1-1-2011

Systems architecture for the acquisition and preservation of wireless network traffic

Brian Cusack
Digital Forensic Research Laboratories, Auckland

Thomas Laurenson
Digital Forensic Research Laboratories, Auckland

9th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, 5th -7th December 2011

SYSTEMS ARCHITECTURE FOR THE ACQUISITION AND PRESERVATION OF WIRELESS NETWORK TRAFFIC

Brian Cusack, Thomas Laurenson
Auckland University of Technology
Digital Forensic Research Laboratories
Auckland, New Zealand
brian.cusack@aut.ac.nz; tom.laurenson@aut.ac.nz

Abstract

Wireless networking provides a ready and cost effective solution for business applications. It has escalated in popularity mainly due to the ability to form computer networks without a wired based infrastructure. However, accompanying the widespread usage also comes the inherent prospect of criminal misuse, including unauthorized application and the launch of system attacks. This paper presents the testing of an innovative Wireless Forensic Model (WFM) system that provides capability for acquisition and preservation of wireless network traffic (802.11) frames by implementing a wireless drone architecture. It is thus a forensic readiness system providing available evidence for forensic investigation. The results show that the tested system has the ability to collect upwards of 90% of all frames, as well as evidence and detection of attacks conducted against the wireless network.

Keywords

Wireless Forensics, Network Traffic, Acquisition, Preservation, 802.11frames

INTRODUCTION

Wireless networking has become both a ubiquitous and an increasingly popular communications technology providing access and services for computing devices not physically connected to a network infrastructure. With the release of the IEEE 802.11 standard, and the subsequent availability of supported devices, Wireless Local Area Networking (WLAN) has grown to be one of the most globally accepted wireless networking standard. Such universality is due to the flexibility of the network, the extension of Local Area Networks (LAN), and the facility of high speed internet access to wireless clients (Varshney, 2003). However, accompanying the widespread usage also comes the inherent prospect of criminal misuse including unauthorized application and specific attacks conducted against WLANs (Slay & Turnbull, 2006). Since the communications medium is conducted over open airwaves it also remains available to possible intruders, creating a high risk factor and making it a logical equivalent to an Ethernet port in a parking lot (Karygiannis & Owens, 2002).

The 802.11 security features have been subjected to extensive scrutiny and a number of risks identified. These include, the weakness of the original Wired Equivalency Protocol (WEP) and Wi-Fi Protected Access (WPA) network encryption attacks (Bittau, Handley & Lackey, 2006; Beck & Tews, 2008), as well as the potential for Man in the Middle (MITM) and Denial of Service (DoS) attacks (Frankel et al., 2007). Associated with the vulnerability and misuse of wireless networks is the availability of consumer devices and software tools that can be easily obtained for conducting the identified attacks. Hence, it is certain that wireless systems will be compromised. The consequence is that systems ought to be readied for forensic investigation and examined for the forensic capability as well as the implementation of security features.

The paper is structured to review the literature and theoretical background to WLAN architectures, define the possibilities of alternative architectures for forensic benefit and to report the findings of testing an alternative architecture. The proposed Wireless Forensic Model (WFM) system architecture and drone components are defined with reference to information gathered from the literature. The system will be implemented and benchmark testing conducted to assess the capabilities of the design. Common WLAN attacks will then be recreated to evaluate the capabilities of the WFM to provide viable digital evidence. The paper concludes with a short review of issues and problem areas

WIRELESS FORENSICS

The overall digital forensic procedure 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 et al., 2006). Wireless forensics is a unique area of digital forensics

and has combined characteristics from both computer and network forensic methodologies (Yim et al., 2008). Traditional computer forensics usually involves extracting data from the storage medium of a device, such as a hard drive from a Personal Computer (PC); while network forensics encompasses the process of capturing and analyzing network traffic as the main source of evidence available (Corey et al., 2002). Furthermore, network forensics can include a number of additional sources of evidence such as analysis of Intrusion Detection systems (IDS) and firewall logs, backtracking network packets and Transmission Control Protocol (TCP) connections and the collection of data from remote network services (Nikkel, 2005). However, since wireless networking is still an emerging technology, and due to the differences in available devices and the information they may contain, performing such procedures is difficult and constantly evolving. Moreover, in terms of network traffic acquisition, wireless forensics differs from network forensics in that the IEEE 802.11 standard defines a new Medium Access Control (MAC) specification for network communication between compatible devices (IEEE 802.11 Std., 2007). Therefore, different methodologies and digital forensic procedures are needed to ensure that viable digital evidence is obtained from the investigation procedure.

Wireless Network Sources of Evidence

Previously conducted research in the field of wireless forensics has identified potential sources of evidence in wireless networks. Turnbull & Slay (2008) categorise potential evidence from 802.11 WLANs and associated devices as either Live or Post-Mortem sources of evidence. Live sources of evidence from WLANs involve the interception and capture of wireless network traffic, specifically 802.11 frames. Captured network traffic has been abstractly described as the preserved communication between multiple nodes on a network (Nikkel, 2006). However, network traffic presents challenges as a source of evidence as, generally, there is only one opportunity to capture data transmitted via the network and inadequate evidence collection systems result in irrecoverable losses (Casey, 2004). Consequently, reliable and tested systems must be used to aid in the collection of potential evidence from network traffic. In contrast, Post Mortem sources of evidence from wireless networks involve performing traditional computer forensic processes on embedded wireless devices and/or client's wireless devices. For example, embedded wireless router systems and laptop clients. However, the type of information stored and how that information may be extracted is dependent on the type of device, the operating system used and how it is configured by the end-user (Turnbull & Slay, 2008). An example is the availability of specific log files and configuration settings.

Proposed Network Forensic Models

Various forensic models have been developed and tested in previous academic research, which involve the methodology of capturing and/or analysis of network traffic. Ngobeni & Venter (2009) proposed a theoretical Wireless Forensic Readiness Model (WFRM) which monitors wireless network traffic from various Access Points (AP). Logging functions are performed to ensure evidence preservation, thereby providing forensically sound evidence to be analyzed and reported should an incident occur. Additionally, it has been proposed that IDSs may also assist in digital forensic investigations. Although the main aim of IDSs is to aid detection of intrusions and to alert administrators, a possible further objective could be to supply evidence in civil or criminal legal proceedings (Sommer, 1999). Potential evidence is gathered and stored in IDS alert logs which may include basic event characteristics, possibly including date and time, source and destination addresses and network protocols used (Kent et al., 2006). These facts would provide forensic investigators with additional information relating to intrusion based events. Finally, Yim et al. (2008) conducted an investigation into the evidence collection of DoS attacks in a wireless network. A Forensic Profiling system is used based on wireless network traffic capture technique implemented on an existing AP using IDS methodologies to identify WLAN attacks.

WIRELESS FORENSIC MODEL: SYSTEM DESIGN

Information from available literature and the review of similar studies of academic research identified methodologies and procedures for conducting wireless forensic investigations. Due to the recognized lack of easily obtainable evidence from wireless devices, coupled with the difficulties of extracting such evidence, it can be concluded that network layer architectures designed to acquire and preserve network traffic have the potential to provide the availability of digital evidence to aid digital forensic investigations. However, as network traffic is a live source of evidence, forensic readiness principles would need to be applied so that potential evidence would be effectively obtained.

The WFM is a digital forensic readiness system designed to perform acquisition and preservation of wireless network traffic as potential digital evidence. By using drones, the WFM design centers on the ability to passively intercept network traffic being communicated between wireless devices and subsequently preserves the collected data in a secure environment. Although the main goal of the WFM system design is to acquire and preserve

wireless network traffic, it was also important that the gathered data should adhere to digital forensic principles making it forensically sound and viable. Furthermore, the design system should also comprise of easily available open source software and hardware solutions. The following subsections specify these requirements and outline the system architecture, components and testing environment used in this research.

System Architecture

The system architecture includes two subsystems: the Wireless Drone and the Forensic Server. The Wireless Drone is a distributed network node which acquires wireless network traffic for a specific AP in a WLAN and forwards the collected data to a centralized Forensic Server for storage and preservation. The system architecture is designed to be implemented in an infrastructure based 802.11 wireless network with multiple APs, where each separate AP is monitored by a wireless drone. Furthermore, the WFM is comprised of external components from a WLAN infrastructure, thus allowing for ease of integration into an existing wireless network. Figure 1 displays the system architecture of the WFM, including the existing WLAN AP and STATION (STA) client, as well as a wireless attacker and FakeAP.

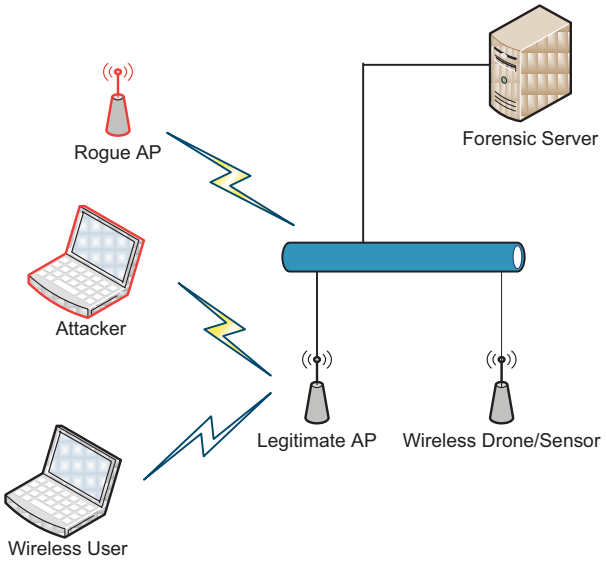

Figure 1. Wireless Forensic Model System Architecture

System Components

The proposed system architecture of the WFM incorporates two subsystems in the overall system design; the Forensic Server and the Wireless Drone. The hardware configuration of the *Forensic Server* includes a PC equipped with an Intel Dual-Core processor, 4GB of Random Access Memory (RAM), and a Gigabyte Ethernet Network Interface Card (NIC). The hardware specifications were based on operating a single wireless drone in the testing environment. Additional wireless drones would increase the computational and network specifications due to increased data from the additional wireless drones. The software configuration of the Forensic Server consists of the Operating System (OS) and a wireless sniffing application. The Ubuntu Desktop Linux OS was implemented on the Forensic Server along with the Kismet wireless sniffer application. Kismet was chosen as the software provides 802.11 passive packet capture ability and a client/server architecture allowing remote packet capture sources (Kershaw, 2011).

The hardware configuration of the *Wireless Drone* includes a wireless router with a wireless chipset which supports monitor mode for passive 802.11 frames packet capture. Additionally, the device should be equipped with Gigabyte Ethernet and a high power Central Processor Unit (CPU) to be capable of collecting and forwarding large portions of wireless network traffic. The software configuration of the Wireless Drone includes an embedded OS to run the wireless router and a wireless sniffer application to acquire wireless network traffic. The OpenWRT embedded Linux OS was used due to the ability to produce a highly customized firmware, and the Kismet application was used to acquire wireless network traffic.

System Testing Environment

In order to evaluate the capabilities of the proposed WFM a practical testing environment was proposed and implemented. It consisted of three separate entities: the WFM (including Forensic Server and Wireless Drone components), the existing WLAN (including an AP and wireless client STA) and, for the final stage of testing,

an attacker to recreate common attacks mounted against WLANs. The existing WLAN infrastructure is comprised of a single AP and client STA. It was proposed that a consumer based wireless router was to be used as the AP, while the client STA would be a laptop computer with a wireless network adapter. The existing WLAN was configured to use the 802.11g standard, with Wi-Fi Protected Access version 2 Pre-Shared Key (WPA2-PSK) mode of network encryption. The final integral part of the testing environment is the attacker. It was proposed that the attacker component would be a laptop computer running the Backtrack 4 OS, designed specifically for computer and network penetration testing. The laptop was also configured with an external wireless adapter.

WIRELESS FORENSIC MODEL TESTING

In order to test the proposed WFM, the system design was required to be implemented by using the prescribed design features. The existing WLAN infrastructure was configured and benchmarked followed by implementation of the WFM into the testing environment. Benchmarking was also conducted to ascertain the capabilities of the WFM followed by recreation of WLAN attacks to determine the effectiveness of the system design.

Existing WLAN Implementation & Benchmarking

The first stage of testing involved the implementation of the testing environment based on the previously prescribed software and hardware requirements. The existing WLAN infrastructure, comprised of an AP and single client STA, was first implemented. Consumer available devices were used, a TP-Link wireless router (model TL—WR1043ND) was configured to operate as an AP using the prescribed 802.11g mode of operation. The AP was also configured to use WPA2-PSK network encryption. The client STA was implemented using an Apple MacBook (model 5,2) and the built-in AirPort Xtreme wireless adapter. The first step of benchmark testing was conducted to evaluate the capabilities of the implemented WLAN. The iPerf application was used to perform a bandwidth test between the AP and client STA. A total of 5 tests, run for 1 minute each, were conducted with an average result of 26.54Mbps aligning with real-world 802.11g bandwidth capabilities.
A packet per second (PPS) benchmark test was then conducted to determine the existing WLAN packet transmission capabilities. The Multi-Generator (MGEN) application was used to generate TCP packet between WLAN devices. MGEN was used due to the ability to generate network traffic at specific rates, as well as extensive logging functionality to ensure correct packet generation rates (NRL, 2011). Three packet generation rates were tested, 2200, 3700 and 6000PPS, based on previous 802.11g wireless benchmarking research (Reddy, Sharma & Paulraj, 2008). Again, each test was conducted 5 times to ensure consistent results. Table 1 displays the findings from testing. It was found that the existing WLAN was capable of maintaining a maximum packet rate of approximately 3700PPS without suffering time delay in packet transmission.

Table 1.Benchmark WLAN Results

Specified PPS generation rate	Number of generated frames	Test Duration (seconds)	Aggregated PPS rate
2200PPS	128942.2	59.90	2152.68
3700PPS	220412.4	59.82	3684.29
6000PPS	357111.2	91.66	3896.84

The findings from benchmark testing provided a baseline performance measurement of the implemented WLAN. Performing benchmark testing was essential as it presented insight into the capabilities of the wireless network while also providing assurance of future results from the WFM testing.

WFM Implementation & Benchmarking

The WFM was implemented into the existing WLAN infrastructure based on the proposed system architecture and components. The first step of implementation involved performing initial testing on the Wireless Drone and Forensic Server components with the prescribed hardware and software configurations. The Wireless Drone first required a hardware platform based on a wireless router. Due to the difficulty in identifying a specific device based on the system design requirements, various consumer available wireless routers were informally tested to ascertain potential solutions. During such testing a stable version of OpenWRT firmware was installed and packet capture capabilities tested. This initial testing revealed the importance of the hardware specifications such as CPU network link speed. Eventually, the Ubiquiti RouterStation Pro was chosen as the desired hardware platform because the device was designed to run OpenWRT. It also has Gigabyte Ethernet and the ability to operate multiple mini-PCI wireless adapters.

Final implementation of the Wireless Drone involved equipping the RouterStation Pro with dual Ubiquiti XtremeRange2 (XR2) wireless mini-PCI wireless adapters. A customized OpenWRT firmware was compiled from development source code using the OpenWRT build environment. The open source ath5k wireless drivers were used which are available with the new generation mac80211 wireless framework. Kismet (version 2010-07-R1) was also included in the firmware build and configured to operate as a drone forwarding collected wireless network traffic to the Forensic Server. The Forensic Server was then implemented. A PC with Gigabyte Ethernet was installed with Ubuntu Desktop Linux OS and Kismet (version 2010-07-R1). Packet capture support was added using libpcap (version 0.8). Kismet was configured to operate in server mode to collect and store all network traffic defined by the available sources. Other minor customizations were made including implementing Network Time Protocol (NTP) on the Forensic Server to enable synchronization of time between WFM devices. Preservation of acquired evidence was manually conducted by hashing the log files produced by Kismet. The md5sum tool was used to produce a unique Message Digest algorithm 5 (MD5) value. The log files were then stored on two separate partitions and mounted as read-only for data analysis.

Benchmark testing involved establishing the capabilities of the implemented WFM and measuring the bandwidth between devices. The Gigabyte network link was tested between the Forensic Server and Wireless Drone, finding an average bandwidth of 286.4Mbps. It illustrated the ability of the implemented system to handle the maximum traffic of the existing WLAN rate (26.54 Mbps) needed to be forwarded after collection by the Wireless Drone. The WFM was then benchmarked using the MGEN application and the same testing methodology at that to measure the PPS capabilities of the existing WLAN. Each TCP packet generated by MGEN was encased in an 802.11 data frame and sent from the AP to client STA on the existing WLAN. The benchmark testing was conducted at 2200 and 3700PPS with single and dual wireless adapters operating in the Wireless Drone. Again, each test was conducted 5 times to ensure consistent results were obtained. However, the test duration was extended to 5 minutes in order to ensure the WFM could handle extended periods of maximum wireless network traffic rates.

Data analysis of packet capture files was conducted using the Wireshark application and a number of 802.11 filtering rules built-in to the application. Wireshark was also used to decrypt the WPA2-PSK encrypted wireless network traffic. Decrypting was possible by capturing the 4-way handshake between AP and client STA initiated at the start of each benchmark test. The total number of acquired network packets was compared to the MGEN packet generation log and statistical percentages calculated. Table 2 displays the findings from the WFM benchmark testing. Acquisition results were based on the total number of frames generated by the MGEN application versus the total number of frames acquired by the WFM. The findings show that the WFM was capable of acquiring a high percentage of wireless network traffic; almost 100% of all data frames generated at 2200PPS and approximately 91% of all data frames with single or dual wireless adapters, operating at the maximum packet transmission speed of the existing WLAN (at 3700PPS). In addition to analysis of the generated data frames, acknowledgement frames were also analysed in regards to acquisition capabilities. It can be deduced that an acknowledgement frame is generated for every data frame sent over the network. Therefore, at 2200PPS or 3700PPS generation rates, the actual number of frames sent over the network is 4400PPS and 7400PPS respectively. However, no logging was available to ensure the number of acknowledgement frames generated. Instead, the results are based on the number of data frames generated. The results show a dramatic drop in frame acquisition capability for acknowledgement frame acquisition at 3700PPS; approximately 56% and 50% for single and dual wireless adapters respectively.

Table 2. Benchmark Acquisition Results

Frame Type	Number of Wireless Adapters	2200PPS	3700PPS
Data Frame	1	100%	92.19%
	2	99.70%	90.35%
Acknowledgement Frame	1	99.99%	56.43%
	2	99.40%	49.97%

WFM: Evidence Collection of Recreated Attacks

In order to evaluate the capabilities of the WFM to produce reliable evidence of WLAN attacks, two different groups of attacks were recreated and targeted against the existing WLAN infrastructure. Denial of Service (DoS) and Fake AP attacks were conducted, with two types in each group, and the WFM configured to collect the wireless network traffic as evidence. Furthermore, the Kismet IDS located on the Forensic Server was also configured to produce alerts based on the built-in intrusion rules provided with the application. Moreover, the Wireless Drone was configured to utilize both wireless adapters to monitor multiple channels during the recreated WLAN attacks in order to try and obtain more information and evidence of the conducted attack. The

first adapter was configured to monitor the AP channel, while the second adapter was configured to 'hop' between the remaining available channels in the 2.4GHz ISM band. With reference to the DoS attacker, two types of attacks were recreated. These were a deauthentication flood attack using the aireplay-ng tool available with the aircrack-ng suite (aircrack-ng, 2011), and an authentication flood attack using the mdk3 tool (Larbig, 2011). Both attacks flood the network with forged 802.11 frames attempting to disturb authorized network communication between WLAN devices by congesting the wireless network.

Table 3. Attack acquisition Results.

Attack Type	Number of DoS frames generated	Number of DoS frames acquired by WFM	Acquisition Percentage
Aireplay-ng Deauthentication Flood Attack	73216	72222	98.64%
Mdk3 Authentication Flood Attack	300290.2	299873.2	99.86%

The DoS attacks were both conducted from the attacker's computer targeted against the AP and client STA in the existing WLAN. The results of the recreated DoS attacks are displayed in Table 3. Again, each test was conducted 5 times, again over a period of 5 minutes. The second group of recreated attacks were Fake AP attacks launched against the existing WLAN infrastructure. The first type was a beacon flood attack, generated using the mdk3 tool and flooding forged beacon frames on a specific channel. Next, an infrastructure Fake AP attack was conducted using airbase-ng, providing a WLAN infrastructure for devices, enticing them to connect to the illegitimate wireless network. Each attack was once more conducted from the attacker's computer, specifically targeting the existing WLAN devices, and conducted 5 separate times over a 5 minute duration to ensure consistent results. The results of the WFM acquisition of Fake AP attacks are displayed in Table 4.

Table 4. Recreated Fake AP Attacks.

Attack Type	Number of Fake AP frames generated	Number of Fake AP frames acquired by WFM	Acquisition Percentage
Mdk3 Beacon Flood Attack	37296	24935.8	66.86%
Airbase-ng Fake Access Point Attack	6333.2	3938.4	62.19%

The findings from the recreated WLAN attacks illustrate the ability to obtain evidence from network events. The WFM was able to acquire an exceptionally high percentage of the recreated DoS attack traffic, though the acquisition percentage of the Fake AP attacks was a lot lower; approximately 62% and 66% for each test conducted. A lower acquisition rate from Fake AP attacks was caused by the attack occurring on a different channel from the AP channel. However, additional frames were collected by the wireless adapter configured to hop between the available channels. In terms of the evidence collected, the WFM was able to acquire and preserve 802.11 frames injected by the attacker from each recreated attack. Each frame contained information regarding the attack, such as source MAC address, frame type, timestamp and sequence number. However, the Kismet IDS proved inadequate at detecting network intrusions, being only able to detect one of the four attacks, the mdk3 beacon flood attack, which raised the APSPOOF alert based on Service Set Identifier (SSID) naming convention and a list of authorized MAC addresses.

CONCLUSION

The conducted testing phases reported significant findings regarding the capabilities of the WFM system design. The benchmark testing revealed that the WFM was capable of acquiring a large proportion of the maximum packet generation rates of the existing WLAN. Therefore, the system design implemented in the existing WLAN provided assurance of acquiring and preserving a high percentage of wireless network traffic. However, due to the nature of wireless networks using the airwaves as a transportation medium, a complete data set is unobtainable. Nevertheless, the configuration of the WFM shows that correct implementation of a system design for a specific wireless network can increase acquisition percentage and reduce data loss from a live evidence source.

In terms of the recreated attacks, the WFM was again capable of acquiring and preserving evidence of the attacks conducted against the existing WLAN. Although digital evidence of the recreated attacks was able to be acquired, there still exist potential issues with the evidence collected. This is especially true in the case of Media Access Control (MAC) address spoofing. The unique MAC address is an exceptionally important piece of information in wireless forensics as it links the wireless network traffic to a unique device. However, it continues to be difficult for a forensic investigator to link the collected evidence to an attacker's device (wireless network adapter) in the case where MAC spoofing is implemented. Furthermore, MAC address spoofing is built-in to many WLAN attack tools as a needed command parameter, thus providing the attacker assurance of anonymity when injecting forged 802.11 frames.

In terms of the WFM system design, the practical implementation demonstrated that a digital forensic readiness model is able to be constructed using readily available hardware and software. The Kismet application formed the backbone of the WFM software configuration and proved reliable at acquiring and preserving wireless network traffic in the packet capture file format. However, the IDS functionality lacks significant capabilities in terms of detecting wireless attacks. A number of potential issues surrounding the WFM system design such as attack detection capabilities, data loss and the effect of monitoring a large scale WLAN with multiple APs. Nevertheless, the proposed WFM presents a practical system design able to acquire wireless network traffic from a live source of evidence providing preserved evidence for examination and analysis in Digital Forensic investigations.

REFERENCES

aircrack-ng. (2010). Retrieved September 20, 2011 from http://aircrack-ng.org/doku.php?id=aircrack-ng

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

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.

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

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

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.

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.

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

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. (2011). Kismet ReadMe. Available online or with application http://www.kismetwireless.net/documentation.shtml#readme

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

Larbig, P. (2011). ASPj's WiFi Page: mdk3, rt73, rt2570 and other aircrack-ng experiments. Retrieved September 27, 2011 from http://homepages.tu-darmstadt.de/~p_larbig/wlan/

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

NRL (Naval Research Laboratory). (2011). Networks and Communication System Branch. Retrieved September 28, 2011 from http://cs.itd.nrl.navy.mil/work/mgen/index.php

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.

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

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

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.

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.

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.

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

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.