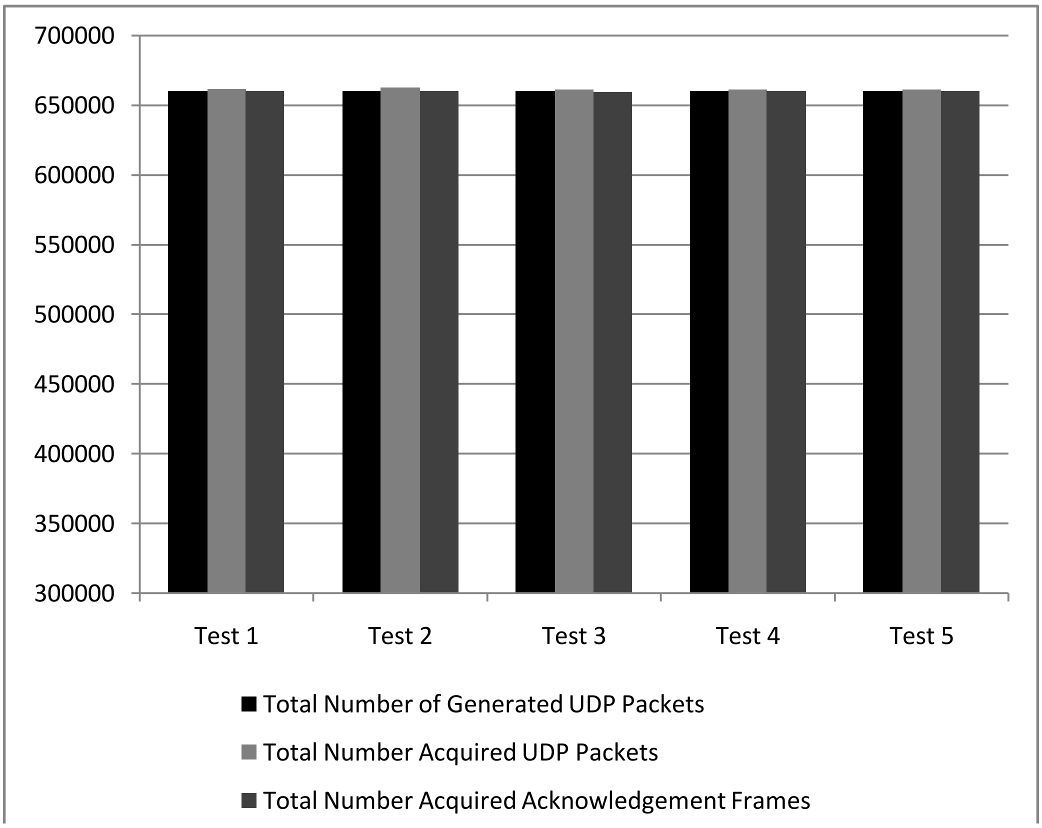

Figure 4.3: Stabilised WFM Benchmark Findings: 2200PPS Single Wireless Adapter.

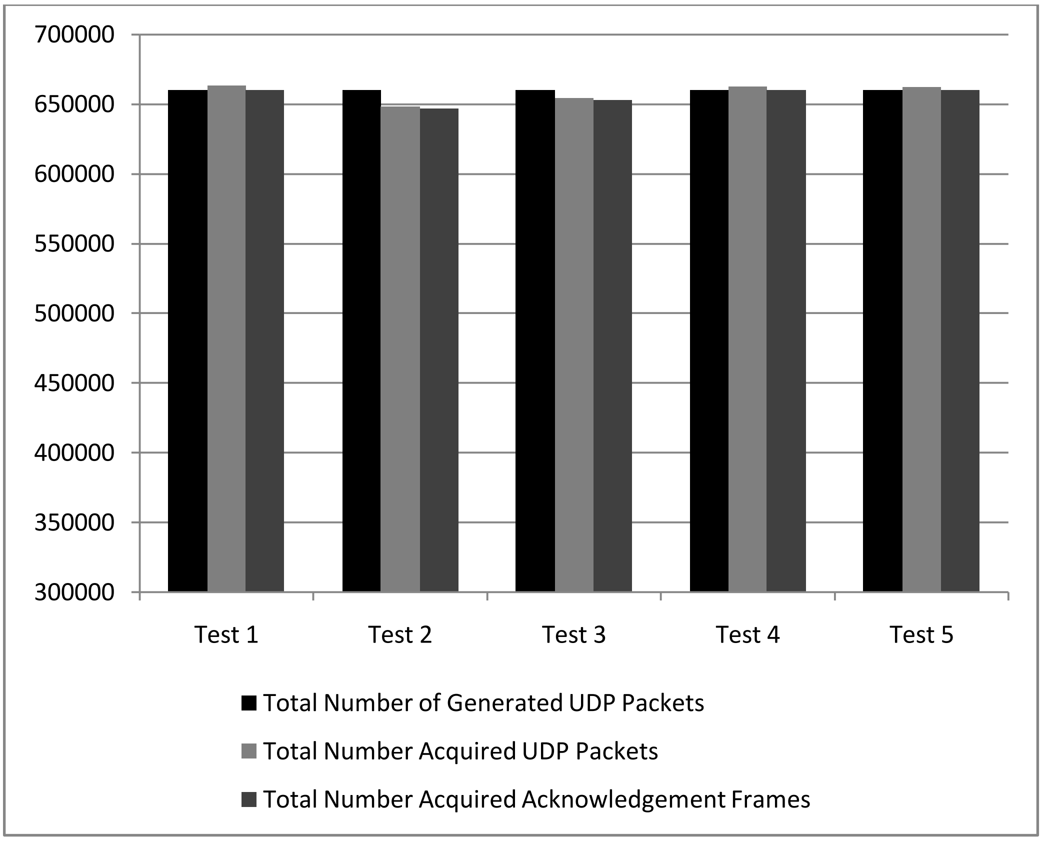

Figure 4.4: Stabilised WFM Benchmark Findings: 2200PPS Dual Wireless Adapters.

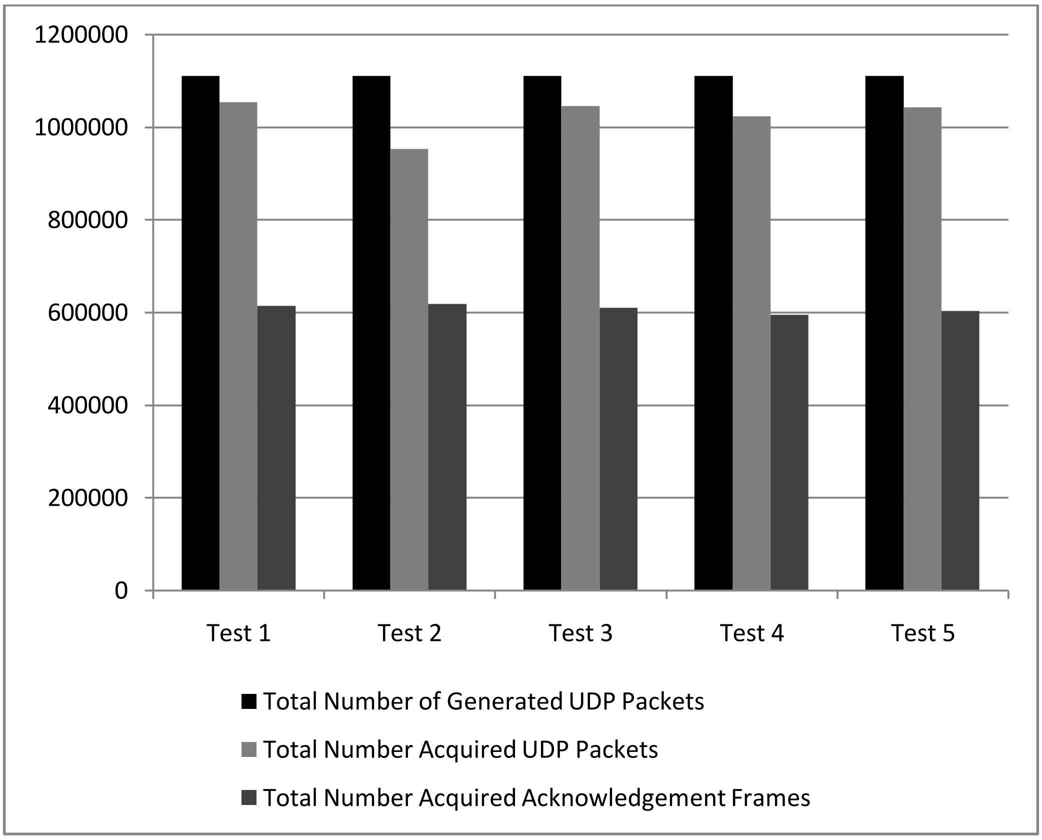

Figure 4.5: Stabilised WFM Benchmark Findings: 3700PPS Single Wireless Adapter.

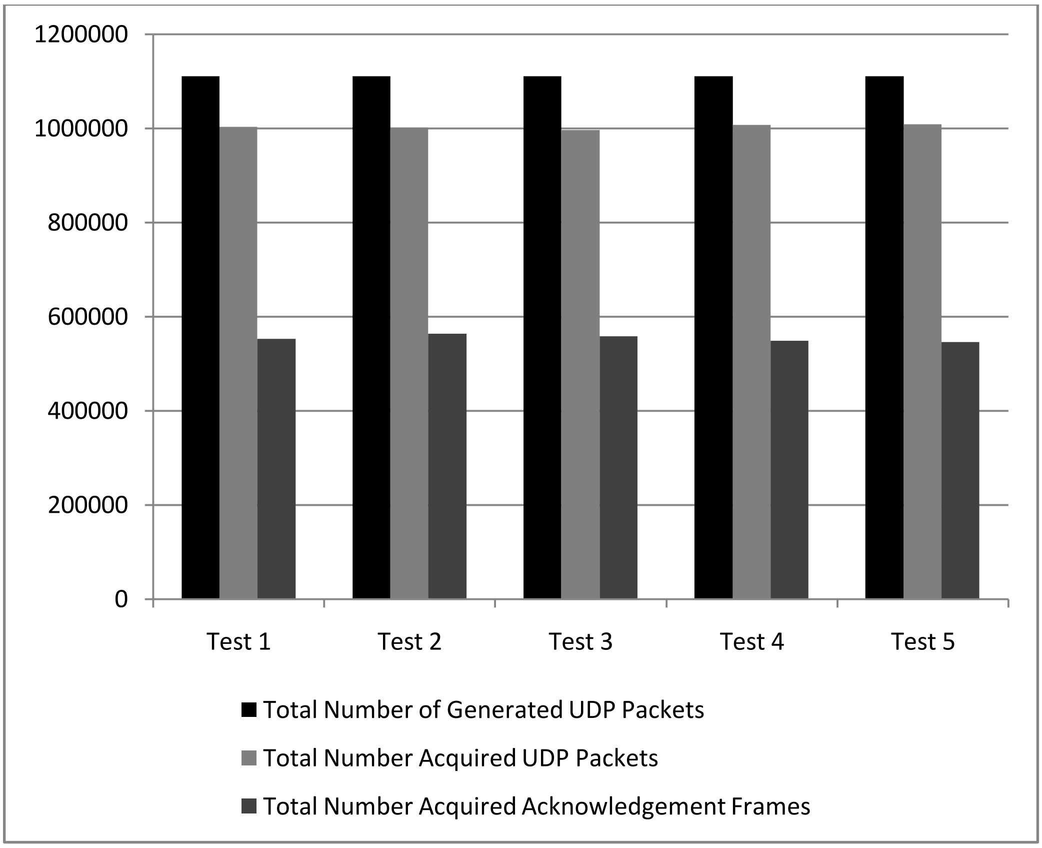

Figure 4.6: Stabilised WFM Benchmark Findings: 3700PPS Dual Wireless Adapters.

Phase Four of testing involved the recreation of attacks against the existing WLAN infrastructure. Two types of attacks were recreated: DoS and FakeAP attacks. Figures 4.7 and 4.8 present the results from the recreated DoS attacks using the aireplay-ng and mdk3 tools respectively. Figure 4.7 displays the total number of DoS frames generated by the aireplay-ng deauthentication DoS attack and the total number of frames acquired by the WFM for each of the 5 separate tests conducted. Figure 4.8 displays the total number of DoS frames generated by the mdk3 authentication DoS attack and the total number of frames acquired by the WFM for each of the 5 tests conducted. The high percentage acquisition capabilities of the WFM are visually seen in Figures 4.7 & 4.8 based on the closeness of generated frames versus acquired frames for each of the 5 tests conducted, for both DoS attacks performed.

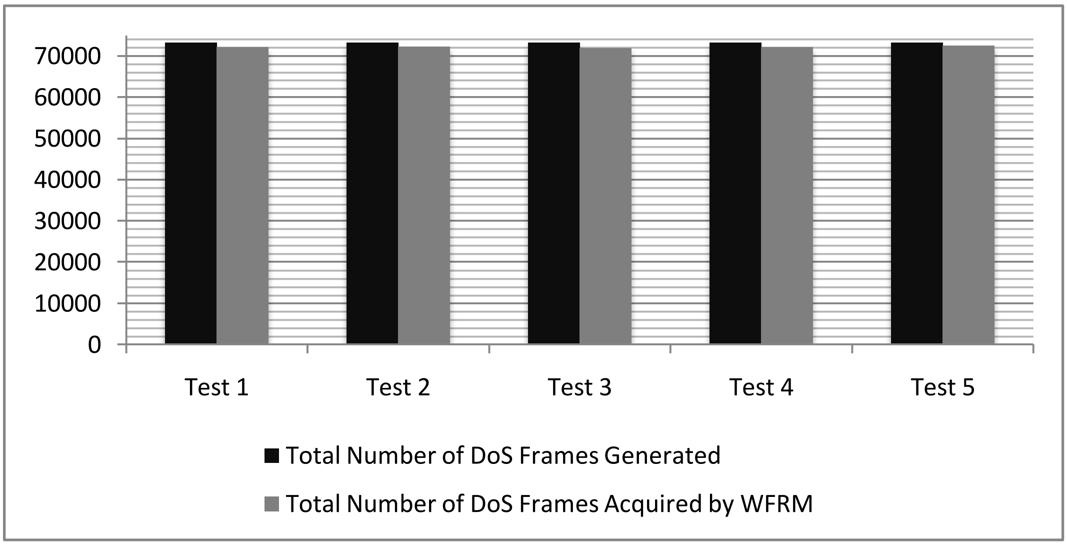

Figure 4.7: Aireplay-ng DoS Attack: Frame Generation vs WFM Frame Acquisition.

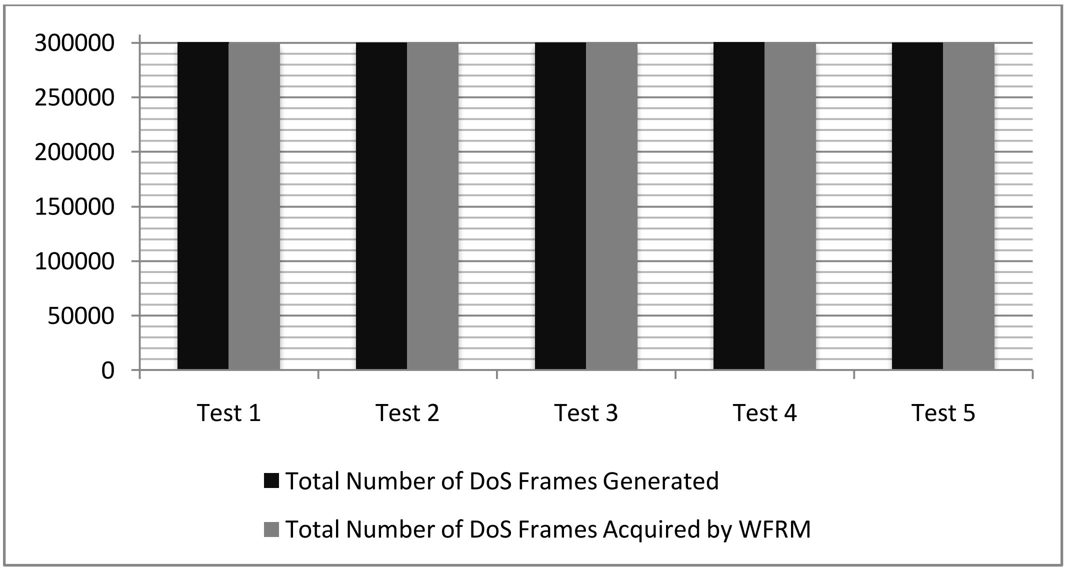

Figure 4.8: Mdk3 DoS Attack: Frame Generation vs WFM Frame Acquisition.

The findings from the recreated FakeAP attacks, using mdk3 and aireplay-ng, are presented in Figures 4.9 and 4.10 respectively. Figure 4.9 displays the mdk3 FakeAP attack findings, showing the total number of forged beacon frames generated by the attacker, as well as the number of forged beacon frames acquired by the WFM. Figure 4.10 displays the airebase-ng FakeAP attack findings, presenting the total number of injected FakeAP frames by the attacker and the total number of frames acquired by the WFM.

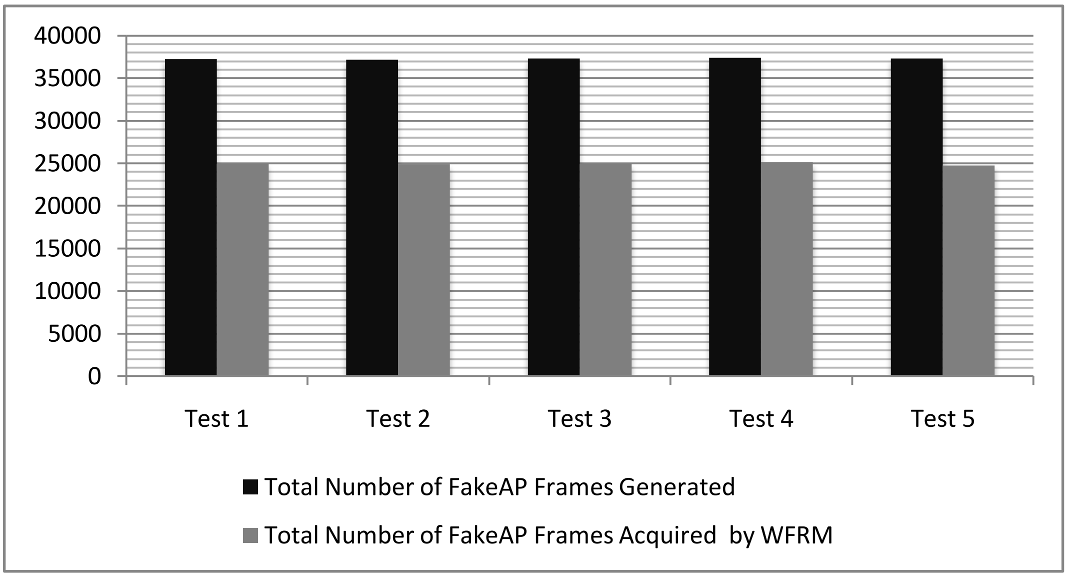

Figure 4.9: Mdk3 Beacon Flood FakeAP Attack: Frame Generation vs WFM Frame Acquisition.

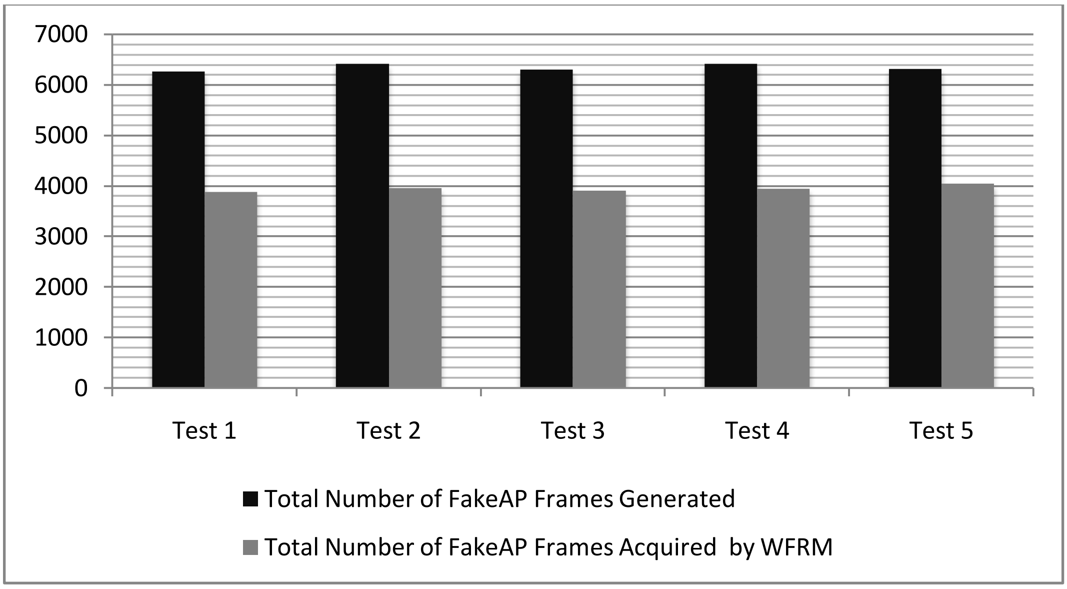

Figure 4.10: Airbase-ng FakeAP Attack: Frame Generation vs WFM Frame Acquisition.

Figures 4.11 and 4.12 illustrate the channel based acquisition findings of the recreated FakeAP attacks. Figure 4.11 presents the channel based acquisition results of the WFM for the mdk3 beacon flood FakeAP attack, while Figure 4.12 presents the channel based acquisition results of the WFM for the airbase-ng FakeAP attack.

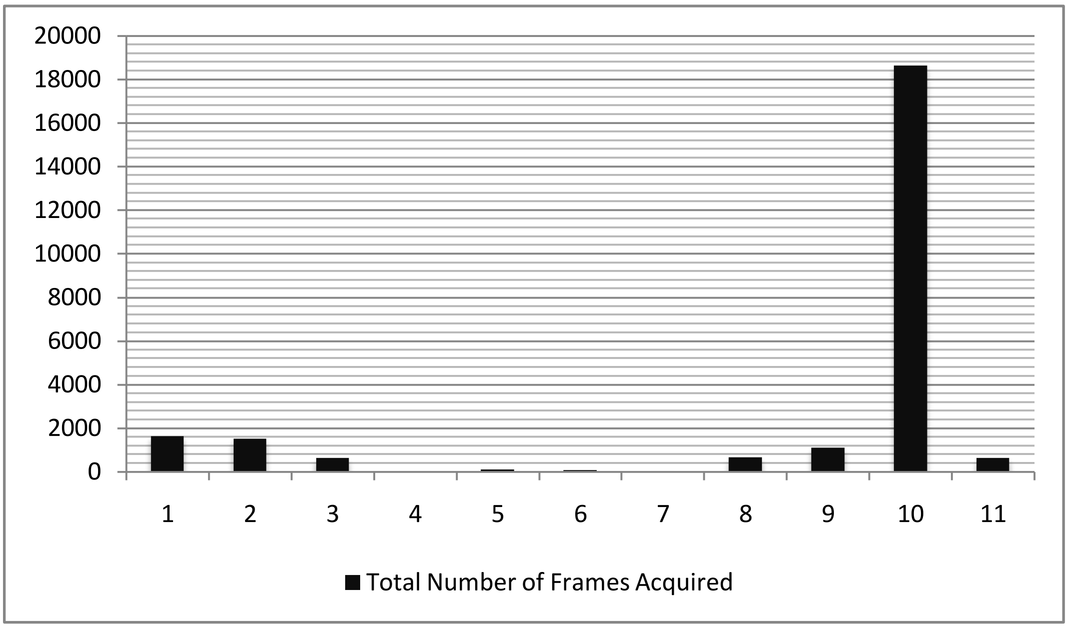

Figure 4.11: Mdk3 Beacon Flood FakeAP Attack: WFM Frame Acquisition based on the Channel Collected.

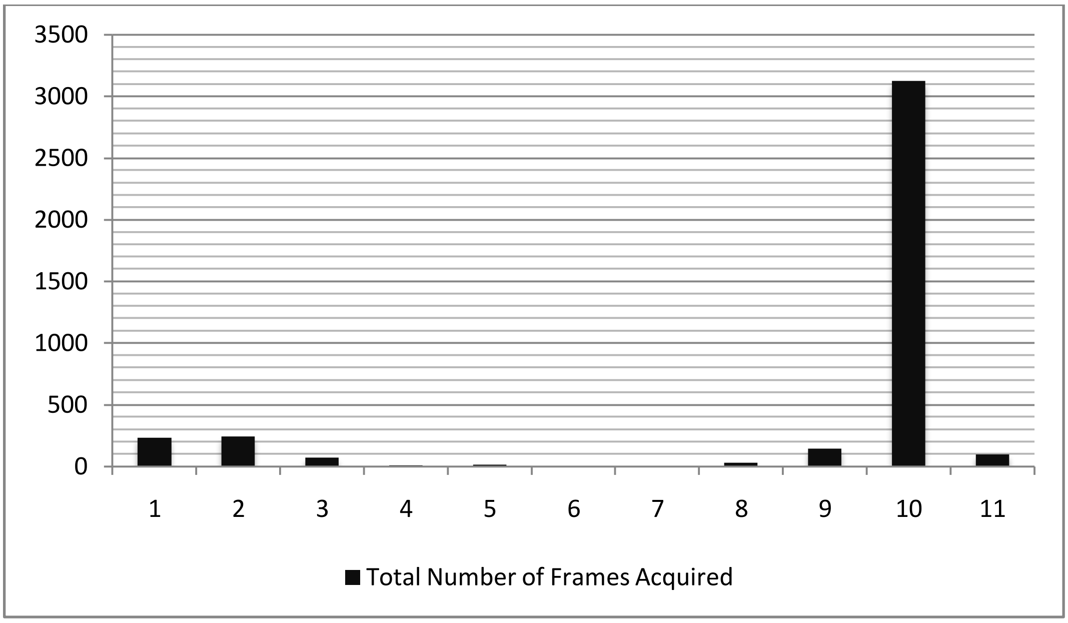

Figure 4.12: Airbase-ng FakeAP Attack: WFM Frame Acquisition based on the Channel Collected.

Figures 4.11 and 4.12 visually display results from the recreated FakeAP attacks based on the specific channel which the Drone acquired the attacker’s injected frame from. For example, when the second wireless adapter in the Wireless Drone was hopping between remaining channels, additional frames were acquired from the attack. Both figures show that the majority of the attacker’s frames were discovered by the first wireless adapter, which was statically collecting network traffic from channel 10.

4.5 CONCLUSION

Chapter 4 has covered the reporting, analysing and presentation of the research findings discovered during the research testing phases. Variations to the originally proposed data requirements (Section 3.4) were outlined and discussed in order to clarify specific changes made to the proposed testing methodology. Initial testing was then conducted, evaluating the existing WLAN capabilities (Phase One), followed by the implementation and benchmarking of the WFM (Phase Two). Initial testing discovered the existing WLAN bandwidth and packet per second transmission capabilities. Furthermore, the wireless drone and Forensic Server components of the WFM were implemented and benchmarked to assess the capabilities of the system design. Stabilised testing was next undertaken (Phase Three) involving benchmarking the stabilised WFM. A final system build was ultimately implemented based on the initial testing results, and a final benchmarking evaluation of the WFM was conducted. The culmination of research testing then involved subjecting the existing WLAN to a series of recreated attacks and evaluating the resultant evidence collection abilities of the stabilised WFM (Phase Four).

Key findings included the ability of the Wireless Forensic Model (WFM) to acquire and preserve wireless network traffic from a Wireless Local Area Network (WLAN). Specifically, the WFM was able to collect a high percentage of wireless network traffic as well as evidentiary trails of recreated WLAN attacks. Furthermore, the evidence acquired was able to be preserved by using hashing methods to ensure the integrity of the collected evidence. The findings show that the proposed system design is capable of acquiring and preserving wireless network traffic as a source of potential digital evidence

Chapter Five

RESEARCH DISCUSSION

5.0 INTRODUCTION

Chapter 4 reported the significant findings achieved from each phase of research testing. The purpose of proposing a research methodology and then performing the various different phases of testing was to investigate the forensic potentiality of the WFM. Chapter Five will now form a discussion of the research findings for each testing phase so that the significance of the results can be evaluated relating to and in association with the discipline area. Furthermore, the findings will be linked to the discussion to provide assurance when evaluating the research methodology, results achieved and conclusions drawn.

To begin with, Section 5.1 will present the previously developed research questions (Section 3.2) in a tabled format. Each question will be answered and discussed in terms of the asserted hypotheses. Arguments will be made for and against the hypotheses and a summary made of the outcome. Following the tabulated questions, the findings of the research will then be discussed in detail in Section 5.2. The reason is to thoroughly evaluate the results, the implementation of the WFM system design and why the results are important for the growth of knowledge in the realm of conducting digital forensic investigations in WLANs. The chapter concludes with Section 5.2 in which the knowledge gained from the research conducted will be used to develop recommendations from the writer outlining best practices and testing methodologies to further promote digital forensic investigations in WLANs.

5.1 EVIDENCE FOR RESEARCH QUESTION ANSWERS

The main question and the following sub-questions were developed from both the literature review (Chapter 2) and the study of similar research cases (Section 3.1). The research questions will now be set out and answered in a table format. The table will be headed by each question asked, followed by the hypothesis as first outlined in the research methodology (Section 3.2). The asserted hypothesis given is a brief theoretical explanation using the knowledge gathered from the literature reviewed at the outset of the research project. The table will then present both the arguments for and the arguments against the hypotheses made, based on the findings of the research testing phases and technical knowledge learned. The arguments for, will be those that find in support of, or prove the hypothesis, while arguments against, will refute or disprove the offered hypothesis. Reference will be made to specific findings to substantiate the statements providing rational reasoning for each argument. At the end of each table, a brief summary of the research question and tested hypothesis will be given in order to accept, reject or found as indeterminate based on the findings achieved.

5.1.1 Main Research Question and Associated Hypothesis

The main research question was developed to provide a specific goal for the research testing phases and to concentrate testing on a particular area. The main research question was: *What are the capabilities of a design system to acquire and preserve wireless network traffic as viable evidential trails from 802.11 WLANs?*

In order to answer the proposed research question several phases of testing were proposed and conducted. The system design of a WFM was implemented and subjected to various testing to determine the capabilities of a system to acquire and preserve wireless network traffic as a source of evidence.

Table 5.1 displays the main research question, the associated hypothesis, arguments for and against are made and a summary of the tested hypothesis is given.

5.1.2 Secondary Research Questions and Associated Hypotheses

A total of 5 secondary research questions were also developed to assist in supporting or answering the different components needed to answer the main research question.

Tables 5.2, 5.3, 5.4, 5.5 and 5.6 display the secondary research questions, from question one to five respectively. Each table also presents the associated hypothesis, the arguments for and against the hypothesis, a summary of points discussed and the significance of the research outcome for each question. A statement of position accepting, rejecting or deeming the hypothesis indeterminate is also given for each question.

Table 5.1: Main Research Question and Tested Hypothesis.

<table>
<tr><td colspan="2"><b><i>Main Question:</i></b> <i>What are the capabilities of a design system to acquire and preserve wireless network traffic as viable evidential trails from 802.11 WLANs?</i></td></tr>
<tr><td colspan="2"><b>Main Hypothesis:</b>
That a system designed to acquire and preserve wireless network traffic is capable of providing viable evidential trails together with ample information to support digital forensic investigations in which WLANs are involved.</td></tr>
<tr><td><b>ARGUMENT FOR:</b>
Wireless network traffic acquisition and preservation is able to be accomplished by the WFM system design.

Evidential trails are able to be acquired and preserved following digital forensic principles and guidelines for electronic evidence handling. The evidential trails consisted of acquired wireless network traffic (see Section 4.2.2), database of discovered wireless devices and an Intrusion Detection System (IDS) alert log from one of the four recreated attacks (see Table 4.17)

In terms of evidentiary trails of WLAN attacks the WFM system design was capable of acquiring and preserving wireless network traffic containing evidence of the conducted attacks (see Section 4.3.2).</td><td><b>ARGUMENT AGAINST:</b>
A full packet capture of wireless network traffic is not able to be acquired and preserved due to limitations of the implemented system, (see Table 4.8), therefore, restricting the possibility of event reconstruction due to lost data.

Further research and testing are still needed in a number of areas surrounding digital forensic practice in WLANs. For example, development of applications used during testing, such as Kismet and Wireshark, for specific forensic purposes. Without such development, viability of acquired evidence may potentially decrease if certain digital forensic principles are not met. Such issues are identified in future research areas (see Section 6.2).

The implemented WFM only provides a single source of evidence derived from wireless network traffic for forensic investigation. Additional sources of evidence may be needed to augment and support the evidential trails acquired and preserved by the WFM.</td></tr>
<tr><td colspan="2"><b>SUMMARY:</b>
The WFM was capable of acquiring a large portion of the network traffic generated on the existing WLAN. Furthermore, the system was also capable of acquiring evidentiary trails of the attacks recreated against the existing WLAN, and in one case, also IDS alerts pertaining to the attack conducted. Although the system design of the WFM is capable of both acquiring and preserving evidentiary trails from 802.11 based WLANs when collecting wireless network traffic, there were limitations in the results obtained. There are still a number of potential issues of the system design and architecture as well as the software and hardware used to implement the system design. The arguments made for and against prove the hypothesis to be indeterminate.</td></tr>
</table>

Table 5.2: Secondary Question 1 and Tested Hypothesis.

<table>
<tr><td colspan="2"><b><i>Secondary Question 1:</i></b> <i>What are the hardware and software requirements for the successful acquisition of wireless network traffic as digital evidence for forensic purposes?</i></td></tr>
<tr><td colspan="2"><b>Hypothesis 1:</b>
That the hardware configurations used need to be ably sufficient to collect and process network traffic, including fast CPU power, high RAM availability and fast LAN links between the system components. The software requirements will need to include the capability to acquire and preserve wireless network traffic using a wireless sniffer based application.</td></tr>
<tr><td><b>ARGUMENT FOR:</b>
The hardware performance showed that CPU usage was very important for wireless network traffic acquisition which increases at higher PPS traffic rates (see Table 4.9).
Wired LAN links between components are important and affect the WFM system design, therefore, must accommodate the needed bandwidth to transport the acquired wireless network traffic transfer of data between components (see Tables 4.1 and 4.7).
The wireless sniffer is also very important to acquire and preserve wireless network traffic. The Kismet application handled all data collection so the capability of the implemented system relies heavily on the software.</td><td><b>ARGUMENT AGAINST:</b>
The hardware performance test determined that RAM was not as important as was anticipated (see Table 4.9).
In terms of software, it was proven that wireless drivers were as important as the sniffer application used (see Section 4.2.3).
Due to the wireless drone design, OpenWRT embedded Linux OS was also considered to be essential from the software perspective, allowing great customisation of the software powering the hardware device.</td></tr>
<tr><td colspan="2"><b>SUMMARY:</b>
Hardware is especially important, both for the Forensic Server and wireless drone components of the WFM. In particular, fast CPU speed and LAN links are crucial. However, high RAM availability was not essential in the acquisition of wireless network traffic. Software requirements included wireless sniffer software as the backbone of the WFM and provided capabilities to acquire and preserve wireless network traffic. However, the firmware and wireless drivers were also discovered to be vital so as to provide a reliable and stable system for the collection of viable digital evidence. The arguments made for and against prove the hypothesis to be indeterminate.</td></tr>
</table>

Table 5.3: Secondary Question 2 and Tested Hypothesis.

<table>
<tr><td colspan="2"><b><i>Secondary Question 2:</i></b> <i>What are the capabilities of the proposed system design to acquire and preserve a full data set of wireless network traffic?</i></td></tr>
<tr><td colspan="2"><b>Hypothesis 2:</b>
That the proposed system will not be capable of acquiring a full data set of WLAN traffic due to the proposed method of monitoring a WLAN with an external device. Nevertheless, enough data can still be acquired to determine and reconstruct certain events, such as an attack against the WLAN. Furthermore, the preservation and integrity of the acquired evidence will be able to be maintained.</td></tr>
<tr><td><b>ARGUMENT FOR:</b>
The WFM was not always capable of acquiring and preserving a full data set of network traffic generated during benchmark testing. For example, the benchmark results from stabilised testing at 3700PPS (see Table 4.8). The WFM was also not capable of acquiring a full data set at lower PPS rates, such as the recreated WLAN attacks in Phase Four. For example, both DoS attacks had low PPS rates (128 & 1000PPS) with approximately 99% acquisition of attack frames.
The network traffic collected from the recreated WLAN attacks provides enough data to determine that an attack has taken place, therefore, providing the ability to reconstruct an attack event from the data gathered.
Using hashing methods, the preserved evidence acquired by the WFM maintains forensic integrity (see Section 2.2.3).</td><td><b>ARGUMENT AGAINST:</b>
At specific wireless network traffic rates the WFM is capable of acquiring 100% of the data generated in the existing WLAN. For example, the stabilised WFM was capable of acquiring 100% of generated network traffic at 2200PPS (see Table 4.8).
In certain scenarios, such as higher level protocol analysis, the inability of acquisition of a full data set may provide potential issues for event reconstruction.</td></tr>
<tr><td colspan="2"><b>SUMMARY:</b>
A full data set of wireless network traffic was not always able to be achieved in certain scenarios. During recreated attacks a full data set was also not collected. However, the significance of the outcome was that enough data was collected to provide information about the attack. Therefore, the hypothesis is proved to be accepted.</td></tr>
</table>

Table 5.4: Secondary Question 3 and Tested Hypothesis.

<table>
<tr><td colspan="2"><b><i>Secondary Question 3:</i></b> <i>What are the capabilities of the system design to provide digital evidence from WLAN attacks?</i></td></tr>
<tr><td colspan="2"><b>Hypothesis 3:</b>
That digital evidence from recreated WLAN attacks is possible by acquiring and preserving wireless network traffic between devices of the WLAN. The IDS system will also provide additional digital evidence of the attacks conducted. Furthermore, the collected evidence will provide details of the type of attack conducted and digital evidence to aid in digital forensic investigation.</td></tr>
<tr><td><b>ARGUMENT FOR:</b>
Each recreated WLAN attack had digital evidence acquired and preserved by the WFM. The attack could be discovered by filtering the packet capture log file based on the forensic profiles developed (see Tables 4.10 and 4.15)

A very high percentage of the 802.11 DoS attack frames injected by the attacker were acquired by the WFM, approximately 99% for both DoS attacks (see Tables 4.13 and 4.11).

However, lower averages of FakeAP frames were acquired by the WFM due to the attacker using different channels to launch the attack. Approximately 67% and 62% of the FakeAP frames injected by the attacker were acquired by the WFM (see Tables 4.18 and 4.16).</td><td><b>ARGUMENT AGAINST:</b>
The IDS did register an intrusion alert for one of the four attacks, however, no intrusion alert was triggered for the other 3 attacks. Therefore, the capabilities of the wireless IDS used in the WFM provide minimal digital evidence</td></tr>
<tr><td colspan="2"><b>SUMMARY:</b>
The WFM is capable of acquiring and preserving wireless network traffic as a source of digital evidence from recreated WLAN attacks. The importance is that the type of attack may be identified based on certain properties of the frames injected by the attacker from which Forensic Profiles were developed. The arguments made for and against prove the hypothesis is accepted.</td></tr>
</table>

Table 5.5: Secondary Question 4 and Tested Hypothesis.

<table>
<tr><td colspan="2"><b><i>Secondary Question 4:</i></b> <i>What is the effect of monitoring multiple 802.11 WLAN channels simultaneously in terms of digital evidence acquired?</i></td></tr>
<tr><td colspan="2"><b>Hypothesis 4:</b>
That multiple 802.11 WLAN channels may be monitored to provide additional evidence for events occurring on different channels, however, the performance and acquisition capability of system may decrease.</td></tr>
<tr><td><b>ARGUMENT FOR:</b>
Additional evidence of recreated FakeAP attacks was acquired by the second wireless adaptor hopping between the remaining channels. However, approximately only 23% of all FakeAP attack frames were acquired by the addition of the second wireless adapter (see Table 4.19, and Table 4.11 and 4.12).
MGEN benchmark testing of the WFM discovered that using multiple wireless adapters affected the acquisition performance of wireless network traffic (see Tables 4.5 and 4.6). The findings from stabilised benchmark testing of the WFM showed an approximate 2% decrease in acquired wireless network traffic data at 3700PPS when the wireless drone was using both wireless adapters (see Table 4.8). Furthermore, acquisition of acknowledgement frames also decreased approximately 6% at 3700PPS when both wireless adapters were in use (see Table 4.8).</td><td><b>ARGUMENT AGAINST:</b>
Although additional evidence was acquired by monitoring multiple 802.11 channels, the amount of evidence gained from the second wireless adapter was minimal (see Table 4.19 and Figures 4.11 and 4.12). Approximately 77% of all Fake AP attacks were collected by the first wireless adapter when monitoring channel 10 only.</td></tr>
<tr><td colspan="2"><b>SUMMARY:</b>
When monitoring multiple 802.11 WLAN channels simultaneously, additional evidence was acquired during the recreated FakeAP attacks; even on different channels to that which the AP was configured for. Nevertheless, the additional evidence was minimal compared to the frames acquired by the first wireless adapter when monitoring the existing WLAN channel 10 only. It was also proven that the WFM, especially the wireless drone component, suffered a decrease in performance when monitoring multiple channels simultaneously. The arguments made for and against prove the hypothesis is accepted.</td></tr>
</table>

Table 5.6: Secondary Question 5 and Tested Hypothesis.

<table>
<tr><td colspan="2"><b><i>Secondary Question 5:</i></b> <i>What are the methodologies, techniques and tools used to conduct digital forensic examination and analysis of the acquired data from wireless network traffic?</i></td></tr>
<tr><td colspan="2"><b>Hypothesis 5:</b>
That examination and analysis of the acquired wireless network traffic follow similar methodologies and techniques to that of wired network traffic. Also, that previously used tools and methods for wired network traffic can be utilised.</td></tr>
<tr><td><b>ARGUMENT FOR:</b>
The same fundamental methodologies and techniques used to analyse wired network traffic, such as data reduction and protocol decoding (see Section 3.1.1) may be used to analyse acquired wireless network traffic in the packet capture file format.
The process of filtering was heavily used during analysis of the data collected during testing (for an example see Tables 4.10 and 4.15). Wireless traffic was filtered using previously outlined methods from literature reviewed. Packet capture logs were filtered by MAC addresses, frame types and timestamps.
Similar tools used to analyse wired network traffic, such as Wireshark, may be used to analyse wireless network traffic as long as the 802.11 protocol is supported by the application.</td><td><b>ARGUMENT AGAINST:</b>
Although fundamental methodologies and techniques may be used during analysis, WLANs have unique properties when compared to normal network traffic. Therefore, wireless network traffic does require specific methodologies and techniques to perform examination and analysis. For example, being able to filter and sort 802.11 frames based on frame sequence number or the ability to identify a frame captured which has a sequence number out of range of the preceding frames.</td></tr>
<tr><td colspan="2"><b>SUMMARY:</b>
Although traditional methodologies and techniques may be used to analyse wireless network traffic, there are a number of specific challenges that wireless network packet capture analysis and examination requires. The significance is that while traditional network packet analysis tools have the capability to analyse 802.11 based wireless network traffic, additional application features would greatly aid in packet capture analysis. Moreover, forensic tools need to be carefully adapted and then tested to provide robust digital forensic packet capture analysis for wireless systems. The arguments made for and against prove the hypothesis is indeterminate.</td></tr>
</table>

5.2 DISCUSSION OF FINDINGS

The research findings have been reported, analysed and presented in Chapter 4. Section 5.2 will now discuss and comment on each of the four phases of research testing and the significance of those results. Each phase of testing will be discussed based on the importance of the findings in terms of answering the various research questions. The WFM will also be evaluated according to the capabilities that the system design was able to achieve and will be further evaluated on the basis of the implemented system design including the hardware and software configurations used. Examination of the performance of the WFM will be carried out based on the prescribed system components. To conclude the discussion, potential issues discovered during testing will be outlined and suggested solutions presented.

5.2.1 Discussion of Testing Phases

Research testing was divided into initial and stabilised testing, comprised of four separate testing phases, each with specific goals. The discussion comprised of the research testing phases will be conducted in order to identify and highlight the important findings. Reference will be made to specific outcomes of interest discovered during testing as well as the research questions which were addressed by each significant test conducted.

Phase One of research testing was critical in setting the stage for the investigation of the main research question. The existing WLAN infrastructure was first implemented and then subjected to various benchmark testing. Although the testing conducted in Phase One did not directly involve answering the research questions, the results obtained proved that a stable WLAN infrastructure for the project had been implemented. The bandwidth of the link between client Station (STA) and the Access Point (AP) was operating at a satisfactory level in terms of the 802.11g standard configured on the existing WLAN (see Table 4.1). A PPS benchmark test was also conducted to establish the WLAN's maximum packet per second (PPS) rate achievable, which was discovered to be approximately 3900PPS, being the average from the 6000PPS Multi-Generator (MGEN) application benchmark test. Furthermore, the testing discovered that the existing WLAN could sustain constant packet flooding rates of 2200 and 3700PPS. Thus, a baseline level of performance results were arrived at and subsequently used during later benchmark testing of the WFM system design. As the WFM is specifically engineered to monitor the WLAN infrastructure, benchmark results are crucial so that the capabilities of the implemented system are clearly known and can be relied on.

Phase Two of research testing involved the implementation and subsequent benchmarking of the WFM. As outlined in the findings (Section 4.2.2), initial implementation of the WFM components involved different software configurations in order to reach a stabilised design. The proposed system design and architecture prescribed by the proposed research model (Section 3.3) provided a foundation on which to implement the WFM. Readily available open source software was used, including Kismet, OpenWRT and Ubuntu Linux. During implementation and testing the wireless drone was discovered to be the most influential component of the WFM in terms of the capabilities of the system design. This was significant in that two separate wireless drone configurations needed to be trialled, with the main difference being the wireless adapters used in each configuration (see Sections 4.2.2.1 and 4.2.2.2). The Forensic Server was also installed and configured which proved to operate reliably and able to store and preserve the wireless network traffic forwarded from the wireless drones. Benchmark testing was then conducted on the two different WFM implementations (see Tables 4.5 and 4.6). The findings provided valuable insight into the capabilities of the initial WFM as well as the hardware and software requirements needed to produce a reliable and functioning system design. Therefore, secondary research question 1 could ably be explained from the findings discovered. As expected, issues were encountered with the system design configuration, such as wireless driver and hardware device capabilities, but did provide detailed information to be later used to implement a stabilised forensic model. For example, issues were discovered with the ath9k driver which collected corrupt beacon frames, therefore, illustrating a problem with the viability of the acquired evidence. While initial testing also provided findings that could be partly used to answer other research questions, the future benchmarking and testing of the stabilised WFM in Phases Three and Four, would provide better representation.

Phase Three of research testing involved implementing the stabilised configuration of the WFM based on knowledge gained from initial testing. As discussed, there were problems encountered, ranging from performance issues to the reliability of data collected. However, the findings from Phase Two provided insight into the necessary requirements of the prescribed software and hardware configurations needed to re-configure the WFM. Section 4.3.1 outlined the changes made to the WFM system configuration which involved upgrading various software applications mainly on the wireless drone component. After a new stabilised system was accomplished, benchmark testing was again conducted to evaluate the capabilities of the re-configured WFM. The goal of stabilised testing of the WFM was now specifically conducted to provide answers to the main research question as well as secondary research question 2. In terms of the capabilities of the stabilised WFM, the findings proved that the system design was capable of acquiring and preserving a high percentage of the data generated on the existing WLAN (see Table 4.8). In answering secondary question 2, the capabilities of capturing a full data set of wireless network traffic by the WFM was not always possible.

However, the results show that on average a high percentage of wireless network traffic was able to be acquired at the maximum transmission rate of the WLAN. Furthermore, the findings also illustrate the effect of monitoring multiple channels available for wireless communication, providing constructive insight into secondary question 4. It was discovered that the use of an additional wireless adapter to monitor multiple channels decreased the overall performance of the WFM.

Phase Four was the final and most important testing phase and a culmination of the learnt outcomes of earlier phases of testing. Various WLAN attacks were recreated and subsequent evaluation of the evidentiary trails that the WFM was able to obtain was undertaken. Two distinct types of attacks were conducted against the WLAN, including DoS and FakeAP attacks. The findings of Phase Four have earlier been reported in Section 4.3.2, analysed in Section 4.3.3 and presented in Tables 4.10 to 4.18. Phase Four aided in answering the main research question as well as secondary questions 3 and 4. The findings showed the evidence collection capabilities of the WFM, including what information and details may be extracted from the collected evidence, and why the information gained will aid a digital forensic investigation involving a WLAN.

Two separate recreated DoS attacks were launched against the existing WLAN infrastructure. The WFM was implemented so that attempts could be made to collect evidence of the conducted attacks. It was effectively demonstrated that firstly, the ping tests conducted during the recreated DoS attacks displayed why it is necessary to implement a forensic system into a WLAN. It was also significant that the ping test findings showed that both of the DoS attacks disrupted communication between devices during the entire duration of the attack. The implemented WFM provided 3 separate log files from which to analyse data regarding the WLAN attack event. The Kismet packet capture log provided an archive of wireless network traffic. The 802.11 frames used in each DoS attack were able to be acquired and preserved by the WFM. It was shown that approximately 99% of all DoS frames from the attacks were acquired and preserved by the packet capture log. Even though potential evidence was able to be acquired, there were a number of considerations that need to be discussed regarding the properties of the obtained evidence. The packet capture log of wireless network traffic proved to be the main source of evidence regarding the DoS attacks conducted, providing an almost complete record of 802.11 frames injected by the attacker. However, due to the discovered operation of the tools used, all of the forged 802.11 frames did not contain the specific wireless adapter’s native Media Access Control (MAC) address of the attacker. Instead the frames contained a MAC address that was spoofed by the attacker when injecting the 802.11 frame, therefore, making it difficult to link the wireless adapter of the attacker to the acquired evidence. In summary, it was determined that the WFM was capable of acquiring and preserving digital evidence providing details of the type of DoS attacks conducted, the time which the attack occurred and the duration of the attack.

Two separate FakeAP attacks were also conducted against the existing WLAN. Once more, similar to the DoS attacks previously discussed, a number of logs generated by the Kismet application were analysed to determine the evidence that could be used for a digital forensic investigation. The logs of interest included the Kismet packet capture log, database of discovered devices and an IDS alert log. The Kismet packet capture provided an evidentiary trail of wireless network traffic captured by the WFM. Furthermore, the database of discovered devices also contained evidence of the FakeAP attacks. In answer to secondary question 4 the design of the wireless drone and the use of dual wireless adapters were specifically implemented to assist in evidence acquisition of attacks occurring on different WLAN channels available (see Table 4.19). Therefore, the recreated FakeAP attacks tested the implemented design as the attacks occurred on different channels from which the existing WLAN was configured for.

Although a phase of testing was not specifically developed for analysis of the collected data, it became apparent that data analysis was an exceptionally important aspect of the research. The collected data from Phases Two, Three and Four was analysed to produce aggregated findings and to determine the capabilities of the WFM. Moreover, data analysis provided an appreciation in being able to address secondary research question 5, as various methodologies and techniques were used to perform data analysis on the acquired wireless network traffic. A network packet analysis tool, namely Wireshark, was used to perform forensic analysis of acquired data using techniques such as filtering and protocol decoding. Therefore, an understanding was gained into the methodologies, techniques and tools that can be used to perform digital forensic examination of wireless network traffic. The discoveries were significant as they provided experience in the techniques used and tools available for conducting wireless network packet capture analysis.

5.2.2 Wireless Forensic Model: Capabilities Evaluation

The main research question addressed during the project focussed on the capabilities of a design system to acquire and preserve wireless network traffic to provide evidentiary trails from WLANs. Therefore, it is prudent to discuss the capabilities of the WFM which was implemented and tested during the project. Each testing phase provided findings and further understanding of the capabilities of the implemented WFM system design.

Firstly, the WFM proved to be capable of acquiring and preserving wireless network traffic, which in turn provided evidentiary trails from WLANs. Therefore, the main source of evidence collected, is the actual wireless network traffic actively communicated between WLAN devices. The acquired data was preserved by the WFM and logged in packet capture file format. The data collected can then be forensically examined to determine the possible use of the data gathered.

The WFM uses a distributed architecture by placing wireless drones at points throughout the WLAN, specifically the wireless drone should be placed at every AP location in a WLAN. The WFM can also be described as a centrally administered system architecture. The Forensic Server is the backbone of the system design, allowing connection to the various drones via the wired portion of the network as well as control of the wireless drones using remote console sessions. The wireless drone is designed to require minimal interaction with the drone device itself, essentially when the drone is placed and configured it should need minimal maintenance.

The significant findings of the various testing phases have been discussed in Section 5.2.1. The results demonstrate that the WFM is capable of acquiring a very high percentage of the existing WLAN traffic as maximum transmission rates. Furthermore, the forensic model is also capable of providing viable and potentially useful evidentiary trails from the acquired network traffic.

In terms of the forensic soundness, the evaluated system design of the WFM provides viable evidence from the collected wireless network traffic. The network traffic was acquired using a stable wireless driver, with no apparent issues operating in monitor mode, thus, allowing correct wireless network traffic acquisition. The data forwarded to the Forensic Server, where it is preserved using hashing techniques, multiple archived copies and storage of data on a write protected medium. All of which add to the forensic soundness of the collected data. Therefore, in conclusion the acquired and preserved wireless network traffic is forensically sound.

5.2.3 Wireless Forensic Model: System Design Evaluation

Throughout the research process, various conclusions were drawn regarding the WFM system components that were implemented and tested. The following section will discuss the capabilities of the Forensic Server and wireless drone components and evaluate the system design. The hardware and software used are first considered and will largely discuss the tested hypothesis of Secondary Question 1. The potential issues encountered during testing of the WFM system design and the evaluation of the WFM capability will then be discussed.

5.2.3.1 WFM hardware evaluation

The hardware evaluation will focus on a discussion of the hardware design and capabilities of the Forensic Server and wireless drone components of the WFM. The wireless drone component of the WFM has been extensively trialled throughout the research testing phases. The RouterStation Pro device, eventually used as the selected hardware platform for the wireless drone, proved to be very reliable. The Forensic Server also proved to be exceptionally reliable. The WFM was run constantly during each benchmark test which involved intense stress testing to determine the wireless network traffic acquisition capabilities. The outcome proved the hardware was stable. However, testing of the initial WFM revealed that the wireless drone could benefit from additional CPU power being made available. Therefore, the device was overclocked to 800MHz (from 680MHz) to attempt to increase the acquisition performance of the wireless drone component. The findings from Phase Three, that is performance testing of the stabilised WFM, showed that running either a single or dual wireless adapter at 3700PPS produced extremely high CPU usage, at approximately 99% and 100% respectively. Furthermore, the Kismet application turned out packet acquisition errors when the CPU was too overloaded to collect all network traffic. Such instances lead to incomplete data collection of the generated wireless network traffic. The findings indicated that a more powerful CPU could potentially increase the acquisition performance of the WFM.

Both the Forensic Server and wireless drone were equipped with Gigabyte Ethernet network adapters. The benefit of using Gigabyte Ethernet is the considerable increase in LAN speed achievable, of up to 1000Mbps, compared to older Ethernet technologies with a maximum speed of 100Mbps. Thereby, the use of Gigabyte Ethernet hardware devices increases the bandwidth between the Forensic Server and wireless drone. The addition of Gigabyte Ethernet was not necessarily needed for the testing system as the bandwidth of the existing WLAN (26.54Mbps) could easily be handled by 100Mbps Ethernet. However, if multiple wireless drones were used the additional capacity would be necessary due to the increased bandwidth of acquired network traffic being forwarded to the Forensic Server for preservation. Furthermore, if the newest 802.11n standard was used in the existing WLAN, Gigabyte Ethernet would be absolutely necessary due the dramatic increase in bandwidth of the existing WLAN and wireless network traffic acquired.

Assessment of the Forensic Server capabilities proved that the hardware used during the research testing phases was capable of preserving the forwarded wireless network traffic from the distributed wireless drones. If a large number of wireless drones were to be deployed, the Forensic Server would most likely need to have upgraded hardware to maintain the performance of the role to process and preserve wireless network traffic. Possible upgrades to improve performance may entail increasing the CPU and wired LAN performance of the Forensic Server.

5.2.3.2 WFM software evaluation

The main software used to implement the WFM included Kismet, OpenWRT and Ubuntu Linux. Furthermore, the Wireshark application was used for all analysis of Kismet packet capture log files.

In terms of acquisition of wireless network traffic Kismet performed well due to a variety of design features present in the application. Given that the acquisition and preservation of wireless network traffic was the main priority of data collection and a key point of the research question, the Kismet application succeeded at performing the intended role of the WFM system design. An advantage discovered in the Kismet application was the client server architecture of the application, allowing for different components of the application to be run on separate devices and communicate over wired network links. Furthermore, the Kismet application had the ability to be implemented to produce a wireless drone from readily available hardware devices.

However, there are also negative aspects of using Kismet as the wireless sniffer application of choice for the WFM. The reality is that Kismet is not specifically designed for digital forensic purposes and lacks certain principles needed for handling of data for later use as evidence. For example, the Kismet logging component is not designed to handle collected data based on forensic principles such as performing hashing on the Kismet packet capture log files. Another disadvantage of the Kismet application in terms of forensic limitations includes the inability to provide any details of potential packet loss. However, due to the open source development of Kismet and available source code, such additions could be added to the application based on recommendations made.

The capabilities of the Kismet IDS are very poor especially when compared to the claims of other available commercial wireless IDSs. During Phase Four of testing, all of the available intrusion alerts were configured to report an intrusion if a specific alert rule was raised. However, the only attack for which a Kismet IDS alert was triggered was the mdk3 beacon flood FakeAP attack, which triggered the 'APSPOOF' alert. The IDS capabilities were very disappointing and provided minimal weight as additional evidence to support the acquired wireless network traffic.

OpenWRT wireless router firmware was used as the operating system of choice for the wireless drone component of the WFM. The firmware proved to be an exceptionally reliable platform on the RouterStation Pro device which is designed specifically to be run on the OpenWRT firmware. During testing the wireless drone device did not suffer from system instability such as rebooting or stalling. Considering the stress of benchmark testing, the stability of the wireless drone device can be considered capable of constantly monitoring a WLAN if used in a real world environment. An advantage of the OpenWRT firmware is that it is constantly in development, with availability of the most current wireless drivers and ability to customise the firmware to the requirements needed for the specific design of the wireless drone. Furthermore, the current availability of the Kismet application from OpenWRT application repositories provides the ability of creating a wireless drone sufficiently easier than compiling the source code with the OpenWRT build environment.

Ubuntu Linux was the operating system of choice for the Forensic Server component of the WFM. Ubuntu also proved to be very reliable and stable to power the Forensic Server and maintain uptime to ensure processing and preservation of wireless network traffic forwarded from the wireless drones.

All of the analysis conducted on the collected network packet capture log files was performed using Wireshark and the variety of additional tools included with the application such as editcap, capinfo and mergecap. The forensic capabilities of the tools used have been reviewed when performing analysis of data during the testing phases. A range of Wireshark capabilities were used and tested during the analysis of the collected data. However, the reliability of these tools was not specifically tested during the research testing phases as it was not seen as a high priority of the research. Despite that, the tools were checked to ensure correct packet capture file manipulation. For example, when dividing the Kismet packet capture log file from the MGEN testing, each run of tests contained each of the 5 separate tests of 5 minute durations. The packet capture files were then split into 5 separate files using Wireshark's editcap tool, based on the timestamps of the frame from the original packet capture file. Each packet capture file was then subsequently analysed to ensure that the correct duration of the MGEN test was included in each split file. The editcap tool split the packet capture files without any errors, always containing the desired time duration used to split the packet capture file. Such capabilities show that the tools used worked well and without errors. However, to ensure forensic viability of altered data, specific independent testing would first need to be conducted on the tools used to ensure that robust evidence is produced.

5.2.3.3 WFM potential issues

The WFM is the key component of the research conducted and the evaluation of the system's ability to acquire and preserve wireless network traffic as a source of evidence is the focus of the main research question. During each phase of testing and later analysis of the data collected, various issues were encountered with the design of the WFM. Table 5.7 outlines the potential issues and possible solutions that were discovered with the implementation and operation of the WFM. Each issue will also be discussed in order to evaluate the possible solutions available.

Table 5.7: Potential Issues Discovered During Testing of the WFM.

Issue	**Suggested Solutions**
Amount of data acquired and subsequently preserved	Only collect frame header. Discard 802.11 data frame payload. Implement various filtering techniques.
Logging issues	Additional logging functionality to address forensic limitations of current system capabilities.
Multiple wireless drone effect	Implement Gigabyte Ethernet. Implement multiple Ethernet adapters on Forensic Server for large scale WLANs. Reduce data transmitted from wireless drone.
Data loss	AP and Wireless Drone placement. Improved hardware and software capabilities.
Costs	System costs versus potential risk and achieved benefits of implementation.

One important factor to consider regarding the WFM is the amount of data that has to be acquired and subsequently preserved. The initial testing of the existing WLAN infrastructure confirmed the bandwidth of the 802.11g network to be 26.5Mbps. If the WFM was implemented in a relatively busy WLAN, the issue of acquiring a full data set of network traffic could prove a difficult task in terms of the amount of data that then needs to be stored on the Forensic Server. For example, at the current bandwidth in the testing model, a total of approximately 95.4GB of network traffic was generated each hour. While such a scenario is unlikely in a real world environment it is theoretically still possible. Another example regarding the amount of data that is needed to be collected by the WFM was the Kismet log files obtained from benchmarking the WFM during initial and stabilised testing. The average amount of data collected by the WFM during the varying MGEN testing was 1.25GB at 3700PPS and 800MB at 2200PPS. The tests conducted at each rate were conducted 5 times for a total of 5 minutes, thus the results illustrate the amount of data collected over an approximate duration of 25 minutes. Even with the increasing size of hard drives and the reduction of price, such a large amount of data could potentially cause issues with preserving all wireless traffic. Furthermore, there also exist issues regarding the amount of data being sent from the wireless drones to the Forensic Server. As discussed, the amount of data needed to be preserved in the Forensic Server could potentially be very large. The data also needs to be transported from the wireless drone to the Forensic Server, thus, creating more network traffic on the wired Distributed System (DS) of the network. An increase in network traffic may cause potential issues due to the amount of bandwidth consumed by forwarding data from the wireless drone to Forensic Server. Moreover, if the original data collected by the WFM is intended for the wired portion of the network, twice as much data is needed to be transferred through the network. Since the WFM is designed to be integrated into an existing network, the issue of consuming additional available bandwidth is an important concern which would need be addressed in certain circumstances.

The potential issues discussed regarding the WFM and the amount of data acquired and transmitted identifies the problem of collecting a full data set of wireless network traffic. Also, it presents another issue of the necessity of acquiring a full data set for potential evidence. During the testing phases of the research no filters or other data reduction techniques were implemented in the WFM. Therefore, all wireless network traffic that could have been acquired by the WFM was collected. The possibility of performing data reduction is feasible using the available filters and other configuration options included in the Kismet application. Firstly, Kismet includes various filtering techniques that may either be excluded from the *tracker* function (frames not processed in anyway) or from the *export* function (frames which are excluded from the logging). The filters can be based on AP Basic Service Set Identifier (BSSID) and source or destination address. By using a data reduction technique network traffic, which is designated as not important to the WLAN being monitored, would be discarded therefore, reducing the data storage needed. However, due to the unique nature of the WFM, implementing such a technique could reduce the effectiveness of attack detection and associated acquisition and preservation of the evidence relating to the attack. For example, when filtering traffic based on AP BSSID all of the frames not relating to the specific BSSID will be discarded. In the scenario of a Fake AP attack, the evidence that would have been acquired by the WFM would have been filtered and discarded if a different BSSID value was used.

Another alternative to data reduction, aside to filtering and the possibility of data loss, would be to only collect the frame headers. Since the 802.11 data frame is potentially the largest (in terms of data size) because of the payload which it carries, the removal of the payload would result in less storage used for evidence preservation. Conveniently, there is now a *hidedata* option in Kismet that allows the truncation of all data frames that are collected by the Kismet server. If a data frame is processed by the Kismet server, the 802.11 data frame payload containing any encapsulated data is dropped except for the frames header. If the *hidedata* configuration was implemented the amount of data having to be preserved in the Forensic Server would be greatly reduced. Furthermore, using such a technique would also not prevent the detection of 802.11 specific attacks, which usually involve manipulation of the management or control frames. However, the described technique of data reduction does have one issue regarding the analysis and examination of higher level protocols carried by the data frame, although the technique of reconstructing higher level protocols to aid forensic investigation was beyond the scope of the research. However, previous studies have identified the possibility of using various methods to analyse network traffic to be used as potential evidence. If the *hidedata* methodology was used, the potential evidence gained from higher level protocols would be unavailable.

Although there are a number of potential issues regarding the amount of data storage required by the WFM there are possible solutions and the methods of filtering or stripping the data frame payload were discussed. Although both methods have potential weaknesses, either may be adopted in the right scenario to reduce the amount of data storage required. It should be noted however, that neither method will reduce the network traffic between the wireless drone and Forensic Server, as both methods are carried out by the Kismet server component on the Forensic Server.

A further potential issue with the implemented WFM was the limitations of the Kismet logging functionality. The issues became apparent due to the lack of control the user has over the logging functionality and when the digital forensic principles are not met. Firstly, the Kismet logs begin when the Kismet server application is started and close when the application is exited. Therefore, the Kismet logs are not able to be extracted until the Kismet server is exited, which produces issues since the WFM is designed to constantly monitor the WLAN. The suggested solution for the lack of logging functionality is to adapt the open source code of Kismet to add additional logging features, such as splitting log files into even timeslots, automatically hashing the created logs and starting a new set of log files.

Another previously outlined limitation of the research testing was that the use of multiple wireless drones was not to be included in testing due to the costs in additional hardware. It is theoretically possible that the addition of multiple drones may affect the performance of the WFM. Such issues may arise due to the increased bandwidth needed to transport data on the wired portion of the network from multiple wireless drones. In order to cater for the increased network traffic generated, Gigabyte Ethernet must be implemented into the wireless drone and Forensic Server. The Forensic Server hardware may also need to be upgraded to handle a large distribution of wireless drones, such as increasing the CPU power and addition of multiple Ethernet adapters. Another potential solution to manage the amount of data transported between the wireless drone and Forensic Server could be reducing the amount of data forwarded by the wireless drone, therefore, reducing the overall network traffic. Various methods have already been discussed, such as only collecting 802.11 frame header or discarding the data frame payload. However, Kismet currently performs the filtering and removal of the data frame payload via the Kismet server component, meaning that the wireless drone will still forward all wireless network traffic collected. If these techniques could be mimicked on the wireless drone, less bandwidth would be needed between the WFM components to transport the acquired data to the Forensic Server.

Data loss is another potential issue of the WFM system design. Specifically data loss issues are concerned with loss of wireless network traffic that potentially could have been acquired. Such data loss may occur due to radio frequency interference and the distance between wireless devices which affect collection of wireless network traffic by the WFM. Such issues may be solved by wireless drone placement and improved hardware and software capabilities. For example, placing the wireless drone in the immediate vicinity of the AP (1-2 metres) for which it is intended to monitor. Then, theoretically, if a client STA is able to communicate with the AP the wireless drone will also be able to monitor the wireless network traffic between the wireless devices. Improvement of hardware and software capabilities to improve evidence acquisition have previously been discussed, involving increasing CPU speed, LAN bandwidth available and improved software based collection capabilities.

Another potential issue of the WFM system design are the associated costs involved in implementing the proposed solution into an existing WLAN. Expenses include the initial cost of implementing the system with the necessary hardware devices and ongoing costs of maintaining and managing the WFM. The system design requires a wireless drone for each AP in a WLAN, as well as a dedicated computer for the Forensic Server component. The wireless drone component of the WFM cost approximately $NZ500 to implement, including the RouterStation Pro device, dual wireless adapters with omni-directional antennas and an indoor enclosure. Such a price may seem excessive, especially for a large WLAN with many APs. Furthermore, there are the overheads of specialised staff to implement and manage the system, as well as process and maintain the evidence collected. The costs outlined are additional to the WLAN infrastructure and in certain scenarios may not be required. However, the expense can be justified by evaluating the achieved benefits of implementation versus the system costs and potential risks without the WFM system.

5.3 RECOMMENDATIONS

The findings discovered from research testing (Chapter 4) and the preceding discussion sections has led to a growth of knowledge in the area of digital forensic procedures in WLANs. Specifically, the digital forensic process of acquisition, preservation and subsequent analysis of wireless network traffic was researched. The knowledge gained will now be drawn on to outline recommendations for WLAN and WFM benchmark testing. Furthermore, potential evidence available from wireless network traffic will be outlined as well as recommendations for best practices for acquisition and preservation of wireless network traffic.

5.3.1 WLAN & WFM Benchmarking Recommendations

A bonus from Phase One, was that the proposed, trialled and proven testing methodology to evaluate and benchmark the capabilities of the existing WLAN could later be used to implement the WFM. Furthermore, the benchmark testing also provided an assessment of the configuration of the existing WLAN to ensure optimal network capabilities were achieved. It was vital to establish a baseline level to assess the wireless network traffic acquisition capabilities of the WFM to ensure correct testing results. During the testing process a number of discoveries were made surrounding the proper implementation of benchmark testing for the proposed system design. Table 5.8 displays the following recommendations in order to achieve correct MGEN data generation capabilities when performing the packet rate capabilities of the existing WLAN.

Table 5.8: Recommendations to Ensure Correct Benchmarking Results.

Recommendations	Description
Use benchmark tool in client/server mode	In order to correctly generate network traffic between network devices, MGEN must be configured to send packets from the server to the client. If there is no client able to receive the generated packets, incorrect packet rates will be reported.
Implement logging functionality	Implementation of MGEN logging will provide detailed information of packets sent and/or received. However, when an AP is the MGEN server, correct logging might be unavailable due to the hardware capabilities of the device to process and record large log files.
Use specific functions to provide accurate data generation	To ensure accurate data generation, various specific MGEN script options should be used. For example, the ‘PRECISE’ option should be used in WLAN benchmark testing to ensure accurate real time packet generation.
Perform multiple tests to ensure consistent results	To ensure the data generation during benchmark testing is correct, multiple tests should be performed and the findings analysed to discover average baseline result in terms of WLAN capabilities.

5.3.2 Potential Evidence Obtained from Wireless Network Traffic

The research revealed that collecting wireless network traffic may aid in digital forensic investigations by providing detailed information that may be extracted from the collected data. One of the most important aspects of the collection of wireless network traffic is that the acquired and preserved data contains a complete record of all activity taking place on the network. However, this is only the case if a high percentage of the data transmitted on the WLAN is able to be acquired. Figure 5.1 displays the information that may be obtained from collected wireless network traffic taken from subsequent analysis of the packet capture log file produced.

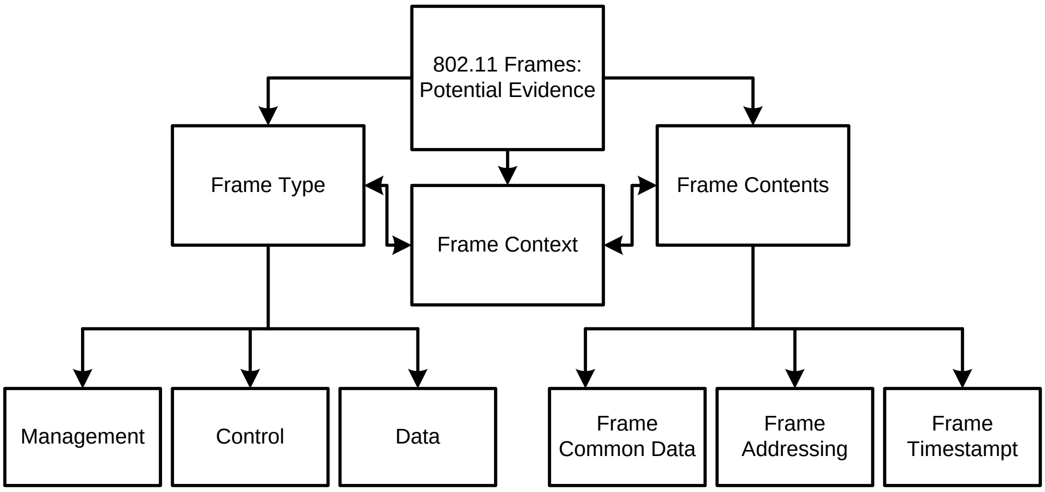

Figure 5.1: Potential Evidence from Wireless Network Traffic.

The potential evidence collected from wireless network traffic provides information extracted from the raw 802.11 frame itself. The 802.11 Medium Access Control (MAC) frame format (see Figure 2.3) contains a number of unique values which can be examined from the acquired wireless network traffic. Potential evidence is regarded as any information that may identify or aid in the digital investigation process being conducted. Various details important to digital forensic investigations in WLANs are available from wireless network traffic, based on the 802.11 frame type, the frame contents and the context of the frame within the flow of network traffic.

Wireless network traffic is comprised of various types of 802.11 frames, including management, control and data frames. Each specific frame type is used to accomplish defined responsibilities in an 802.11 WLAN. For example, a beacon frame (a subtype of management frame) is used to broadcast the availability of the wireless service being offered by the AP device while disassociation management frames are used to end the association of two wireless devices. Data frames are especially important as they contain higher level data, such as Transmission Control Protocol (TCP) or User Datagram

Protocol (UDP) network packets or application data which is being transported across the wireless network medium. Further analysis of encapsulated data would also provide additional evidence of worth. Each individual frame provides unique information regarding the activity occurring on a wireless network.

However, in order to understand the overall purpose of specific frame types and to reconstruct an event based on the collected data, the frames should be viewed in the original context. That is, in a logical progression based on frame acquisition time. For example, review of a single deauthentication frame means little unless examined in the flow of network traffic; however, an event can be rebuilt with surrounding information to provide details of network activity. If only a single deauthentication frame was discovered in the data analysis, it can be presumed that an authorised client disconnected legitimately from the WLAN. However, if a large number of deauthentication frames were discovered in the network traffic flow, it can be speculated that a DoS flood may have occurred.

A further point of potential evidence is the actual contents of the individual 802.11 frames, including common data, addressing and the frames timestamp. Common data includes miscellaneous information regarding the 802.11 frames origin and network configuration. For example, common data usually includes the channel of operation, network data rate, encryption type and signal strength. Furthermore, the frame sequence number may also be extracted from 802.11 frames. The identified common data may be used for a variety of reasons to aid as digital evidence, such as determining the distance from a device by signal strength, identify MAC address spoofing based on sequence number, and determining possible network security breaches due to lack of security.

Regarding the frame contents, all 802.11 frames contain a total of 4 address spaces; the two most common being the source and destination MAC address of the wireless devices. Such values can be considered as valuable as an Internet Protocol (IP) address in an Internet investigation, providing a unique electronic address of the person in question. The address values will provide evidence of the unique devices involvement when communicating on the WLAN.

The final outlined source of potential evidence from wireless network traffic is the timestamp provided with the 802.11 frame. Each frame has a timestamp based on the time the frame was acquired by the wireless network traffic acquisition tool. The timestamp can be used to provide an accurate time of when certain events occur based on examination of the collected data.

5.3.3 Wireless Network Traffic Acquisition and Preservation: Best Practices

From the experience gained from implementing and testing the WFM, as well as answering the research questions, a number of best practices were able to be formulated as recommended procedures for acquiring and preserving wireless network traffic as a source of viable digital evidence. The best practices displayed in Table 5.9 outline the various recommendations.

Table 5.9: Wireless Network Traffic Acquisition and Preservation: Best Practices.

Best Practice	**Procedure**
Use libpcap library	When capturing wireless network traffic, use libpcap library for acquiring and preserving 802.11 frames.
Wireless Drone positioning	Place the wireless drone in the immediate area of the AP being monitored, approximately 1-2 metre radius.
Use tested software and hardware configurations	Tested software and hardware configurations should be used, or conduct testing to ensure viable digital evidence is collected. For example, the use of stable wireless drivers and sniffer applications.
Perform benchmarking tests	Benchmark testing at each phase of implementation to progressively evaluate the capabilities of the WLAN and WFM.
Maintain digital forensic soundness of collected data.	Use hashing methods (such as MD5) to preserve the integrity of the collected evidence. Maintain duplicate copies of collected data. Store collected data in a write protected storage device to ensure no modifications are made to the data files.

The first recommendation outlines the use of the libpcap library for capturing wireless network traffic. Libpcap provides a system with the ability to perform packet capture and saves the data collected to a special file type which can later be examined using supported applications. Libpcap is currently the most advanced and updated packet capture library available as well as the most supported application library for performing network traffic capture. For those reasons, best practices dictate the use of libpcap for acquisition and preservation of wireless network traffic. In a situation where libpcap cannot be used, such as Microsoft Windows OS, it is recommended to use a libpcap alternative, in this case WinPCap.

The positioning of the wireless drone, or any type of wireless sniffer system, is exceptionally important to the performance of wireless network traffic acquisition.

Similar to the techniques used when implementing normal wireless devices, special attention must be given to physically place the device to provide the best range, signal strength as well as reduce potential Radio Frequency (RF) interference. Since the wireless drone is designed to monitor one specific AP, it should be placed in the immediate area of the AP destined to be monitored. Theoretically, if the wireless drone is close enough to the AP and if the AP and client STAs are able to communicate effectively, then a large proportion of network traffic should be collected. Nevertheless, if the wireless drone is too close to the AP there may be an issue with malformed of corrupted frames being collected. That being so, best practices outline that the wireless drone should be positioned in a radius of 1-2 metres from the AP being monitored and also tested for performance once placed in the desired drone location.

Another important aspect of wireless network traffic acquisition is the software and hardware configurations used. As there are no specific applications or procedures currently available to obtain viable digital evidence from wireless network traffic, special attention must be given to the software and hardware configurations used for data collection. In terms of software requirements, the wireless driver used by the wireless adapter and the functionality it provides is exceptionally important. The wireless drivers used during research testing illustrate the significance of stability and reliability which the wireless drivers provide. To obtain viable wireless network traffic, wireless drivers must function correctly in Radio Frequency Monitor (RFMON) mode, allowing for the acquisition of 802.11 frames destined for any wireless device. The findings illustrated problems with the ath9k wireless driver and the Mikrotik R52N wireless adapter which collected corrupt 802.11 beacon frames (see Figure 4.1), raising issues when using the data as digital evidence. In addition, wireless sniffer software must also be tested to establish the capabilities and reliability of collected wireless network traffic when used for digital forensic investigation purposes. In terms of hardware configuration, the use of stable hardware devices which is well supported by the desired software is recommended as a best practice. In summary, the software and hardware configurations must be judiciously made and rigorously tested to provide assurance that the potential data gathered is viable and can be used as digital evidence.

Since the WFM is designed to monitor a specific WLAN implementation, benchmark testing is essential to identify the capabilities of the system design and implementation. Since a WLAN infrastructure may vary greatly due to configuration or devices used, WLANs should be benchmarked to establish capabilities such as maximum PPS rates. Subsequent testing of the WFM system design is also vital to establish the capabilities of wireless network traffic acquisition from a digital forensic viewpoint.

A further best practice procedure that should be applied so that forensic soundness of the collected data can be maintained, is the use of cryptographic hashing functions which can be used to calculate a unique hash value of a specific file. The use of hashing can be used on the collected data, such as packet capture log files, to preserve the integrity of that data. If the file is manipulated in any way which modifies the file contents, the hash value will change indicating that the file has not maintained forensic integrity. Duplicate records of collected data should also be maintained to provide a back up copy of the digital evidence. In addition, storing the collected data on a read-only storage medium also provides assurance that the collected data cannot be modified. For example, currently there are no network applications specifically designed for forensic analysis of wireless network traffic, therefore other alternatives have to be used. However, performing analysis with such tools may alter the collected data which may then create potential issues of forensic soundness. If the collected data is stored and analysed in a read-only medium, the chance of modification to the data is removed.

5.4 CONCLUSION

Chapter 5 has developed a discussion of the findings from the research testing which was reported, analysed and presented in Chapter 4. The research questions proposed in the research methodology (Section 3.2) have been answered and discussed in terms of the previously asserted hypotheses, and a conclusion reached regarding the validity of the predicted hypotheses. The findings achieved during the various testing phases were discussed and the WFM evaluated based on the system capabilities, hardware and software configuration, and the potential issues that may hinder the performance of the system design.

The main research question of the project was centred on the capabilities of a design system to acquire and preserve wireless network traffic to provide evidentiary trails from WLANs. Subsequently, a research model was formed (Section 3.3) and a system design prescribed. During research testing the WFM was implemented and benchmarked, a stabilised design was formed, and attacks were recreated to determine the systems capabilities. The findings discovered that the WFM was able to be implemented with readily available hardware and software and able to acquire a very high percentage of wireless network traffic at the maximum transmission rate of the existing WLAN infrastructure. Furthermore, evidentiary trails were able to be achieved from the recreated attacks, proving the WFM was indeed capable of the fulfilling the intended tasks. The body of knowledge gained was finally used to provide recommendations and best practices to help aid in advancing digital forensic procedures in WLANs.

Chapter 6 concludes the thesis project and presents a summary of the research conducted and the significant results that have been discovered. Limitations to the research will be outlined to determine specific areas of research that were hindered in some form. In closing, other prospective fields of research within the discipline area will be discussed to highlight the many potential avenues open to future research.

Chapter Six

CONCLUSION

6.0 CONCLUSION

Chapter Six presents the final conclusion of the thesis and the research conducted. Therefore, a summary of the research findings (Chapter 4), and subsequent review of the discussion of the findings (Chapter 5) is made. The chapter then concludes giving a synopsis of the limitations of the conducted research but also identifies exciting avenues for potential future research within the chosen topic area.

The IEEE 802.11 standard for Wireless Local Area Networking (WLAN) was chosen as the wireless networking technology to be investigated. The popularity and current wide use of wireless devices is unprecedented; however, this also co-occurs with the trend of increasingly widespread illegal practices involving computer crime. The very nature of the technology medium gives rise to potential security issues and misuse. Due to current problems of insufficient guidelines and procedures surrounding the process of digital forensics in wireless networks, the chosen field of research focussed on the acquisition and preservation of wireless network traffic to aid in the process of digital forensic investigations of wireless networks.

Subsequent to a critical review of academic literature, and the analysis of similar research studies, a main research question was formed to provide a research goal. The aim was to design a system model capable of acquiring and preserving the wireless network traffic communicated between devices in a WLAN. The system design involved implementation of a Wireless Forensic Model (WFM), using wireless drones to intercept network traffic from a WLAN, and subsequent storage of the collected data maintained on a Forensic Server. The overall findings showed that the proposed system design was capable of acquiring and preserving wireless network traffic to provide evidentiary trails and that the information may aid in digital forensic investigations involving WLANs. Furthermore, the WFM system architecture was designed to adhere to key digital forensic principles and was proved capable of maintaining the integrity of the acquired evidence.

Chapter 4 reported the findings from the proposed research phases. The findings were then analysed and subsequently presented. The phases involved initial and then stabilised testing and will be briefly discussed in order to conclude the results that were discovered. Initial testing was undertaken in order to assess preliminary results and any early problems encountered so that the groundwork to develop a stabilised design was researched. Initial testing included Phases One and Two of the research model. Phase One involved implementing the existing WLAN infrastructure, comprised of an Access Point (AP) and a client Station (STA). The existing WLAN was then benchmarked to evaluate performance factors. Bandwidth testing found that the WLAN was capable of an average throughput result of 26.54Mbps. Packet per second (PPS) testing discovered the existing WLAN was able to maintain approximately 3700PPS. Both findings are in correlation with previous testing where the 802.11g standard was used with network encryption implemented. The findings showed that the existing WLAN was operating correctly and provided baseline levels of performance to use in the later testing phases.

Phase Two then specified the implementation of the WFM based on the proposed components and configurations. The Forensic Server and wireless drone components were installed and configured, and benchmarking was conducted using two separate wireless drone configurations. The findings and analysis of the benchmarking results discovered that the WFM was capable of acquiring and preserving wireless network traffic. Acquisition percentages varied between the two configurations. However, at the maximum PPS rate the existing WLAN could sustain (3700PPS) a large proportion of the generated traffic, with approximately 98% and 95% of wireless network traffic acquired. The initial WFM benchmarking tests show that even from an initial system implementation, the proposed system design proved to be clearly capable of providing digital evidence from the acquired and preserved wireless network traffic even though a few problems with the system design were encountered. An example was wireless driver instability, identifying problems with the initial WFM implementation.

Stabilised testing was then conducted, comprised of research Phases Three and Four. Phase Three required using the knowledge gained from initial testing and implementing a stabilised WFM, which was again benchmarked to evaluate the final system design capabilities. Findings discovered that the stabilised WFM was capable of acquiring a large proportion of wireless network traffic. At 3700PPS approximately 90% of all generated network traffic was acquired and preserved successfully. Although the results achieved were slightly lower than initial benchmark testing, the overall performance and reliability of the WFM components was greatly increased, producing a stable system design. Performance testing was also conducted in which the findings demonstrated the importance of Central Processor Unit (CPU) power and wired network links between the WFM components. The findings, again, illustrate the WFM was clearly capable of acquiring and preserving wireless network traffic for the potential use as digital evidence. Furthermore, the findings from Phases Two and Three reinforce that digital forensic principles are able to be maintained, thus producing viable digital evidence.

The final stage of testing, Phase Four, involved recreating attacks against the monitored WLAN to evaluate the WFM capabilities to provide evidentiary trails of a specific event. A total of 2 Denial of Service (DoS) and 2 Fake Access Point (FakeAP) attacks were recreated. The WFM proved to be capable of acquiring a high percentage (approximately 99%) of the frames that were injected by the attacker during both of the DoS attacks. It was additionally noted that both DoS attacks caused loss of communication between the wireless devices in the WLAN. With respect to the FakeAP attacks, the WFM was also capable of acquiring the frames injected by the attacker. A unique aspect of the wireless drone component was the addition of multiple wireless adapters. The design allowed non-stop monitoring of the existing WLAN, by sniffing all traffic on the designated channel, while also hopping between other available channels in an attempt to acquire additional digital evidence. However, the findings of the recreated FakeAP attacks conducted on a random channel discovered minimal additional evidence (approximately 23% of the total frames acquired), and also affected the performance of the WFM due to additional CPU usage by the wireless drone.

The findings from Phase Four illustrated that the WFM was capable of acquiring evidentiary trails from attacks conducted against the WLAN. The collected evidence was also able to provide detailed information regarding the attack event that occurred and potential information linking the attack to a specific device. However, there are still some concerns surrounding the acquired digital evidence. The ease of Media Access Control (MAC) address spoofing proved to affect the ability to link the evidence to an attacker based on the unique address. Results also indicate that the additional evidence provided by the wireless Intrusion Detection System (IDS) component of the WFM was minimal, only detecting one of the four recreated attacks. Nevertheless, it was also discovered that the addition of an intrusion alert can greatly assist forensic investigation during the analysis of acquired evidence by providing a timestamp of the detected attack, allowing location of potential evidence in the acquired wireless network traffic.

To sum up, each phase of testing provided findings to aid in answering the main research question and the associated hypothesis. The findings discovered that the WFM system design was able to be implemented using various 802.11 wireless devices and readily available open source software. It was also concluded that digital evidentiary trails were able to be obtained by acquiring and preserving wireless network traffic. However, there are still a number of potential issues regarding the WFM system design including attack detection capabilities, data loss and the effect of monitoring a large WLAN with numerous APs. Therefore, in answer to the main research question, the WFM design system is capable of acquiring and preserving wireless network traffic to provide evidentiary trails from 802.11 WLANs but still requires future research and improvements to address the discovered shortcomings. Finally, the knowledge gained was used to outline recommendations to promote techniques for conducting digital forensic processes in WLANs. Recommendations include benchmark testing best practices; possible information that is able to be extracted from wireless network traffic and guidelines for ensuring wireless network traffic is collected efficiently and in compliance with digital forensic principles.

6.1 LIMITATIONS OF RESEARCH

The earlier identified limitations of the research methodology (Section 3.5) were outlined at the pre-testing stage of the proposed research, based on the defined research model and projected system design. Those limitations that continue to be important after conducting the testing phases will be briefly reiterated. Then, limitations identified from the research findings and subsequent research discussion presented in Chapter 4 and 5 will be discussed.

A number of previously discussed limitations (Section 3.5) are still apparent, and remain a factor to the research conducted and findings achieved. Firstly, only the 802.11g mode of operation was tested: the four main WLAN standards operate quite differently, such as network bandwidth capabilities and the radio frequency used, which in turn may affect the requirements, capabilities and performance of the WFM system design. Also the existing WLAN was to be only tested using a single configuration, including network encryption type, number of APs and client STAs. Thus, any changes made to the existing WLAN configuration may also affect the WFM design and findings obtained. Another foreseen limitation was that only one wireless drone was to be implemented in the WFM, while being aware that multiple drones may affect the system’s capabilities. Finally, the analysis of higher network protocol, which 802.11 frames transport, was also not conducted during the testing phases, again limiting the outcome of achieved findings.

The process of implementing the WFM system design, performing various testing phases and analysing and discussing the findings has revealed a number of other limitations. Firstly, the project theme centered on the acquisition and preservation of wireless network traffic as a source of digital evidence to provide evidentiary trails. In addition, the sources of evidence, apart from the preserved wireless packet capture, included a database of discovered devices and IDS alert log, both of which were derived from the acquired wireless network traffic; meaning that all of the gathered evidence was based on the acquired network traffic which was processed by the Kismet server application. Therefore, the system design is limited to providing only a single source of evidence.

Another limitation is that testing was not conducted on the ability to perform digital forensic investigation on the components of the existing WLAN, nor the attacker's computer, both of which could potentially provide additional sources of digital evidence. For example, the forensic acquisition and subsequent analysis of the attacker's computer may have identified possible locations of wireless artefacts on a Linux based Operating System (OS).

There were also limitations as a result of the software used during testing, as well as the non-use of expensive commercial systems. Firstly, only open source software, such as Kismet, was used. The writer feels that the major downside of the achieved findings were those presented in the IDS capabilities results. It was envisioned that the intrusion alerts would provide a prominent source of digital evidence for the forensic investigator to identify the attack and subsequently analyse the acquired wireless network traffic capture for further information. However, as Kismet is not specifically an IDS, minimal intrusion alert rules are available; not all attacks were detected, even when a rule is defined and it would appear that development is focussed on other functions that the application provides. Commercial IDSs, such as AirMagnet, proclaim advanced IDS features which can detect numerous wireless attacks.

Another software limitation was the lack of development that could have been made to the open source tools used. Since the source code of all tools used (Kismet, OpenWRT and Wireshark) are released under various GNU General Public Licences (GPL), the source code is available for modification provided that certain licence specifications are met. The Kismet application, in particular, could have benefited from the addition of digital forensic functionality. However, no additions were attempted due to the defined scope of the conducted research and it not being a part of the project brief.

6.2 FUTURE RESEARCH

The research conducted during the project has provided additional insight to the chosen topic area of the process of digital forensics in WLANs. The project also highlighted a number of aspects for further research to performing digital forensic investigation in WLAN environments.

A major area to target for future study relates to viability of wireless network traffic, or for that matter even normal wired based network traffic, as a source of digital evidence. The viability of the evidence that can be collected and how that data is acquired needs to be investigated to a greater extent. For example, is the method of acquiring wireless network traffic forensically sound, and if not, what measures can be implemented to ensure that traditional forensic principles are maintained to produce viable evidence that may be relied upon in a court of law?

One exceptionally important area of much needed groundwork is the advancement in specialised forensic tools for acquisition, preservation and analysis of wireless network traffic to produce viable and trusted digital evidence. Additionally, future research could focus on the development of currently available applications, especially the two main tools used during research testing: Kismet and Wireshark. Due to the unique requirements of digital forensics, additional development of tools could provide benefits to the viability of the digital evidence collected. For example, if Wireshark was provided with additional forensic capabilities such as recording a log of all the actions an investigator makes when analysing collected data. Ongoing work is necessary to identify all of the required additions to the currently used tools which are not specifically designed or intended for present-day digital forensic use. Another example is the Kismet application which was used as the backbone of the WFM design. Although Kismet is not designed for forensic use, it does work very well at acquiring and preserving wireless network traffic, as discovered by the WFM capabilities testing. Further research could identify and implement additional functionality, thus creating a dedicated forensic wireless sniffing application. The development could improve wireless network traffic acquisition and preservation by implementation of features such as automatic log file hashing, enhancing the forensic soundness of collected data.

A further area of development that could benefit, would be the investigation of performing the digital forensic process on the various existing WLAN components, such as the AP and client STA devices, or the attacker’s computer. The digital forensic process used could be based on traditional computer forensic principles, by conducting the four phases of digital forensics on the volatile and non-volatile storage of devices under investigation. Additional investigation is needed as most scenarios will require specialised knowledge and techniques to extract and analyse the data. Although some points of future research areas proposed have been previously investigated, such as wireless artefacts stored on Windows OS, there are still a large number of salient questions which need to be addressed. For example, can wireless artefacts be extracted from a Linux based OS, how can data be extracted and analysed from an AP, and what additional evidence could potentially be acquired from digital investigation of the WLAN devices or the attacker’s computer?

Another proposed area for future research, similar to performing the digital forensic process on wireless devices, would be the development of a ‘Forensic Friendly’ wireless router; essentially the AP device with additional functionality specifically to aid digital forensic investigations. Development could consist of an AP operating on the wireless router which allows ease of extraction of digital evidence, such as the flash memory which contains the OS of the device. For example, if the wireless router had the software capable of forensically imaging the device’s flash memory (where the firmware resides) to an external storage device. Such a technique could be easily achieved using a wireless router with a Universal Serial Bus (USB) slot, and running OpenWRT firmware which allows use of the ‘dd’ command to take a disk image of the device’s flash memory. The proposed technique could provide a method of acquiring the forensic image of the OS of the wireless router with little interaction with the device itself, therefore, potentially maintaining forensic soundness. Additionally, due to being open source, customisation of the OpenWRT firmware could potentially provide additional logging functionality which may also benefit digital forensic investigations. For example, if the AP device was capable of collecting detailed logs of client STA connections with time duration and MAC address values. Another inclusion could be the development of application software to run on OpenWRT firmware to provide additional forensic tools or capabilities.

The legality of acquiring wireless network traffic is a further area needing to be addressed by applied research. The findings showed that various evidentiary trails are able to be collected from the acquired network traffic. However, there still exists potential legal issues regarding capturing the network traffic between devices. For example, due to privacy or surveillance laws governing the area of implementation. Specific research needs to be conducted to assess the potential legal issues surrounding wireless network traffic acquisition, and solutions outlined to ensure that laws are not broken when performing digital forensic investigations from wireless network traffic. For example, is there a difference between acquiring different types of 802.11 frames? If data frames are not collected, which contain predominately user related information, does this affect the legality of wireless network traffic collection? Furthermore, could the acquisition of wireless network traffic be defined in an organisation’s network usage policy to allow the collection of potentially private data?

Altering the system design of the WFM also has exciting potential for ongoing development design. The system design implemented for the project was based on an 802.11 infrastructure system architecture which involves placement of wireless drones to monitor each static AP in the WLAN. However, not all WLANs are based on the infrastructure architecture. Furthermore, not all forensic investigation scenarios require a complete WLAN forensic system. An example is when a forensic investigation requires monitoring of a single AP in a WLAN, during a certain one-time situation or in an environment with highly mobile devices or an ad-hoc network infrastructure. In such scenarios, a potential solution could be a mobile system design based on the WFM implemented during the research testing. For example, the use of a laptop computer and an appropriate wireless adapter which can act as the wireless drone and Forensic Server components of the WFM. There are a number of advantages of the proposed mobile system. Better performance is likely to be expected due to the higher powered hardware provided by the laptop computer. Moreover, implementation of a mobile system can be easier due to the software configuration used in the WFM being designed for a normal Personal Computer (PC) system architecture. However, a mobile system would most likely be used in different locations and to monitor different WLANs. Therefore, the Kismet application would need specific configuration before performing data acquisition. The Kismet application could still be used in such a scenario to perform a quick scan to discover wireless networks, then take the obtained information and configure Kismet for the appropriate network or scenario. Implementation of such a system would require further monitored testing to fully evaluate the actual and potential capabilities of such a system design.

It has thus been shown that many future prospects could be taken up and developed further. The opportunities and potential projects in the accelerating realm of wireless networking technology are endless. Nor will criminal misuse diminish. The era for digital forensic vigilance is upon us.

REFERENCES

ACPO. (n.d.). The Association of Chief Police Officers': Good Practice Guide for Computer-Based Electronic Evidence. http://www.7safe.com/electronic_evidence/index.html#

aircrack-ng. (2010). Retrieved March 20, 2010 from http://aircrack-ng.org/doku.php?id=aircrack-ng

airdecap-ng. (2010). Retrieved March 20, 2010 from http://aircrack-ng.org/doku.php?id=airdecap-ng

airodump-ng. (2010). Retrieved March 20, 2010 from http://aircrack-ng.org/doku.php?id=airodump-ng

Axelsson, S. (2000). Intrusion Detection Systems: A Survey and Taxonomy. Technical Report 99-15, Department of Computer Engineering, Chalmer University Technology, Sweden.

Beck, M. & Tews, E. (2008). Practical Attacks Against WEP and WPA. *Proceedings of the 2nd ACM Conference on Wireless Network Security*. Zurich, Switzerland.

Berghel, H. & Uecker, J. (2004a). Wireless Infidelity I: War Driving. *Communication of the ACM*. *47*(9). 21-26.

Berghel, H. & Uecker, J. (2004b). Wireless Infidelity II: Airjacking. *Communication of the ACM*. *47*(12). 15-20.

Bittau, A. (2005). The Fragmentation Attack in Practice. Retrieved March 27, 2010 from http://www.offensive-security.com/wifu/Fragmentation-Attack-in-Practice.pdf

Bittau, A., Handley, M. & Lackey, J. (2006). The Final Nail in WEP's Coffin. *Proceedings of the 2006 IEEE Symposium on Security and Privacy*. 286-400. Washington DC, USA.

Brown, C.L.T. (2006). *Computer Evidence – Collection and Preservation*. Boston, MA: Course Technology.

CACE Technologies. (2010). CACE Technologies - AirPcap. Retrieved March 7, 2010, from http://www.cacetech.com/products/airpcap.html

Carrier, B.D. (2006). Risks of Live Digital Forensic Analysis. *Communications of the ACM. 49*(2). 56-61.

Carvey, H. (2005). The Windows Registry as a Forensic Resource. *Digital Investigation. 2*(1). 201-205.

Cam-Winget, N., Housley, R., Wagner, D. & Walker, J. (2003). Security Flaws in 802.11 Data Link Protocols. *Communications of the ACM. 46*(5). 35-39.

Casey, E. (2004). Network Traffic as a Source of Evidence: Tools Strengths, Weaknesses, and Future Needs. *Digital Investigation. 1*. 28-43.

Chen, G., Yao, H. & Wang, Z. (2010). An Intelligent WLAN Intrusion Prevention System Based on Signature and Plan Recognition. *2010 Second International Conference on Future Networks*. 168-172.

Corey, V., Peterman, C., Shearin, S., Greenberg, M.S., Van Bokkelen, J. (2002). Network Forensic Analysis. IEEE Internet Computing. *6*(6). 60-66.

Crow, B.P., Widjaja, I., Kim, J.G. & Sakai, P.T. (1997). IEEE 802.11 Wireless Local Area Network. *IEEE Communications Magazine*. September, 1997. 116-126.

CSI/FBI Computer Crime and Security Survey. (2002). *Computer Security Institute*.

Fluhrer, S., Mantin, I. & Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. Lecture Notes in Computer Science: Selected Issues in Cryptography. *2259*(2001). 1-24.

Fluke Corporation. (2010). Airmagnet – Enterprise Wireless Network Security and Troubleshooting. Retrieved March 15, 2010 from http://www.airmagnet.com/

Frankel, S., Eydt, B., Owens, L. & Scarfone, K. (2007). Special Publication 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i – Recommendations of the National Institute of Standards and Technology. Gaithersburg, Maryland.

Gregor, S. (2002). Design Theory in Information Systems. *Australian Journal of Information Systems*. Special Issue. 14-22.

Hoeper, K. & Chen, L. (2009). Special Publication 800-120: Recomendation for EAP Methods Used in Wireless Network Access Authentication. Gaithersburg, Maryland.

Housley, R. & Arbaugh, R. (2003). Security Problems in 802.11-Based Networks. *Communications of the ACM. 46*(5). 31-34.

IEEE Std. 802.11. (1997). 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. NY, USA.

IEEE Std. 802.11. (1999). 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. NY, USA.

IEEE Std. 802.11i. (2004). 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 - Amendment 6: Medium Access Control (MAC) Security Enhancements. NY, USA.

IEEE Std. 802.11. (2007). 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. NY, USA.

IEEE Std. 802.11n. (2009). 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 - Amendment 5: Enhancements for Higher Throughput. NY, USA.

ISO/IEC 27002 Standard. (2006). Information Technology – Security Techniques – Code of Practice for Information Security Management.

ISO/IEC 27037 Standard WD. (2009). Information Technology – Security Techniques – Guidelines for Identification, Collection and/or Acquisition and Preservation of Digital Evidence (N7570).

ITU. (1991). Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications - Recommendation X.800.

Kahai, P., Srinivasan, M. & Pendse, R. (2005). Forensic Profiling System. *International Federation for Information Processing. 194*(2005). 153-164.

Karygiannis, T. & Owens, L. (2002). Special Publication 800-48: Wireless Network Security – 802.11, Bluetooth and Handheld Devices. Gaithersburg, Maryland.

Kent, K., Chevalier, S., Grance, T. & Dang, H. (2006). Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response – Recommendations of the National Institute of Standards and Technology. Gaithersburg, Maryland.

Kershaw, M. (2009). Get Thinking About Wireless Security. Paper presented at Sharkfest, 2009. Stanford University, California.

Kershaw, M. (2010). Kismet ReadMe. Available online or with application http://www.kismetwireless.net/documentation.shtml#readme

KisMAC. (n.d.). kismac-ng. Retrieved March 15, 2010 from http://trac.kismac-ng.org/

Kothari, C.R. (2004). *Research Methodology: Methods and Techniques*. Delhi, India: New Age International Ltd.

Kremmerer, R.A. & Vigna, G. (2002). Intrusion Detection: A Brief History and Overview. *Computer. 35*(4). 27-30.

Lim, Y.X., Schmoyer, T., Levine, J. & Owen, H.L. (2003). Wireless Intrusion Detection and Response. *Proceedings of the 2003 IEEE Workshop on Information Assurance.* West Point, NY.

Lockhart, A. (2005). Snort Wireless. Retrieved April 17, 2010 from http://web.archive.org/web/20080316065137/http://snort-wireless.org/

McKemmish, R., (1999). What is Forensic Computing. Australian Institute of Criminology- Trends and Issues in Crime and Criminal Justice – Instructional Material.

Meghanathan, N., Allam, S.R., Moore, L.A. (2009). Tools and Techniques for Network Forensics. International Journal of Network Security and its Applications. *1*(1). 14-25.

MetaGeek. (2010). inSSIDer Wi-Fi Scanner | MetaGeek. Retrieved March 7, 2010, from http://www.metageek.net/products/inssider

Milner, M. (2004). NetStumbler Readme. Retrieved March 7, 2010, from http://www.stumbler.net/readme/readme_0_4_0.html

Milner, M. (2010). Stumbler dot net. Retrieved March 7, 2010, from http://www.stumbler.net/

Motorola. (2010). Motorola AirDefense Solutions – Enterprise Wireless Security & Compliance, Infrastructure Management & Network Assurance. Retrieved March 18, 2010 from http://airdefense.net/index.php

Murray, J. (2009). An Inexpensive Wireless IDS Using Kismet and OpenWRT. *SANS Institute.*

Ngobeni, S. J. & & Venter, H.S. (2009). Design of a Wireless Forensic Readiness Model. *Information Security South Africa (ISSA2009) Conference.* Johannesburg, South Africa.

Nikkel, B.J. (2005). Generalizing Sources of Live Network Evidence. *Digital Investigation*. *2*(3). 193-200.

Nikkel, B.J. (2006). Improving Evidence Acquisition from Live Network Sources. *Digital Investigation. 3*(2). 89-96.

NIJ. (2004). National Institute of Justice: Special Report – Forensic Examination of Digital Evidence: A Guide for Law Enforcement. Washington, DC.

NIJ. (2007a). National Institute of Justice: Special Report – Investigations Involving the Internet and Computer Networks. Washington, DC.

NIJ. (2007b). National Institute of Justice: Special Report – Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. Washington, DC.

NIJ. (2008). National Institute of Justice: Special Report – Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. Washington, DC.

Oxford Dictionary of English 2e, (electronic), (2003).

Reddy, P., Sharma,H & Paulraj, D. (2008). Multi Channel Wi-Fi Sniffer. *4th International Conference on Wireless Communications, Networking and Mobile Computing.* Dalian, China.

Reith, M., Carr, C. & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence. 1*(3). 1-12.

Richardson, R. (2008). CSI Computer Crime & Security Survey. *Computer Security Institute*.

Rogers, M. K. & Seigfried, K. (2004). The Future of Computer Forensics: A Needs Analysis Survey. *Computers & Security. 23*(1). 12-16.

Scarfone, K., Dicoi, D., Sexton, M. & Tibbs, C. (2008). Special Publication 800-48 (Revision 1): Guide to Securing Legacy IEEE 802.11 Wireless Networks – Recommendations of the National Institute of Standards and Technology. Gaithersburg, Maryland.

Scarfone, K. & Mell, P. (2007). Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS) – Recommendations of the National Institute of Standards and Technology. Gaithersburg, Maryland.

Shirley, R. (2000). Internet Security Glossary. Available online from http://www.ietf.org/rfc/rfc2828.txt

Simon, H.A. (1981). The Sciences of the Artefact (2nd Ed.) Cambridge: MIT Press.

Slay, J. & Turnbull, B. (2005). The 802.11 Technology Gap: Case Studies in Crime. *Tencon – 2005, IEEE Region 10 Conference.* Melbourne, Australia.

Slay, J. & Turnbull, B. (2006). The Need for a Technical Approach to Digital Forensic Evidence Collection for Wireless Technology. *Proceedings of the 2006 IEEE Workshop on Information Assurance*. Westpoint, NY.

Sommer, P. (1999). Intrusion Detection Systems as Evidence. *Computer Networks. 31*(23-24). 2477-2487.

Standards Australia. (2003). Guidelines for the Management of IT Evidence - Handbook 171-2003. Sydney, Australia.

SWGDE. (2006). Scientific Working Group on Digital Evidence: Best Practices for Computer Forensics – Version 2.1.

Turnbull, B. & Slay, J. (2007). Wireless Forensic Analysis Tools for use in the Electric Evidence Collection Process. *Proceedings of the 40th Hawaii International Conference on System Sciences*. *9*. 4502-4511.

Turnbull, B. & Slay, J. (2008). Wi-Fi Network Signals as a Source of Digital Evidence: Wireless Network Forensics. The Third International Conference on Availability, Reliability and Security. 3. 1355-1360.

Van Aken, J. (2004). Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-tested and Grounded Technological Rules. *Journal of Management Studies*. *41*(2). 219-246.

Varshney, U. (2003). The Status and Future of 802.11-Based WLAN's. *IEEE Computer*. *36*(6). 102-105.

Vladimirov, A.A., Gavrilrnko, K.V. & Mikhailovsky, A.A. (2004). Wi-Foo – The Secrets of Wireless Hacking. Boston, MA: Pearson Education, Inc.

Yang, H., Xie, L. and Sun, J. (2004). Intrusion Detection Solution to WLANs. *IEEE 6th CAS Symposium on Engineering Technologies: Mobile and Wireless Communication.* Shanghai, China.

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.* Paper presented at the 2008 International Conference on Information Science and Security. Seoul, Korea.

Wi-Fi Alliance. (2009). Wi-Fi Alliance. Retrieved March 15, 2010 from http://www.wi-fi.org/.

APPENDICES

APPENDIX A:

Initial Testing: Phase One

Existing WLAN Specifications: Wireless Access Point Hardware Specifications.

Model	TP-Link TL-WR1043ND (version 1.4)
Wireless Chipset	Atheros 9100
CPU Speed	400MHz
Flash Memory	8MB
RAM Memory	32MB
Supported 802.11 Standards	802.11b, g and n
MAC Address	00:27:19:FE:40:88
Ethernet	4 x Gigabyte Ethernet ports
Notes: Device also contains an external USB 2.0 slot.	

Existing WLAN Specifications: Wireless Access Point Software Specifications.

Firmware	OpenWRT Kamikaze Bleeding Edge Trunk Development Branch (revision 22321)
Linux Kernel	2.6.32.16
Wireless Drivers	mac80211 ath9k (version 2010-07-16-1)
Benchmarking Tools	MGEN (version 5.01b)
	iPerf (version 2.0.5-1)
NTP Software	ntpclient (version 2007_365-4)
SSID	tplink1043ap

Existing WLAN Specifications: Client STA Hardware Specifications.

Model	Apple MacBook 5,2
CPU	Intel Core 2 Duo 2GHz
Memory	2 GB DDR2 SD RAM
Wireless Chipset	AirPort Extreme, Broadcom BCM43xx
MAC Address	00:24:36:B5:0C:A7

Existing WLAN Specifications: Client STA Software Specifications.

Operating System	Mac OS X 10.5.8
Darwin Ports	Kernel version 9.8.0
Benchmarking Tools	MGEN (version 5.01b)
	iPerf (version 2.0.4-1)
NTP Software	Built-in OS X System Preferences

MGEN Benchmark Script: Server Example.

```
################################################
##
##      Test MGEN script
##      2200 Packets/Second Test
##      Over 1 Minute Interval
##
##      initiate test with "./mgen input 2200script.mgn precise ON"
##
################################################


0.0 ON 1 UDP DST 192.168.1.6/5000 COUNT 6600 PERIODIC [2200.0 64]
```

MGEN Benchmark Script: Client Example.

```
################################################
##
##      Test MGEN script
##      Listen to server
##      initiate test with "./mgen input listen_script.mgn precise ON"
##
################################################


0.0 LISTEN UDP 5000
```

INITIAL WLAN BENCHMARKING FINDINGS

Existing WLAN Benchmark Testing Using MGEN at 2200PPS: Time Results

Test Number	Start Time	Stop Time	Test Duration (seconds)	Number of MGEN real time errors
1	10:43:42.366040	10:44:42.117876	59.751836	0
2	10:45:43.197623	10:46:43.107529	59.909906	0
3	10:47:35.222929	10:48:35.047407	60.175522	0
4	10:49:03.901048	10:50:03.737007	59.835959	0
5	10:50:30.326325	10:51:30.146789	59.820464	0
Total Number			**299.493687**	**0**
Average			**59.8987374**	**0**

Existing WLAN Benchmark Testing Using MGEN at 2200PPS: Packet Analysis Results

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Percentage of Packets Logged by Client	Average Packet Per Second Rate Achieved
1	132000	128344	97.23030303	2147.950734
2	132000	129269	97.93106061	2157.723299
3	132000	128853	97.61590909	2141.285953
4	132000	129117	97.81590909	2157.849597
5	132000	129128	97.82424242	2158.592417
Total Number	**660000**	**644711**		
Average	**132000**	**128942.2**	**97.68348485**	**2152.6804**

Existing WLAN Benchmark Testing Using MGEN at 3700PPS: Time Results

Test Number	Start Time	Stop Time	Test Duration (seconds)	Number of MGEN real time errors
1	10:31:31.846890	10:32:31.593806	59.746916	0
2	10:36:19.180444	10:37:18.932898	59.752454	0
3	10:38:12.229652	10:39:12.052650	59.822998	0
4	10:39:34.557426	10:40:34.472214	59.914788	0
5	10:40:57.297821	10:41:57.185240	59.887419	0
Total Number			**299.124575**	**0**
Average			**59.824915**	**0**

Existing WLAN Benchmark Testing Using MGEN at 3700PPS: Packet Analysis Results

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Percentage of Packets Logged by Client	Average Packet Per Second Rate Achieved
1	222000	220022	99.10900901	3682.566645
2	222000	219792	99.00540541	3678.376122
3	222000	219825	99.02027027	3674.590163
4	222000	220642	99.38828829	3682.59669
5	222000	221781	99.90135135	3703.298684
Total Number	**1110000**	**1102062**		
Average	**222000**	**220412.4**	**99.28486486**	**3684.285661**

Existing WLAN Benchmark Testing Using MGEN at 6000PPS: Time Results

Test Number	Start Time	Stop Time	Test Duration (seconds)	Number of MGEN real time errors
1	10:15:09.014294	10:16:42.316236	93.301942	26
2	10:17:32.666065	10:19:04.750973	92.084908	26
3	10:20:04.744917	10:21:33.995103	89.250186	22
4	10:22:23.189451	10:23:54.030333	90.840882	24
5	10:24:25.657953	10:25:58.509703	92.85175	25
Total Number			**458.329668**	**123**
Average			**91.6659336**	**24.6**

Existing WLAN Benchmark Testing Using MGEN at 6000PPS: Packet Analysis Results

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Percentage of Packets Logged by Client	Average Packet Per Second Rate Achieved
1	360000	356478	99.02166667	3820.692178
2	360000	357800	99.38888889	3885.544415
3	360000	357360	99.26666667	4004.025269
4	360000	357051	99.18083333	3930.510054
5	360000	356867	99.12972222	3843.40629
Total Number	**1800000**	**1785556**		
Average	**360000**	**357111.2**	**99.19755556**	**3896.835641**

APPENDIX B:

Initial Testing: Phase Two

WFM Specifications: Forensic Server Hardware Specifications.

Model	Desktop PC
CPU	Intel Core 2 Duo 2.66GHz (model E8200)
Memory	2 GB
Ethernet Card	TP-Link Gigabyte Ethernet adapter (TG-3269)

WFM Specifications: Forensic Server Software Specifications.

Operating System	Ubuntu Desktop Edition 10.04
Linux Kernel	2.6.32-21
Kismet	Version 2010-01-R1
Libpcap	Version 0.8
Libnl	Version 1.1-5
Libpcre	Version 7.8-3
NTP	NTP and ntpdate Version 1:4.2.4
Firewall	iptables Version 1.4.4-2
Wireshark	Version 1.2.7-1

WFM Specifications: Wireless Drone Hardware Specifications.

Model	Ubiquiti RouterStation Pro
CPU Speed	720MHz (Atheros AR7161 MIPS 24K processor)
Flash Memory	16MB
RAM Memory	128MB
Ethernet	3 x Gigabyte Ethernet ports 1 x PowerOverEthernet port
Additional Components	3 x mini-PCI slots
Notes: Device also contains a serial port (RS-323). External storage slots include one USB 2.0 port and one SecureDigital slot.	

WFM Specifications: Wireless Drone Configuration One.

Kismet Drone	Version 2010-01-R1
Wireless Cards	2 x Mikrotik RouterBoard R52N mini-PCI cards
Wireless Driver	mac80211 ath9k (version 2010-07-16-1)
Firmware	OpenWRT Kamikaze Bleeding Edge Trunk Development Branch (revision 22321)
Linux Kernel	2.6.32.16
NTP Software	ntpclient (version 2007_365-4)
Firewall	iptables (version 1.4.6-2)

WFM Specifications: Wireless Drone Configuration Two.

Kismet Drone	Version 2010-01-R1
Wireless Cards	2 x Ubiquiti XtremeRange 2 mini-PCI cards
Wireless Driver	mac80211 ath5k (version 2010-07-16-1)
Firmware	OpenWRT Kamikaze Bleeding Edge Trunk Development Branch (revision 22321)
Linux Kernel	2.6.32.16
NTP Software	ntpclient (version 2007_365-4)
Firewall	iptables (version 1.4.6-2)

INITIAL WFM BENCHMARKING FINDINGS: Wireless Drone Configuration One

MGEN Benchmarking @ 2200PPS - Single Wireless Adapter

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Total Number of Data Frames Acquired by WFM	Percentage of Data Frames Acquired by WFM	Total Number of Acknowledgement Frames Acquired by WFM	Percentage of Acknowledgement Frames Acquired by WFM
1	660000	648143	659681	99.95166667	646488	97.95272727
2	660000	655077	660061	100.0092424	652763	98.90348485
3	660000	657914	651837	98.76318182	647258	98.06939394
4	660000	657064	661826	100.2766667	639190	96.8469697
5	660000	657567	666299	100.9543939	655278	99.28454545
Total Number	**3300000**	**3275765**	**3299704**		**3240977**	
Average	**660000**	**655153**	**659940.8**	**99.9910303**	**648195.4**	**98.21142424**

MGEN Benchmarking @ 2200PPS - Dual Wireless Adapters

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Total Number of Data Frames Acquired by WFM	Percentage of Data Frames Acquired by WFM	Total Number of Acknowledgement Frames Acquired by WFM	Percentage of Acknowledgement Frames Acquired by WFM
1	1110000	1105938	1068441	96.25594595	1030466	92.83477477
2	1110000	1106651	1071972	96.57405405	1032289	92.99900901
3	1110000	1098182	1098806	98.99153153	1050680	94.65585586
4	1110000	1102179	1091037	98.29162162	1086148	97.85117117
5	1110000	1107568	1084565	97.70855856	1079595	97.26081081
Total Number	**5550000**	**5520518**	**5414821**		**5279178**	
Average	**1110000**	**1104103.6**	**1082964.2**	**97.56434234**	**1055835.6**	**95.12032432**

MGEN Benchmarking @ 3700PPS - Single Wireless Adapter

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Total Number of Data Frames Acquired by WFM	Percentage of Data Frames Acquired by WFM	Total Number of Acknowledgement Frames Acquired by WFM	Percentage of Acknowledgement Frames Acquired by WFM
1	660000	658559	653492	99.01393939	651424	98.70060606
2	660000	658378	655316	99.29030303	651804	98.75818182
3	660000	659407	657498	99.62090909	655436	99.30848485
4	660000	658595	657389	99.60439394	655282	99.28515152
5	660000	658453	696361	105.5092424	658127	99.71621212
Total Number	**3300000**	**3293392**	**3320056**		**3272073**	
Average	**660000**	**658678.4**	**664011.2**	**100.6077576**	**654414.6**	**99.15372727**

MGEN Benchmarking @ 3700PPS - Dual Wireless Adapters

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Total Number of Data Frames Acquired by WFM	Percentage of Data Frames Acquired by WFM	Total Number of Acknowledgement Frames Acquired by WFM	Percentage of Acknowledgement Frames Acquired by WFM
1	1110000	1107194	947390	85.35045045	817434	73.6427027
2	1110000	1108771	975923	87.92099099	851117	76.67720721
3	1110000	1107884	1020668	91.95207207	920354	82.91477477
4	1110000	1107496	977144	88.03099099	856427	77.15558559
5	1110000	1109057	1007616	90.77621622	898972	80.98846847
Total Number	**5550000**	**5540402**	**4928741**		**4344304**	
Average	**1110000**	**1108080.4**	**985748.2**	**88.80614414**	**868860.8**	**78.27574775**

INITIAL WFM BENCHMARKING FINDINGS: Wireless Drone Configuration Two

MGEN Benchmarking @ 2200PPS - Single Wireless Adapter

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Total Number of Data Frames Acquired by WFM	Percentage of Data Frames Acquired by WFM	Total Number of Acknowledgement Frames Acquired by WFM	Percentage of Acknowledgement Frames Acquired by WFM
1	660000	648938	661684	101.9641322	659949	101.6967723
2	660000	659394	660768	100.2083731	660029	100.0963005
3	660000	659540	652321	98.90544925	651623	98.79961792
4	660000	658739	660278	100.2336282	659141	100.0610257
5	660000	658863	661145	100.3463542	659942	100.163767
Total Number	**3300000**	**3285474**	**3296196**		**3290684**	
Average	**660000**	**657094.8**	**659239.2**	**100.3315874**	**658136.8**	**100.1634967**

MGEN Benchmarking @ 2200PPS - Dual Wireless Adapters

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Total Number of Data Frames Acquired by WFM	Percentage of Data Frames Acquired by WFM	Total Number of Acknowledgement Frames Acquired by WFM	Percentage of Acknowledgement Frames Acquired by WFM
1	1110000	1108878	1042567	94.01999138	632380	57.02881652
2	1110000	1109620	1053895	94.97801049	649723	58.553649
3	1110000	1107592	1052704	95.04438457	649528	58.64325492
4	1110000	1107917	1051394	94.89826404	647138	58.41033218
5	1110000	1107310	1046592	94.51662136	638156	57.63119632
Total Number	**5550000**	**5541317**	**5247152**		**3216925**	
Average	**1110000**	**1108263.4**	**1049430.4**	**94.69145437**	**643385**	**58.05344979**

MGEN Benchmarking @ 3700PPS - Single Wireless Adapter

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Total Number of Data Frames Acquired by WFM	Percentage of Data Frames Acquired by WFM	Total Number of Acknowledgement Frames Acquired by WFM	Percentage of Acknowledgement Frames Acquired by WFM
1	660000	648821	660207	101.7548754	659702	101.6770419
2	660000	658575	674550	102.4256918	660030	100.2209316
3	660000	658579	786924	119.4881707	660094	100.2300407
4	660000	658717	672653	102.1156278	659319	100.0913898
5	660000	658698	660420	100.2614248	659982	100.19493
Total Number	**3300000**	**3283390**	**3454754**		**3299127**	
Average	**660000**	**656678**	**690950.8**	**105.2091581**	**659825.4**	**100.4828668**

MGEN Benchmarking @ 3700PPS - Dual Wireless Adapters

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Total Number of Data Frames Acquired by WFM	Percentage of Data Frames Acquired by WFM	Total Number of Acknowledgement Frames Acquired by WFM	Percentage of Acknowledgement Frames Acquired by WFM
1	1110000	1104255	1035598	93.78250495	610432	55.27998515
2	1110000	1101094	1029707	93.51672064	615775	55.92392657
3	1110000	1108233	1037767	93.64158981	619852	55.93155952
4	1110000	1107435	1035598	93.51320845	610432	55.12124865
5	1110000	1108628	1034437	93.30785439	613750	55.36122126
Total Number	**5550000**	**5529645**	**5173107**		**3070241**	
Average	**1110000**	**1105929**	**1034621.4**	**93.55237565**	**614048.2**	**55.52358823**

APPENDIX C:

Stabilised Testing: Phase Three

NOTE: The hardware specifications for the Forensic Server and Wireless Drone are the same as depicted in Appendix 2 aside from a single change. The Wireless Drone CPU was over clocked from 720Mhz to 800Mhz.

Stabilised WFM Specifications: Forensic Server Software Specifications.

Operating System	Ubuntu Desktop Edition 10.04
Linux Kernel	2.6.32-21
Kismet	Version 2010-07-R1
Libpcap	Version 0.8
Libnl	Version 1.1-5
Libpcre	Version 7.8-3
NTP	NTP and ntpdate Version 1:4.2.4
Firewall	iptables Version 1.4.4-2
Wireshark	Version 1.4.1

Stabilised WFM Specifications: Wireless Drone Software Specifications.

Kismet Drone	Version 2010-07-R1
Wireless Cards	2 x Ubiquiti XtremeRange 2 mini-PCI cards
Wireless Driver	mac80211 ath5k (version 2010-09-28-1)
Firmware	OpenWRT Kamikaze Bleeding Edge Trunk Development Branch (revision 23264)
Linux Kernel	2.6.32.24
Libpcap	Version 1.0.0.2
NTP Software	ntpdate (version 4.2.6p2-1)
Firewall	iptables (version 1.4.9.1-2)

STABILISED WFM BENCHMARKING FINDINGS

MGEN Benchmarking @ 2200PPS - Single Wireless Adapter

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Total Number of Data Frames Acquired by WFM	Percentage of Data Frames Acquired by WFM	Total Number of Acknowledgement Frames Acquired by WFM	Percentage of Acknowledgement Frames Acquired by WFM
1	660000	659186	661624	100.2460606	660045	100.0068182
2	660000	659344	662310	100.35	660140	100.0212121
3	660000	659086	661210	100.1833333	659428	99.91333333
4	660000	659298	661316	100.1993939	660152	100.0230303
5	660000	659432	661280	100.1939394	660182	100.0275758
Total Number	**3300000**	**3296346**	**3307740**		**3299947**	
Average	**660000**	**659269.2**	**661548**	**100.2345455**	**659989.4**	**99.99839394**

MGEN Benchmarking @ 2200PPS - Dual Wireless Adapters

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Total Number of Data Frames Acquired by WFM	Percentage of Data Frames Acquired by WFM	Total Number of Acknowledgement Frames Acquired by WFM	Percentage of Acknowledgement Frames Acquired by WFM
1	1110000	1072310	1053050	94.86936937	614248	55.33765766
2	1110000	942523	952792	85.83711712	617744	55.65261261
3	1110000	1108651	1044647	94.11234234	609522	54.91189189
4	1110000	1188740	1022952	92.15783784	594948	53.59891892
5	1110000	1109218	1042842	93.94972973	602424	54.27243243
Total Number	**5550000**	**5421442**	**5116283**		**3038886**	
Average	**1110000**	**1084288.4**	**1023256.6**	**92.18527928**	**607777.2**	**54.7547027**

MGEN Benchmarking @ 3700PPS - Single Wireless Adapter

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Total Number of Data Frames Acquired by WFM	Percentage of Data Frames Acquired by WFM	Total Number of Acknowledgement Frames Acquired by WFM	Percentage of Acknowledgement Frames Acquired by WFM
1	660000	659416	663368	100.510303	660161	100.0243939
2	660000	659175	648331	98.2319697	646761	97.99409091
3	660000	633525	654364	99.14606061	652978	98.93606061
4	660000	659109	662370	100.3590909	660207	100.0313636
5	660000	658756	661943	100.2943939	660063	100.0095455
Total Number	**3300000**	**3269981**	**3290376**		**3280170**	
Average	**660000**	**653996.2**	**658075.2**	**99.70836364**	**656034**	**99.39909091**

MGEN Benchmarking @ 3700PPS - Dual Wireless Adapters

Test Number	Total Number of Packets Generated	Total Number of Packets Logged by Client	Total Number of Data Frames Acquired by WFM	Percentage of Data Frames Acquired by WFM	Total Number of Acknowledgement Frames Acquired by WFM	Percentage of Acknowledgement Frames Acquired by WFM
1	1110000	1105747	1002070	90.27657658	552243	49.75162162
2	1110000	1108459	1000914	90.17243243	562622	50.68666667
3	1110000	1102311	995331	89.66945946	557277	50.20513514
4	1110000	1108142	1007208	90.73945946	548084	49.37693694
5	1110000	1108958	1008806	90.88342342	545009	49.09990991
Total Number	**5550000**	**5533617**	**5014329**		**2765235**	
Average	**1110000**	**1106723.4**	**1002865.8**	**90.34827027**	**553047**	**49.82405405**

APPENDIX D:

Stabilised Testing: Phase Three

Attacker’s Hardware Specifications.

Model	Asus EEE PC 900HD
CPU	900MHz
Memory	1 GB
Wireless Card	Alfa AWUS036H 1000mW wireless USB Adapter
MAC Address	00:C0:CA:37:B2:15

Attacker’s Software Specifications.

Operating System	Backtrack 4 R1
Linux Kernel	2.6.34
Wireless Driver	rtl8187 - Compact Wireless Version 2010-07-10
Wireless Driver Patch	Aircrack-ng Wireless Driver Patch – mac80211 compact wireless 2009-08-08-2 > frag+ack patch (Version 1)
NTP Software	ntpdate (version 4.2.6)
Wireshark	Version 1.2.6
Libpcap	Version 1.0.0.2
Libnl	Version 1.1-3
Aircrack-ng suite	Version 1.1 (revision 1738)
Mdk3	Version 3.0 (revision 6)

STABILISED WFM ATTACK RECREATION FINDINGS: Denial of Service Attacks

Aireplay-ng Deauthentication Flood Denial of Service Attack

Test Number	Total Number of DoS Frames Generated	Total Number of DoS Frames Acquired by WFM	Percentage of DoS Frames Acquired by WFM	Total Number of Pings Sent	Number of Secessful Pings	Percentage of Ping Packet Loss
1	73216	72216	98.63417832	310	16	94.83870968
2	73216	72316	98.77076049	310	17	94.51612903
3	73216	71935	98.25038243	310	13	95.80645161
4	73216	72156	98.55222902	310	19	93.87096774
5	73216	72487	99.004316	310	13	95.80645161
Total Number	**366080**	**361110**		**1550**		
Average	**73216**	**72222**	**98.64237325**	**310**	**15.6**	**94.96774194**

Mdk3 Authentication Flood Denial of Service Attack

Test Number	Total Number of DoS Frames Generated	Total Number of DoS Frames Acquired by WFM	Percentage of DoS Frames Acquired by WFM	Total Number of Pings Sent	Number of Secessful Pings	Percentage of Ping Packet Loss
1	300346	299108	99.58780873	309	34	88.99676375
2	300233	299952	99.90640602	306	28	90.8496732
3	300131	299944	99.93769387	306	29	90.52287582
4	300526	300439	99.97105076	305	42	86.2295082
5	300218	299923	99.90173807	307	29	90.55374593
Total Number	**1501454**	**1499366**		**1533**		
Average	**300290.8**	**299873.2**	**99.86093949**	**306.6**	**32.4**	**89.43051338**

STABILISED WFM ATTACK RECREATION FINDINGS: Fake Access Point Attacks

Mdk3 Beacon Flood Fake Access Point Attack

Test Number	Total Number of FakeAP Frames Generated	Total Number of Frames Acquired by WFM	Total Number of FakeAP Frames Acquired by WFM	Percentage of FakeAP Frames Acquired by WFM	Total Number of Kismet IDS Alerts Raised
1	37260	33439	24963	66.99677939	120
2	37168	32882	24896	66.98235041	120
3	37332	32679	24978	66.90774671	120
4	37400	32746	25084	67.06951872	120
5	37320	32698	24758	66.3397642	120
Total Number	**186480**	**164444**	**124679**		**600**
Average	**37296**	**32888.8**	**24935.8**	**66.85923188**	**120**

Airbase-ng Fake Access Point Attack

Test Number	Total Number of FakeAP Frames Generated	Total Number of Frames Acquired by WFM	Total Number of FakeAP Frames Acquired by WFM	Percentage of FakeAP Frames Acquired by WFM	Total Number of Kismet IDS Alerts Raised
1	6250	12920	3870	61.92	0
2	6412	12926	3954	61.66562695	0
3	6288	12696	3898	61.99109415	0
4	6412	12612	3937	61.40049906	0
5	6304	12962	4033	63.97525381	0
Total Number	**31666**	**64116**	**19692**		**0**
Average	**6333.2**	**12823.2**	**3938.4**	**62.19049479**	**0**

Mdk3 Beacon Flood Fake Access Point Attack: Findings Based on Channel Acquired

		Total Number of Frames Acquired per Test							
Channel	**Frequency**	**Test 1**	**Test 2**	**Test 3**	**Test 4**	**Test 5**	**Total**	**Average**	**Percentage**
1	2412	1684	1602	1640	1604	1619	8149	1629.8	6.536351386
2	2417	1574	1468	1521	1482	1484	7529	1505.8	6.039046458
3	2422	556	599	585	664	664	3068	613.6	2.46085729
4	2427	25	55	30	63	6	179	35.8	0.143576745
5	2432	74	110	89	101	16	390	78	0.312820842
6	2437	30	110	89	103	24	356	71.2	0.285549281
7	2442	20	36	28	40	9	133	26.6	0.106679928
8	2447	597	638	698	676	596	3205	641	2.570745637
9	2452	1116	1087	1101	1087	1063	5454	1090.8	4.374679158
10	2457	18672	18563	18636	18644	18647	93162	18632.4	74.72568018
11	2462	613	627	560	619	628	3047	609.4	2.44401309
Total Number		**24961**	**24895**	**24977**	**25083**	**24756**	**124672**		**100**

Airbase-ng Fake Access Point Attack: Findings Based on Channel Acquired

		Total Number of Frames Acquired per Test							
Channel	**Frequency**	**Test 1**	**Test 2**	**Test 3**	**Test 4**	**Test 5**	**Total**	**Average**	**Percentage**
1	2412	219	213	198	261	268	1159	231.8	5.885638838
2	2417	209	186	207	297	298	1197	239.4	6.078610603
3	2422	43	23	49	110	111	336	67.2	1.706276661
4	2427	4	2	0	6	5	17	3.4	0.086329474
5	2432	4	3	1	26	20	54	10.8	0.274223035
6	2437	0	0	0	2	0	2	0.4	0.010156409
7	2442	0	0	4	0	2	6	1.2	0.030469226
8	2447	19	18	26	30	31	124	24.8	0.629697339
9	2452	148	149	149	119	142	707	141.4	3.590290473
10	2457	3120	3205	3135	3048	3101	15609	3121.8	79.26569165
11	2462	104	155	129	38	55	481	96.2	2.442616291
Total Number		**3870**	**3954**	**3898**	**3937**	**4033**	**19692**		**100**