Chapter 8

A FORENSIC READINESS MODEL FOR WIRELESS NETWORKS

Sipho Ngobeni, Hein Venter and Ivan Burke

Abstract Over the past decade, wireless mobile communications technology based on IEEE 802.11 wireless local area networks (WLANs) has been adopted worldwide on a massive scale. However, as the number of wireless users has soared, so has the possibility of cyber crime, where criminals deliberately and actively break into WLANs with the intent to cause harm or access sensitive information. WLAN digital forensics is seen not only as a response to cyber crime in wireless environments, but also as a means to stem the increase of cyber crime in WLANs. The challenge in WLAN digital forensics is to intercept and preserve all the communications generated by the mobile devices and conduct a proper digital forensic investigation. This paper attempts to address this issue by proposing a wireless forensic readiness model designed to help monitor, log and preserve wireless network traffic for digital forensic investigations. A prototype implementation of the wireless forensic readiness model is presented as a proof of concept.

Keywords: Wireless local area networks, digital forensic readiness

1. Introduction

Wireless technologies have become very popular around the world. Wireless local area networks (WLANs) or “hotspots” blanket public places such as convention centers, airports, schools, hospitals, railway stations, coffee shops and other locations to provide seamless public access to the Internet [15]. These hotspots provide several advantages over hard-wired networks, including user mobility and flexible Internet access. However, due to their open nature, WLANs have become a major target for cyber criminals.

WLAN digital forensics involves the application of methodologies and tools to intercept and analyze wireless network events for presentation

K.-P. Chow, S. Shenoi (Eds.): Advances in Digital Forensics VI, IFIP AICT 337, pp. 107–118, 2010.

as digital evidence in a court of law [9]. As such, WLAN digital forensics is complementary to intrusion prevention – when intrusion prevention fails, WLAN digital forensics is useful for obtaining information about the intrusion. However, the primary challenge in WLAN digital forensics is to acquire all the digital evidence related to a crime [6]. This challenge arises from the fact that the devices participating in a WLAN environment are mobile. Furthermore, since the devices are not always connected to the network, it is difficult to attribute criminal activity to a particular device.

This paper proposes a wireless forensic readiness model for monitoring, logging and preserving wireless network traffic for digital forensic investigations. The wireless forensic readiness model builds on the work of Rowlingson [7] related to traditional forensic investigations. A prototype implementation of the readiness model is presented as a proof of concept.

2. Wireless Local Area Networks

WLANs represent a ubiquitous technology that provides seamless high-speed Internet connectivity at public locations. Unlike traditional LANs, WLANs connect computers to the network without physical (wired) connections. WLANs offer tremendous user mobility, enabling users to access files, network resources and the Internet [8].

2.1 Criminal Misuse of WLANs

The lack of a physical connection between a WLAN and its participating mobile devices causes crimes to remain discreet, especially since the mobile devices are potentially far removed. This fact needs to be considered when digital evidence is identified and collected in an investigation involving wireless traffic. Potential criminal misuse of WLANs include [12, 14]:

- **WLAN Detection and Connection:** This type of misuse involves an intruder using the wireless medium as a tool to commit other criminal activities (e.g., unauthorized use of the WLAN or use of the WLAN as a launch pad for other criminal activities).

- **Concealment of Digital Evidence:** This type of misuse involves hidden wireless devices or hidden wireless networks (e.g., fake access points).

- **WLAN as an Attack Vector:** This type of misuse involves attacks against the networked (mobile) devices originating from the wireless network, and attacks against the WLAN medium itself.

2.2 Sources of Digital Evidence

WLANs typically incorporate 802.11-based wireless devices. The locations where digital evidence is stored on devices and the extraction of evidence are dependent on the specific wireless device. However, the fundamental problem with 802.11-based wireless devices is their lack of a physical footprint, which is the most crucial issue in the identification of these devices [14].

It is imperative to locate all the relevant wireless devices in a digital forensic investigation. Various open source and commercial tools (e.g., Wireshark, Kismet and AirCapture) may be used by a digital forensic investigator to identify wireless networks within range, the devices connected to the wireless networks and, possibly, the locations of the wireless devices [13]. The principal drawback of these tools is the high packet drop rate [1]. The large volume of network traffic makes it difficult for the tools to accept and store all the packets; some packets may be dropped, resulting in the loss of evidence.

2.3 WLAN Digital Forensics

Digital forensics deals with the investigation of computers and other digital devices believed to be involved in criminal activities [5]. WLAN digital forensics involves the application of methodologies and tools to capture and analyze wireless network traffic that can be presented as evidence in a court of law [9]. A WLAN digital forensic methodology is a digital forensic process; the tools are software systems that intercept and analyze network traffic. A digital forensic process is a procedure that is followed to investigate a particular criminal activity involving digital evidence [2]. Every digital forensic investigation must go through the following phases of the digital forensic process:

- Define the scope and goals of the investigation.
- Determine the work and materials.
- Acquire the images of the devices to be examined.
- Perform the digital forensic analysis.
- Prepare the report.

Currently, EnCase and FTK are the most popular tools used in digital forensic investigations. The phases of the digital forensic process for EnCase are preview, imaging or acquisition, verification, recovery and analysis, restoration and archiving; the phases for FTK are detection,

Table 1. Digital forensic phases for EnCase, FTK and WFRM.

EnCase	**FTK**	**WFRM**
1. Preview	1. Detection	1. Monitoring
2. Imaging	2. Identification	2. Logging
3. Verification	3. Analysis	3. Preservation
4. Recovery and Analysis	4. Preservation	4. Analysis
5. Restoration	5. Reporting	5. Reporting
6. Archiving		

identification, analysis, preservation and reporting. Table 1 lists the phases for EnCase and FTK along with those for the wireless forensic readiness model (WFRM), which is described in the next section.

According to Table 1, only the analysis phase is common to EnCase, FTK and WFRM. The preservation and analysis phases are common to FTK and WFRM. However, it is worth noting that the digital forensic processes for FTK and EnCase are essentially the same as far as the general digital forensic process is concerned. This suggests that the phases correlate although they are named differently. The inconsistent naming of phases is due to the fact that the digital forensic processes for forensic tools are not standardized. In this paper, we adopt the general digital forensic process described by Casey [2].

Researchers have studied various issues related to wireless network forensics. Yim, *et al.* [16] proposed a WLAN forensic profiling system for collecting digital evidence after denial-of-service attacks on WLANs. Turnbull and Slay [14] consider the potential sources of digital evidence in 802.11-based wireless networking environments. Then [11] discusses methods for examining wireless access points to determine if the devices of interest are connected or were connected to a wireless network. While these efforts and others are useful, a digital forensic readiness approach for WLANs has yet to be articulated.

2.4 Digital Forensic Readiness

The purpose of digital forensic readiness is to reduce the effort involved in performing an investigation while maintaining the level of credibility of the digital evidence being collected [4]. The decrease in effort includes reductions in the time and the cost of incident response. An organization that is "forensically ready" can respond to an attack rapidly and efficiently. In general, reducing the time involved in incident response reduces the cost of the investigation.

Tan [10] discusses an incident in which an intruder took approximately two hours to launch an attack, but digital forensic experts required 40 billable hours to respond to the incident. The response took such a long time because the organization was not forensically prepared for the incident. Organizations deploying WLANs that are at a high risk of cyber attack should be ready to collect digital evidence before an incident occurs. The model presented in the next section addresses the concept of digital forensic readiness in WLANs.

3. Wireless Forensic Readiness Model

The most salient characteristic of the wireless forensic readiness model (WFRM) is that it monitors wireless network traffic at access points. The monitored traffic is stored in a log file and the integrity of the stored information is preserved. Thus, the information needed by digital forensic investigators is readily available should the need arise. The availability of the information reduces the cost of conducting the digital forensic investigation because a major portion of the digital forensic process (monitoring, logging and preservation) has already been conducted based on the WFRM.

Figure 1 shows the five phases of the digital forensic process corresponding to the WFRM. As listed in Table 1, the phases are monitoring, logging, preservation, analysis and reporting.

Phase 1 (monitoring) shows several mobile devices (MDs) connected to a WLAN through different access points (APs). The mobile devices use the access points to connect to the Internet. In addition to providing Internet connectivity, the access points are modified (for the purposes of this model) to monitor all the traffic generated by the mobile devices. For security reasons, the monitoring component uses a firewall to filter inbound and outbound wireless traffic. Filtering is the process of controlling access to the WLAN by screening packets based on the content of their headers [15].

Phase 2 (logging) records all the traffic monitored by the access points. Each access point has its own capture unit (CU) that logs the traffic passing through it. The log file is divided into separate storage areas, each consisting of (for example) 1 MB of data. When the buffer of a capture unit is full, a fixed-size block of data is moved to permanent storage. For example, B1 in Phase 2 represents a block of data consisting of 4 MB.

In Phase 3 (preservation), the capture unit sends the accumulated blocks of data to the evidence store (ES). The capture unit computes a hash value for each block of data, which is saved in the hash store

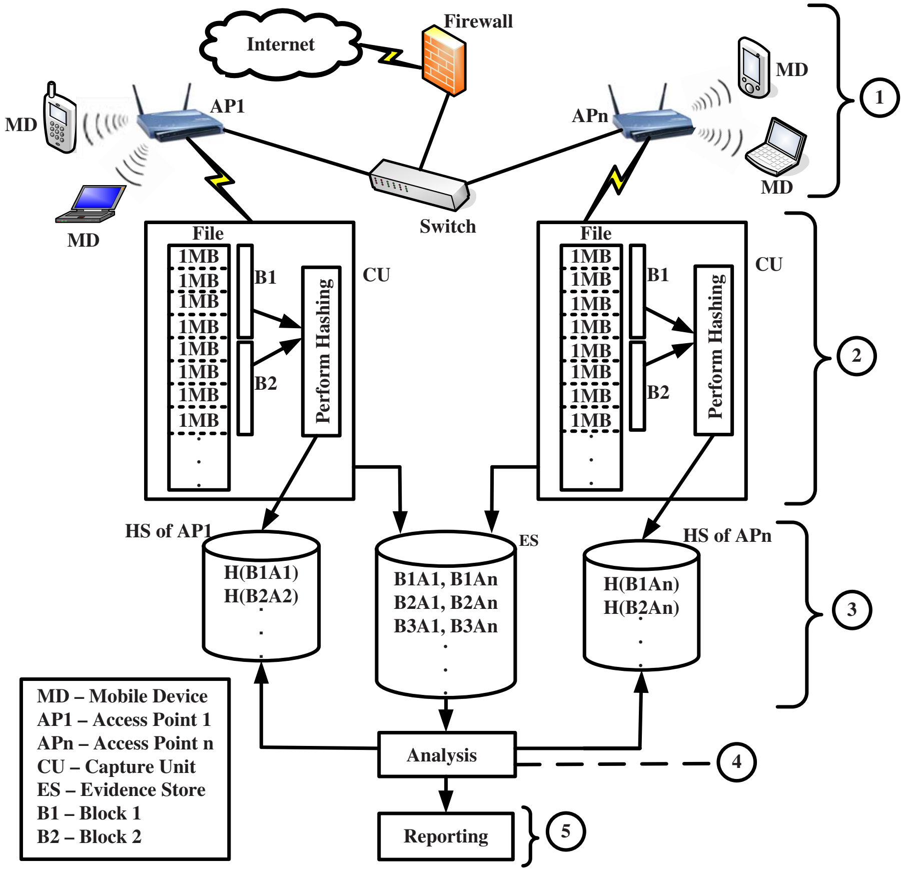


Figure 1. Wireless forensic readiness model (WFRM).

(HS) for integrity checking purposes. Phase 4 involves the analysis of the stored data and Phase 5 involves the creation of a report.

4. WFRM Simulation

The WFRM prototype was simulated using AnyLogic Professional (version 6.0) [3], a Java-based, multi-paradigm, hybrid simulation tool capable of modeling systems as a combination of discrete events, system dynamics and agents. The simulation is designed to validate the use of the WFRM for implementing digital forensic readiness in WLAN environments.

Figure 2 shows a graphical representation of the WFRM before the simulation starts. The *MobileDevice* component generates random simu-

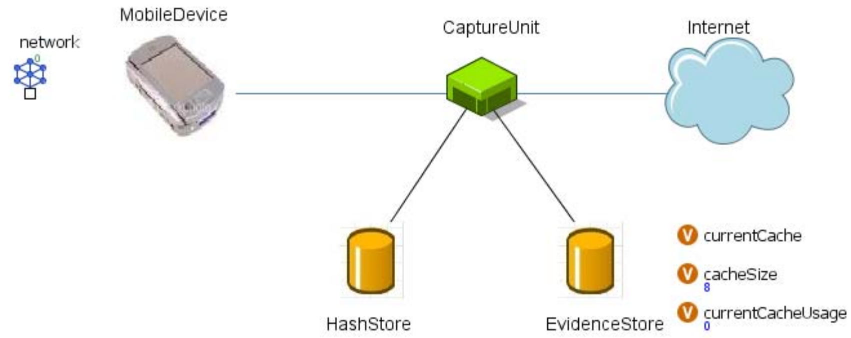


Figure 2. WFRM before the simulation.

lated messages containing source and destination IP addresses, message transmission date and time, and message content.

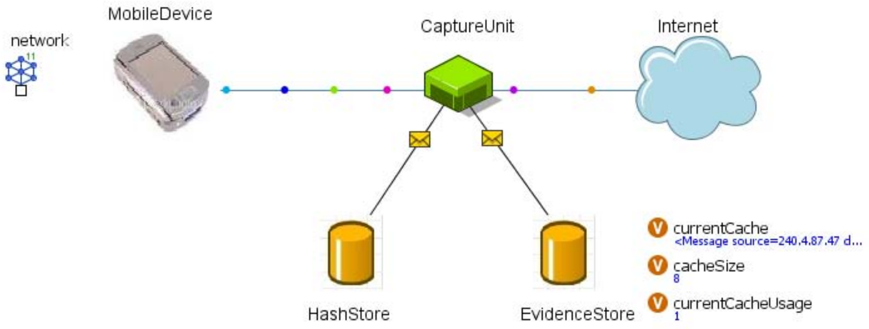
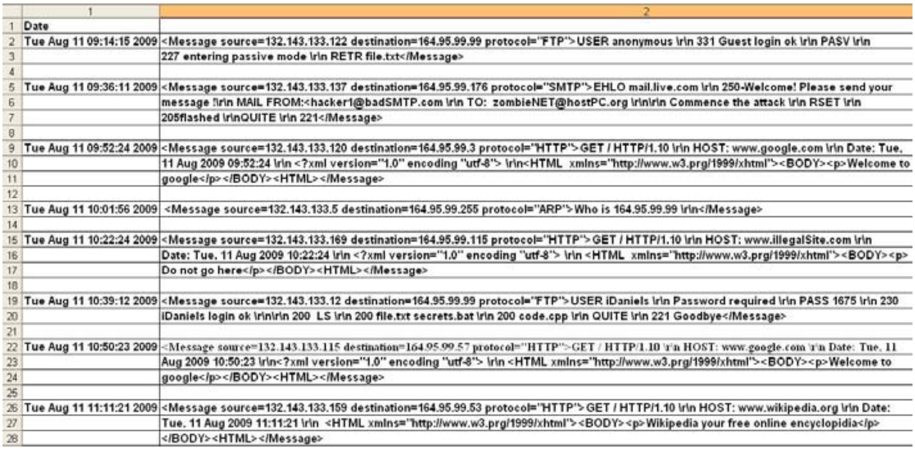


Figure 3. WFRM during the simulation.

Figure 3 shows the simulated messages flowing through the network during the simulation. The simulated messages correspond to the packets that pass through the network from various devices in the WLAN.

CaptureUnit contains the variables *currentCache*, *cacheSize* and *currentCacheUsage*. The *currentCache* variable represents the log file in our model, which works like a buffer; *currentCache* can store up to eight packets (based on the *cacheSize* in Figure 3). The eight captured packets are put together to form a single message; this represents a created block of data in our model. *CaptureUnit* computes the hash value of the formed message and stores the value in the *HashStore*; also, it passes the



	1	2
1	Date	
2	Tue Aug 11 09:14:15 2009	<Message source=132.143.133.122 destination=164.95.99.99 protocol="FTP">USER anonymous \r\n 331 Guest login ok \r\n PASV \r\n
3		227 entering passive mode \r\n RETR file.txt</Message>
4		
5	Tue Aug 11 09:36:11 2009	<Message source=132.143.133.137 destination=164.95.99.176 protocol="SMTP">EHLO mail.live.com \r\n 250-Welcome! Please send your
6		message !\r\n MAIL FROM:<hacker1@badSMTP.com \r\n TO: zombieNET@hostPC.org \r\n\r\n Commence the attack \r\n RSET \r\n
7		205flashed \r\nQUITE \r\n 221</Message>
8		
9	Tue Aug 11 09:52:24 2009	<Message source=132.143.133.120 destination=164.95.99.3 protocol="HTTP">GET / HTTP/1.10 \r\n HOST: www.google.com \r\n Date: Tue.
10		11 Aug 2009 09:52:24 \r\n <?xml version="1.0" encoding "utf-8"> \r\n<HTML xmlns="http://www.w3.prg/1999/xhtml"><BODY><p>Welcome to
11		google</p></BODY><HTML></Message>
12		
13	Tue Aug 11 10:01:56 2009	<Message source=132.143.133.5 destination=164.95.99.255 protocol="ARP">Who is 164.95.99.99 \r\n</Message>
14		
15	Tue Aug 11 10:22:24 2009	<Message source=132.143.133.169 destination=164.95.99.115 protocol="HTTP">GET / HTTP/1.10 \r\n HOST: www.illegalSite.com \r\n
16		Date: Tue. 11 Aug 2009 10:22:24 \r\n <?xml version="1.0" encoding "utf-8"> \r\n <HTML xmlns="http://www.w3.prg/1999/xhtml"><BODY><p>
17		Do not go here</p></BODY><HTML></Message>
18		
19	Tue Aug 11 10:39:12 2009	<Message source=132.143.133.12 destination=164.95.99.99 protocol="FTP">USER iDaniels \r\n Password required \r\n PASS 1675 \r\n 230
20		iDaniels login ok \r\n\r\n 200 LS \r\n 200 file.txt secrets.bat \r\n 200 code.cpp \r\n QUITE \r\n 221 Goodbye</Message>
21		
22	Tue Aug 11 10:50:23 2009	<Message source=132.143.133.115 destination=164.95.99.57 protocol="HTTP">GET / HTTP/1.10 \r\n HOST: www.google.com \r\n Date: Tue. 11
23		Aug 2009 10:50:23 \r\n<?xml version="1.0" encoding "utf-8"> \r\n <HTML xmlns="http://www.w3.prg/1999/xhtml"><BODY><p>Welcome to
24		google</p></BODY><HTML></Message>
25		
26	Tue Aug 11 11:11:21 2009	<Message source=132.143.133.159 destination=164.95.99.53 protocol="HTTP">GET / HTTP/1.10 \r\n HOST: www.wikipedia.org \r\n Date:
27		Tue. 11 Aug 2009 11:11:21 \r\n <HTML xmlns="http://www.w3.prg/1999/xhtml"><BODY><p>Wikipedia your free online encyclopidia</p>
28		</BODY><HTML></Message>

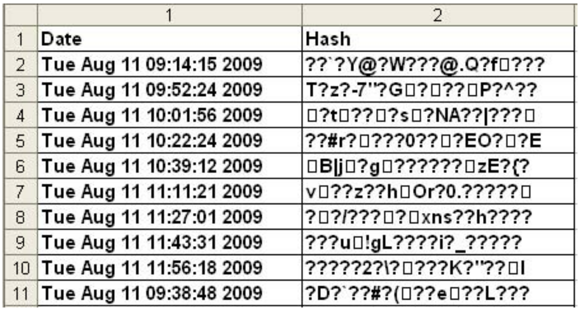
Figure 4. Evidence store.

formed message to the *EvidenceStore* for storage. The variable *currentCacheUsage* keeps track of the number of times that *currentCache* was filled with the eight packets that are combined to form a single message.

Figure 4 presents sample data in *EvidenceStore*. The message in Row 2 shows that an anonymous user with IP address `132.143.133.122` is attempting to log into a remote host via FTP. The fact that this machine is anonymous could be of interest to a digital forensic investigator. The message in Row 5 contains data such as "Please send your message," "hacker1@badSMTP.com" and "zombieNET@hostPC.org." This data seems suspicious and constitutes potential digital evidence.

The message in Row 9 shows that a machine is using HTTP to access Google; this does not appear to indicate any malicious activity. The message in Row 13 shows that the machine with IP address X is asking the machine with IP address Y if it knows the machine with IP address Z; this does not appear to be malicious. However, if Machine Y responds to Machine X that it is not aware of Machine Z, then it is possible that Machine Z is not part of the network and could be an intruder who intends to sniff network traffic between Machines X and Y. The message in Row 15 shows that a machine with IP address `132.143.133.169` is accessing a suspicious website named "www.illegalSite.com;" an error message "Do not go here" pops up when this website is accessed. The message in Row 19 shows that a machine is providing its login details to a website and downloading a suspicious file named `secrets.bat`.

Figure 5 presents the *HashStore* corresponding to the captured simulated messages. Every time a message is captured, a copy of the original



	1	2
1	Date	Hash
2	Tue Aug 11 09:14:15 2009	??`?Y@?W???@.Q?f□???
3	Tue Aug 11 09:52:24 2009	T?z?-7"?G□?□??□P?^??
4	Tue Aug 11 10:01:56 2009	□?t□??□?s□?NA??|???□
5	Tue Aug 11 10:22:24 2009	??#r?□???0??□?EO?□?E
6	Tue Aug 11 10:39:12 2009	□B|j□?g□??????□zE?{?
7	Tue Aug 11 11:11:21 2009	v□??z??h□Or?0.?????□
8	Tue Aug 11 11:27:01 2009	?□?/???□?□xns??h????
9	Tue Aug 11 11:43:31 2009	???u□!gL????i?_?????
10	Tue Aug 11 11:56:18 2009	?????2?\?□???K?"??□I
11	Tue Aug 11 09:38:48 2009	?D?`??#?(□??e□??L???

Figure 5. Hash store.

captured message is hashed and transferred to the *HashStore*. The main reason for hashing the captured information and keeping a separate copy of the original information is to verify the integrity of the captured information and to determine whether or not it was tampered with. The integrity of any message can be verified by extracting and computing the hash value (y) of the message stored in the *EvidenceStore*. The hash value (y) for the particular message block is then retrieved from the *HashStore*. If the hash values x and y match, the content of the original captured message was not tampered with and the integrity of the captured message in the *EvidenceStore* is verified. The integrity checking mechanism was built into the prototype because the integrity of evidence is a crucial requirement in any digital forensic investigation [2].

5. Discussion

In the simulation described in the preceding section, the simulated packets were logged (by *CaptureUnit*) and preserved (by *EvidenceStore* and *HashStore*). However, note that traffic monitoring was not implemented in the prototype because it is performed by the access point mainly for security reasons. After the traffic generated by the mobile devices that have connected to the WLAN has been captured and preserved, the data is ready for analysis in a digital forensic investigation. Because this data is forensically ready and forensically sound, the time and cost involved in conducting the digital forensic investigation are reduced considerably. In fact, the data needed for the investigation is readily available and the bulk of the digital forensic process (i.e., monitoring, logging and preservation) has been completed.

One disadvantage of the WFRM simulation is that the traffic is preserved in the *EvidenceStore* and *HashStore*, which potentially requires a large amount of storage space. This is not a serious problem because storage is becoming ever cheaper. Nevertheless, we are working on compression techniques that will facilitate the preservation of the entire stream of wireless network traffic. Since this might not be an optimal long-term solution to the problem, further research is needed to address the storage issue.

Finally, we note that the digital forensic processes for EnCase, FTK and WFRM (Table 1) are essentially equivalent. However, since our emphasis in this paper is the design of a readiness model, the practical implementation of the digital forensic process employed for WFRM is different from the conventional digital forensic process models for EnCase and FTK.

6. Conclusions

The wireless forensic readiness model helps address the twin challenges of intercepting and preserving all the communications generated by mobile devices in WLANs. In general, WLANs are not forensically prepared to gather digital evidence for use in ensuing investigations. The forensic readiness model focuses on the monitoring, logging and preservation of wireless network traffic. This covers the bulk of the general digital forensic investigation process, reducing both the time and the cost of forensic investigations.

Our future research will focus on several issues. One issue, as mentioned above, is the efficient storage of data in the hash store and evidence store. Another key issue is the analysis of potentially large amounts of data gathered as a result of the application of the wireless forensic readiness model. Other issues involve evidence management and the consideration of infrastructure requirements, admissibility requirements and retention requirements.

References

[1] J. Broadway, B. Turnbull and J. Slay, Improving the analysis of lawfully intercepted network packet data captured for forensic analysis, *Proceedings of the Third International Conference on Availability, Reliability and Security*, pp. 1361–1368, 2008.

[2] E. Casey (Ed.), *Handbook of Computer Crime Investigation: Forensic Tools and Technology*, Academic Press, San Diego, California, 2002.

[3] Coensys, AnyLogic 6: Multi-Paradigm Simulation Software, Cherry Hill, New Jersey (www.coensys.com/anylogic.htm).

[4] B. Endicott-Popovsky, D. Frincke and C. Taylor, A theoretical framework for organizational network forensic readiness, *Journal of Computers*, vol. 2(3), pp. 1–11, 2007.

[5] G. Francia and K. Clinton, Computer forensics laboratory and tools, *Journal of Computing Sciences in Colleges*, vol. 20(6), pp. 143–150, 2005.

[6] R. Newman, *Computer Forensics: Evidence Collection and Management*, Auerbach Publications, Boca Raton, Florida, 2007.

[7] R. Rowlingson, A ten step process for forensic readiness, *International Journal of Digital Evidence*, vol. 2(3), 2004.

[8] K. Scarfone, D. Dicoi, M. Sexton and C. Tibbs, Guide to Securing Legacy IEEE 802.11 Wireless Networks, NIST Special Publication 800-48, Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, 2008.

[9] R. Siles, Wireless forensics: Tapping the air – Part one, Symantec Corporation, Mountain View, California (www.securityfocus.com/infocus/1884), 2007.

[10] J. Tan, Forensic readiness: Strategic thinking on incident response, presented at the *Second Annual CanSecWest Conference*, 2001.

[11] C. Then, Examining wireless access points and associated devices, Forensic Focus (www.forensicfocus.com/downloads/examining-wireless-access-points.pdf), 2006.

[12] B. Turnbull and J. Slay, The 802.11 technology gap – Case studies in crime, *Proceedings of the IEEE Region 10 Conference*, 2005.

[13] B. Turnbull and J. Slay, Wireless forensic analysis tools for use in the electronic evidence collection process, *Proceedings of the Fortieth Annual Hawaii International Conference on Systems Sciences*, 2007.

[14] B. Turnbull and J. Slay, Wi-Fi network signals as a source of digital evidence: Wireless network forensics, *Proceedings of the Third International Conference on Availability, Reliability and Security*, pp. 1355–1360, 2008.

[15] E. Velasco, W. Chen, P. Ji and R. Hsieh, Wireless forensics: A new radio frequency based location system, *Proceedings of the Pacific-Asia Workshop on Cybercrime and Computer Forensics*, pp. 272–277, 2008.

[16] D. Yim, J. Lim, S. Yun, S. Lim, O. Yi and J. Lim, The evidence collection of DoS attack in WLAN by using WLAN forensic profiling system, *Proceedings of the International Conference on Information Science and Security*, pp. 197–204, 2008.