Journal of Universal Computer Science, vol. 18, no. 12 (2012), 1721-1740
submitted: 15/9/11, accepted: 15/2/12, appeared: 28/6/12 © J.UCS

The Modelling of a Digital Forensic Readiness Approach for Wireless Local Area Networks

Sipho Ngobeni
(Council for Scientific and Industrial Research, Pretoria, South Africa
sngobeni@csir.co.za)

Hein Venter
(University of Pretoria, Pretoria, South Africa
hventer@cs.up.ac.za)

Ivan Burke
(Council for Scientific and Industrial Research, Pretoria, South Africa
iburke@csir.co.za)

Abstract: Over the past decade, wireless mobile communication technology based on the 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 cybercrime. WLAN digital forensics is seen as not only a response to cybercrime in wireless networks, but also a means to stem the increase of cybercrime in WLANs. The challenge in WLAN digital forensics is to intercept and preserve all the communications generated by the mobile stations and to conduct a proper digital forensic investigation. This paper attempts to address this issue by proposing a wireless digital forensic readiness model designed to monitor, log and preserve wireless network traffic for digital forensic investigations. Thus, the information needed by the digital forensic experts is rendered readily available, should it be necessary to conduct a digital forensic investigation. The availability of this digital information can maximise the chances of using it as digital evidence and it reduces the cost of conducting the entire digital forensic investigation process.

Keywords: Wireless Local Area Network, Digital Forensics, Digital Forensic Readiness, Access Point, Digital Forensic Process, Cyber Forensic Experts, Hash Value, Digital Evidence, Traffic.
Categories: H.3.1, H.3.2, H.3.3, H.3.7, H.5.1

1 Introduction

Wireless technologies have become immensely popular around the world. Wireless Local Area Networks or "hotspots" blanket public places such as convention centres, airports, schools, hospitals, railway stations, coffee shops and other locations to provide seamless public access to the Internet [Velasco, 08]. 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 a massive quantity of security attacks [Nguyen, 08].

WLAN digital forensics involves the application of methodologies and tools to intercept and analyse wireless network events for presentation as digital evidence in a court of law [Siles, 10]. As such, WLAN digital forensics is complementary to intrusion prevention; whenever such 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 any potential crime such as Denial of Service (DoS) attacks, man-in-the-middle attack, session hijacking, attack against the WEP and may others [Newman, 07]. 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 a criminal activity to a particular device.

This paper proposes a wireless digital forensic readiness model for monitoring, logging and preserving wireless network traffic for digital forensic investigations. The proposed model builds on the work of Rowlingson [Rowlingson, 04] with regard to traditional digital forensic investigations. A prototype implementation of the proposed model is presented as a proof of concept.

The remainder of this paper is structured as follows: Sections 2, 3 and 4 present the background information on WLANs, digital forensics and digital forensic readiness respectively. The paper then proceeds to present the proposed Wireless Digital Forensic Readiness Model (WDFRM) and its related components in Section 5. A prototype implementation of the readiness model is presented in Section 6 as a proof of concept. A general discussion of the advantages and disadvantages of the proposed model and legal issues pertaining to WLAN traffic monitoring is presented in Section 7, while Section 8 concludes the paper and discusses future research work.

2 Wireless Local Area Networks

The IEEE 802.11 specification defines two types of WLANs: the ad-hoc mode and infrastructure mode. The ad-hoc mode is characterised by the lack of access point (AP), where stations communicate with one another in a peer-to-peer fashion. This type of configuration is termed Independent Basic Service Set (IBSS). An IBSS is a short-lived network with a small number of stations created for exchanging data with a vendor in a lobby of the company’s building [Ilyas, 05]. On the other hand, the infrastructure mode of WLAN comprises an access point through which all communications from the mobile clients go. The infrastructure mode is the key focus of this study.

In an infrastructure network, all mobile stations communicate with the access point, which logically connects the mobile stations to the wired LAN [Yang, 05]. In general, the access point is analogous to a base station in cellular phone networks. A basic wireless infrastructure with a single access point is called a Basic Service Set (BSS) and is depicted in Figure 1.

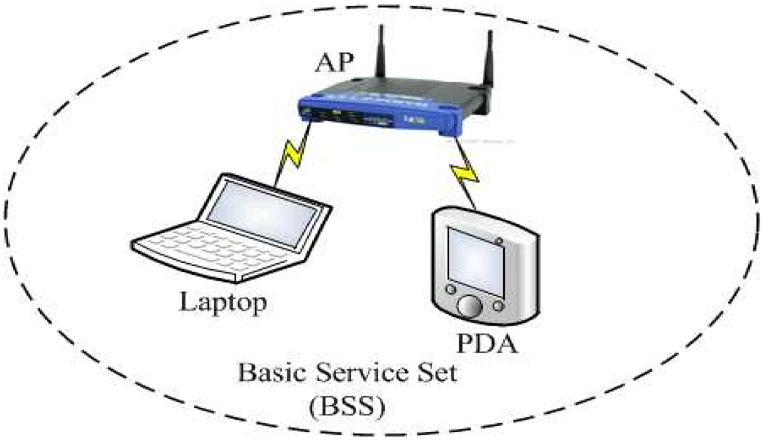

AP
Laptop
PDA
Basic Service Set
(BSS)

Figure 1: Basic Service Set

When more than one access point is connected to the network to form a single sub-network, it is called an Extended Service Set (ESS). An ESS is a collection of BSSs, where the APs communicate among themselves to forward traffic from one BSS to another and to facilitate the movement of mobile stations from one BSS to another. The AP performs all the communications through an abstract layer called the Distribution System (DS). The DS enables mobile station support in a WLAN by providing the logical services that are necessary to perform address-to-destination mapping and seamless integration of multiple BSSs [Mullet, 06]. Figure 2 contains a diagrammatical illustration of an ESS.

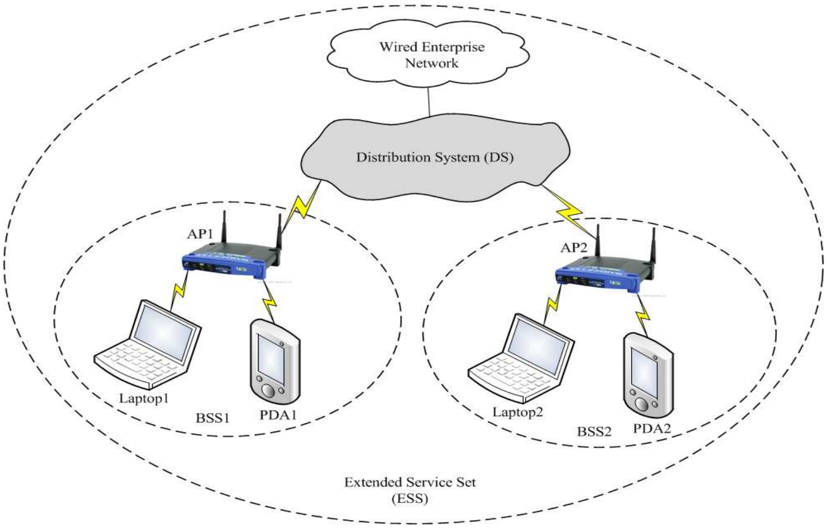

Wired Enterprise
Network
Distribution System (DS)
AP1
AP2
Laptop1
BSS1
PDA1
Laptop2
BSS2
PDA2
Extended Service Set
(ESS)

Figure 2: Extended Service Set

Having discussed the basic components that constitute a WLAN, the next section presents background information on digital forensics and the related digital forensic process.

3 Digital Forensics

Digital forensics is defined as a scientifically proven method for the investigation of computers and other digital devices believed to be involved in criminal activities [Francia, 05]. A digital forensic investigation should follow proper digital forensic procedures or process models for its evidence to be admissible in a court of law. However, to date, there is no standardised or consistent digital forensic investigation process model. In this section, the authors compare and contrast three particular digital forensic investigation process models, and finally deduce a process model suitable for the proposed wireless digital forensic readiness model.

A number of scholars have attempted to create rudimentary digital forensic process models. For example, the Digital Forensic Research Workshop (DFRW) is one of the significant participants in taking an initiative to develop a digital forensic process model [DFRW, 01]. Their process model includes the steps as listed in Table 1. The most challenge about this process model is that, analytical procedures and protocols are not standardised nor do practitioners and researchers use standard terminology [Reith, 2002].

The US Department of Justice (DOJ) also made an attempt to propose a digital forensic process model, where their steps are listed in Table 1. The significant challenge about this process model is that, the US DOJ does not make a distinction between digital forensics applied to computers or other electronic devices. Instead, it attempts to build a generalised process model that will be applicable to most electronic devices [US DOJ, 2001].

Lastly, Mandia et al also made an attempt to define a viable digital forensic process model as listed in Table 1 [Mandia, 2003]. They refer to their process model as incident response methodology. The key challenge about this methodology is that, it only focuses on computer crime and does not address the digital forensic process in terms of other digital devices such as personal digital assistant, smart appliances and other future electronic devices.

Despite the fact that several digital forensic process models exist (as indicated above), consensus has not yet been reached about a single, standardised digital forensic process model that can be adopted internationally. Table 1 summarises the phases of the three digital forensic process models mentioned above and deduce a process model applicable to the WDFRM.

From Table 1, one should be able to note that the logging, analysis, and reporting phases of the WDFRM directly correlate with that of the DFRW, US DOJ and Mandia et al. However, the logging phase of the WDFRM can be viewed as the collection phase in the other three process models. This is because logging wireless network traffic can also be viewed as data collection. The preservation phase of the WDFRM only correlates with that of the DFRW process model. The monitoring phase of the WDFRM does not directly correlate with the other three process models. In a bid to try and align the process models into a process model that would suit our

WDFRM, the phases of the WDFRM were deduced from those process models as indicated in Table 1.

Digital Forensic Process Models			
DFRW	**US DOJ**	**Mandia et al**	**WDFRM**
1. Identification 2. Preservation 3. Collection 4. Examination 5. Analysis 6. Presentation 7. Decision	1. Collection 2. Examination 3. Analysis 4. Reporting	1. Pre-incident preparation 2. Detection of incident 3. Initial response 4. Formulate response strategy 5. Investigate the incident (data collection and analysis) 6. Reporting 7. Resolution, recovery and implement security measures	1. Monitoring 2. Logging 3. Preservation 4. Analysis 5. Reporting

Table 1: A comparison of the digital forensic process models

It should be noted that coming up with the process model as depicted in the WDFRM is not the main focus of this paper. The main focus is rather on building digital forensic readiness into a process model that would be fit for a wireless LAN environment, in order for a digital forensic readiness model to be incorporated.

Having defined digital forensics, compared and contrasted various digital forensic process models with our deduced WDFRM, the next section presents digital forensic readiness.

4 Digital Forensic Readiness

The goal of this section is to show, through a digital forensic expert's opinion, that it is costly to conduct a digital forensic investigation within an organisation that is not forensically ready. We investigated as to how much it would cost to log wireless traffic in a public WLAN environment consisting of an IEEE 802.11g Access Point (AP) and clients connected to it. We first present an overview of digital forensic readiness, followed by a discussion on the performance and characteristics of 802.11g products. The calculation of the average data rate of the 802.11g products is also presented.

4.1 Overview of Digital Forensics Readiness

The purpose of digital forensic readiness is to reduce the effort involved in performing a digital forensic investigation. This is done by taking the necessary prior steps to be ready for any investigation, while maintaining the level of credibility of the digital evidence that is collected [Endicott-Popovsky, 02]. The decrease in effort is the result of the WLAN being in a state of readiness, which reduces the time and cost involved in incident response. An organisation that is ready in terms of digital forensics can respond to an attack rapidly and efficiently. In general, reducing the time involved in incident response can greatly reduce the cost of the entire digital forensic investigation.

Tan [Tan, 01] discusses an incident in which it took the intruder approximately two hours to launch an attack, but the digital forensic experts required almost 40 billable hours to respond to the incident. Their response took so long because the attacked organisation had not been digital forensically prepared for the incident.

4.2 IEEE 802.11g Performance and Characteristics

Table 2 shows a comparison of maximum data rate, modulation, data rate, and frequencies of different IEEE 802.11 specifications [WLAN, 03].

Specifications	**802.11.a**	**802.11b**	**802.11g**
Maximum data rate	54Mbps	11Mbps	*54Mbps*
Modulation	OFDM	DSSS	*OFDM and* DSSS
Data rate	6,9,12,18,24,36.48,54 Mbps	1,2,5.5,11 Mbps	DSSS:*1,2,5.5, 11* OFDM:*6,9,12, 18,24,36.48,54 Mbps*
Frequencies	5GHz	2.4GHz	*2.4GHz*

Table 2: IEEE 802.11 specifications

Theoretically, the data rate of an 802.11g AP is 54Mbps, however, practically, we assume an average data rate of 24Mbps is achievable due to factors such as interference and collision, as well as the fact that the AP is not always utilised 100% [WLAN, 03]. Of course, this data would be achievable if the AP's associated clients are also 802.11g products, also taking into consideration the range between the AP and its associated clients.

4.3 Average Data Rate of an IEEE 802.11g AP

Now that we know an 802.11g network would have an average data rate of 24 Megabits per second (Mbps), we can then calculate the average data rate it would produce in 8 hours in order to simulate a common business day). We first find the average data rate (ADR) an AP would produce in one minute.

ADR per minute = 24 Mbps * 60″
ADR per minute = 1440 / 8 bits
ADR per minute = 180 Mega Bytes (MB)

The ADR of an AP per minute is 180 MB. Now that we know the ADR produced by the AP per minute, we can calculate the ADR of the AP per hour as follows:

ADR per hour = 180 MB * 60′
ADR per hour = 10800 MB ~ 10.8 Gigabytes (GB)

The ADR of an AP per hour is 10.8 GB. To calculate the ADR per day (which in our case is 8 hours), we multiply 10800 MB by 8, which is as follows:

ADR per day = 10800MB * 8hr
ADR per day = 86400 MB ~ 86.2 GB

If a particular public WLAN, e.g. a shopping mall, has five 802.11g APs where clients can connect to them, then, the whole network would generate an average data rate of 431 GB per day. It should be noted that this value is very optimistic in the sense that we doubt that so much data will be generated over the said period, yet we need to cater for such scenarios. The average data rate may vary depending on the factors such as the number of clients associated with each AP, the range between an AP and the clients, and other factors.

4.4 Expert opinion

To show that a digital forensically ready organisation would minimise effort and save cost as Tan suggests [Tan, 01], we then requested Risk Diversion [Risk Diversion, 2012] to quote us how much will it cost to log such wireless traffic in a public wireless LAN environment with five 802.11g APs, assuming they have the necessary legal clearance to do so. Risk Diversion is a (Pty) Ltd company specialising in information security audits as well as computer, cell phone, and network forensic investigation and analysis. According to Risk Diversion, logging wireless traffic in an 802.11g network with five AP for 8 hours would cost about $2000 when hiring a full forensic team.

This shows that if an organisation were to log wireless traffic and store it in a forensically ready manner, say for five days, it would save them up to $10000 compared to hiring a full forensic team. Rather, it would cost the organisation approximately 2TB of storage in order to store all the data, boiling down to about $100 in cost. Even if data needs to be retained for a full year, the storage cost would amount to significantly less. All that would be required is to have a reliable RAID system with a few drives that would be able to accumulate data for about a week, after which the data can be written to tape drives and securely stored for periods as long as required by particular retention policies and laws. Therefore, this cost is much cheaper than carrying out a fully-fledged digital forensic investigation. The point we want to make is simply that it would be cheaper and it would be a once-off expenditure.

Organisations deploying WLANs that are at a high risk of cyber-attacks 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.

5 Wireless Digital Forensic Readiness Model

This section starts by presenting an overview of the proposed Wireless Digital Forensic Readiness Model (WDFRM) in the form of a block diagram. The components of the model are discussed separately, followed by a discussion of the model as an integrated whole.

5.1 Overview of the WDFRM

The principal concept addressed by the WDFRM 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. The information needed by cyber forensic experts is therefore readily available should it become necessary to conduct a digital forensic investigation.

The mere fact that this digital information is now available maximises the chances of it being used as evidence and reduces the cost of conducting an entire digital forensic investigation. This is simply because a large part of the digital forensic process (i.e. the monitoring, logging and preservation) has now already been conducted. Figure 3 indicates in a block diagram how the components of the WDFRM interact with one another.

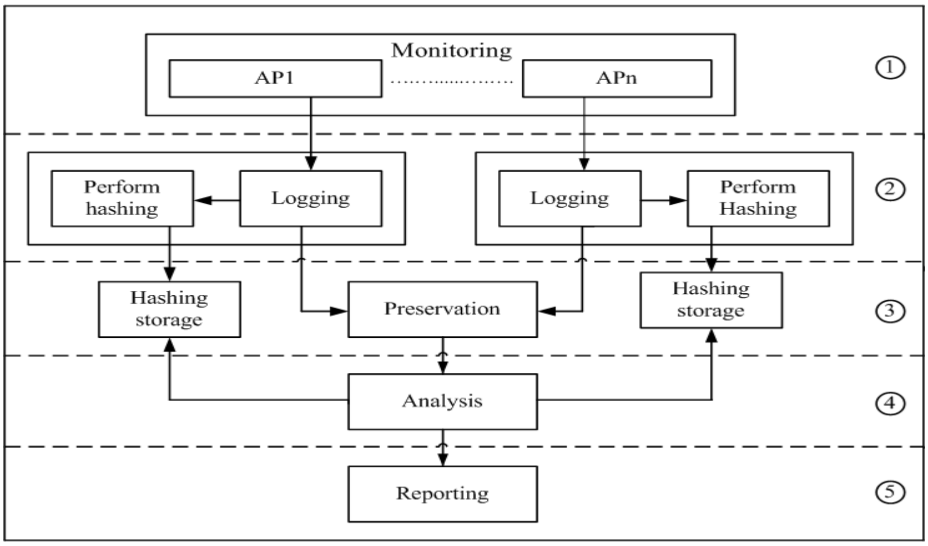


Figure 3: A block diagram of the WDFRM

The circled numbers 1 to 5 on the right-hand side of the block diagram in Figure 3 represent the phases or components of the digital forensic process of the WDFRM as indicated in Table 1. Thus, 1 represents the monitoring phase, 2 represents the logging phase, 3 represents the preservation phase, 4 represents the analysis phase and 5 represents the reporting phase.

5.2 Components of the WDFRM

This section discusses each of the five components of the Wireless Digital Forensic Readiness Model separately in its own subsection. As indicated in Table 1, the components are monitoring, logging, preservation, analysis and reporting.

The shaded area in each of the block diagrams below (from Figure 4 up to Figure 8) indicates the component that is described in more detail in the particular subsection.

5.2.1 Traffic Monitoring

Figure 4 demonstrates the traffic monitoring component whereby Mobile Devices (MDs) are associated to a WLAN through various access points (APs). This can be denoted as APi = {AP1, AP2, AP3, …, APn}, where APi denotes a set of APs from AP1 up to APn. In general, there can be many APs in a single WLAN environment. Each AP monitors all the traffic generated by the MDs that are connected to that particular AP.

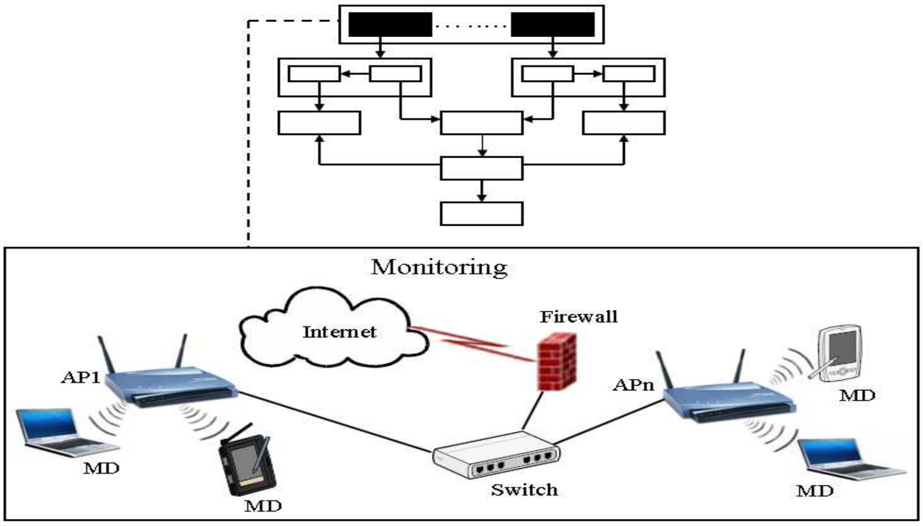


Figure 4: Traffic monitoring component

For security purposes, the monitoring component uses a firewall to filter both inbound and outbound wireless traffic. Filtering is defined as the process of controlling access to the WLAN by examining all the packets based on the content of their headers. However, a firewall cannot detect all the misconduct in a WLAN since some MDs may obscure their identities and will appear as if they are legitimate users of the network. For this reason our proposed model employs a component called the Capture Unit (CU) that records or logs all the monitored traffic. The CU is discussed in detail in the next subsection.

5.2.2 Logging

The CU logs all the traffic monitored by the different APs in order to gather potential evidence. Each AP has its own associated CU that logs the traffic passing through that AP. The CU logs the traffic in a log file as indicated in Figure 5. The log file is divided into separate storage areas with each storage area consisting of, for example, 1 Megabyte (4 MB) of data. As traffic through the AP is monitored and stored in a log file, the storage area of the log file becomes satiated. Therefore, the CU creates a block of data of several MBs, for instance B1 in Figure 5 represents a block of data consisting of 4 MBs. A block is a fixed-size unit of data that is transferred as a whole to a permanent storage area (see Section 5.2.3).

For the purpose of our model, the logged traffic is the packets. Therefore, whenever this paper refers to 'traffic', it means all the packets passing through the APs. Finally, the CU sends the accumulated blocks of data to the Evidence Store (ES) for analysis purposes and creates a hash value for each block of data that is sent to the hashing storage area for the purpose of preserving evidence (see Section 5.2.3).

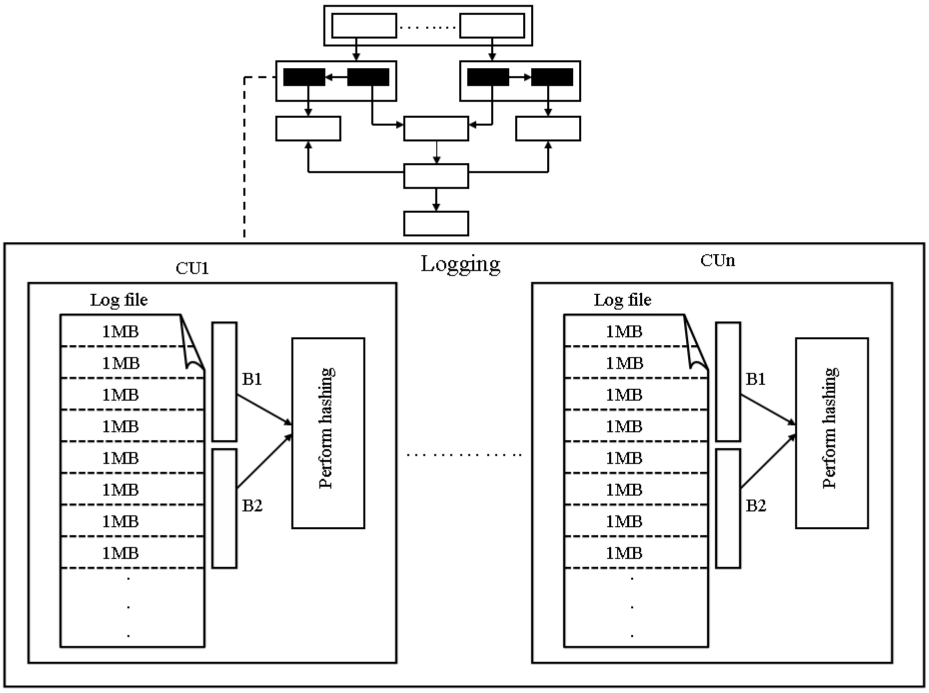


Figure 5: Logging component

5.2.3 Preservation

The primary goal of evidence preservation in WLANs is to ensure that absolutely no changes are made to the logged data once it has been collected [Endicott-Popovsky, 02]. Figure 6 demonstrates how the log files are preserved in the proposed model. The Evidence Server (ES) stores all the blocks of data received from various CUs. In general, the ES acts as a central storage area for all the data monitored by the APs. The ES logs the blocks of data in chronological order. These blocks of data are stored according to the AP from which the traffic was monitored. For example, in the ES, B1AP1 means that block 1 represents the first block of traffic monitored from the first AP, whereas B1APn means that block 1 represents the first block of the traffic monitored from the n^{th} AP.

It is worth noting that the data stored in the ES is needed for analysis purposes only. Analysis of this data will only take place if a particular incident has been reported on the WLAN, which then needs to be investigated.

The hash values of the blocks of data created in the 'perform hashing' subcomponent within the CU is transferred to the hashing storage areas represented as "HS of AP1" (Hashing Storage of AP1) and "HS of APn" (Hashing Storage of the n^{th} AP) (see Figure 6). There is a hashing storage area for each AP on the WLAN. The H(B1AP1) in HS of AP1 shown in Figure 6 represents the hash value of the first block from the first AP, and H(B1APn) in HS of APn represents the hash value of the first block, from the n^{th} AP and so on.

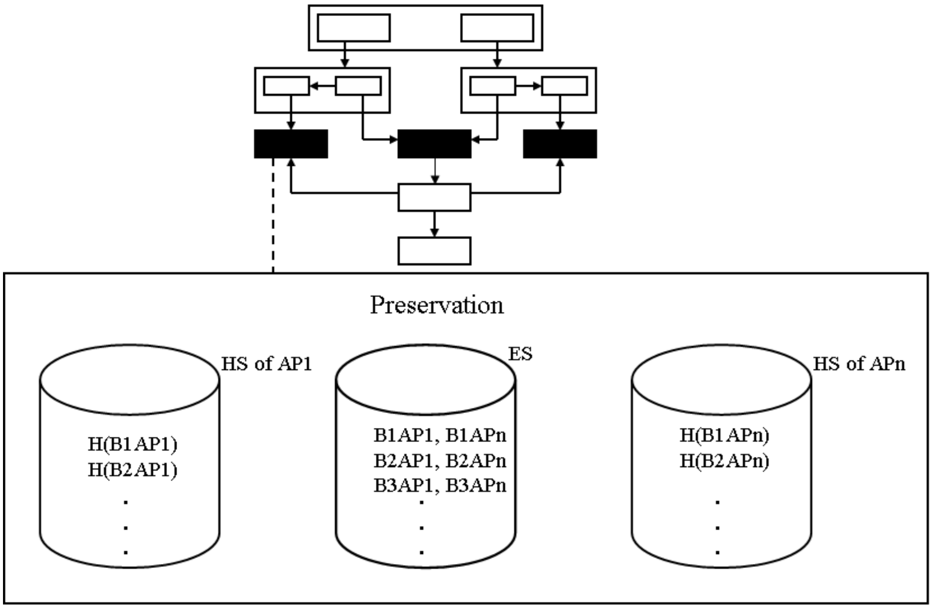


Figure 6: Preservation component

Our proposed model adopts the MD5 and SHA-1 hashing techniques. Hashing is described as a mathematical function that creates a unique fixed-length string from a message of any length [Endicott-Popovsky, 02]. The result of a hash function is a hash value, sometimes called a message digest. It is worth noting that the hashed blocks of data will only be used to check that the logged data on the ES has not been altered during the course of a digital forensic investigation. Preserving the integrity of digital evidence is an absolute requirement of the digital forensic process [Casey, 02].

5.2.4 Analysis

The main purpose of the analysis phase of the WDFRM is to mine and extract the data from the ES in an attempt to come up with evidence that can associate a particular adversary with a criminal activity committed on the WLAN. This process is represented in Figure 7. Although it is not within the scope of this study to discuss data mining in detail, the use of data-mining techniques should not be overlooked during the process of conducting a digital forensic investigation. The analysed data is next passed on to the reporting phase.

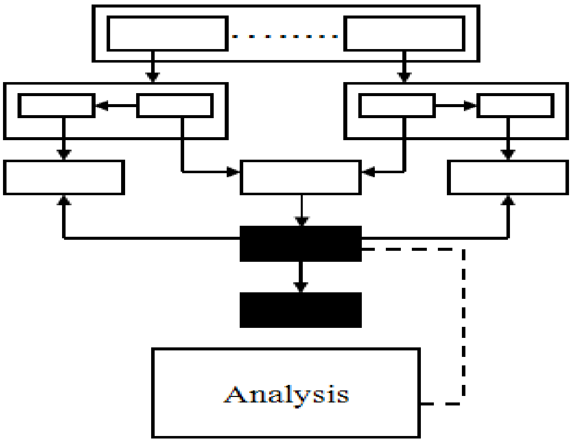


Figure 7: Analysis component

5.2.5 Reporting

During the reporting phase, the final evidence is prepared for the entire digital forensic investigation. The data is used by cyber forensic experts when they testify in a court of law that an intruder should be found guilty due to the evidence that they have gathered in their digital forensic investigation. The prosecutor in a court of law has to decide whether the intruder is guilty or not, based on the evidence presented by the cyber forensic experts concerned. Figure 8 indicates the reporting phase.

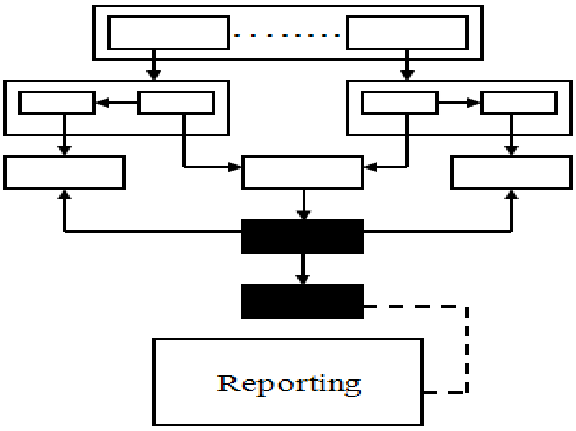


Figure 8: Reporting component

5.3 The WDFRM as an integrated whole

In this section the components discussed in the previous section are integrated. The WDFRM is depicted with all its components/phases as explained in the preceding section. Figure 9 shows how wireless traffic is monitored in the WLAN, how the monitored traffic is logged, how the digital evidence is preserved and how it is stored for analysis purposes so as to render information that is forensically ready to be used by digital forensic experts.

Figure 9 shows all the components of the WDFRM, with circled numbers 1 to 5 representing the five phases or components of the digital forensic process. Four mobile devices (MDs) and two access points (APs) are involved in the monitoring component. Two of the MDs are connected to each of the APs. These MDs probably have Internet access in a particular hotspot. In terms of the WDFRM our study assumes that a particular device is deployed closer to the WLAN. This device has a number of capabilities – i.e. monitoring wireless traffic, logging the monitored traffic, preserving the traffic, and analysing the traffic. The component that does the logging receives all the monitored wireless traffic from an AP and stores the data in a log file. The log file is divided into separate storage areas of, say, 4 MB. The reason for choosing the 4 MB storage capacity is that, larger file sizes will reduce the number of records in the database (DB) which means during reconstruction, fewer records need to be extracted from the DB. However, devices have a limited file storage space. Larger data files mean there will be less transmission to the server. As the log file accumulates data, every fourth block, for example, is merged as a block of data. These blocks are then transferred to the Evidence Server (ES), which constitutes the preservation component. Our study also assumes that the ES is a sufficiently large mass storage device. The hash values of each of these blocks are next created and transferred to the hashing storage area. In this way the integrity of the data that flows through the WLAN is preserved.

Let us assume that an incident is being reported on the WLAN. Responding to the reported incident will not require much effort because the digital data is already forensically ready. The cyber forensic experts will simply extract the data from the ES and do the necessary analysis. The integrity of the analysed data can be proven beyond any doubt by creating hash values of each block from which the evidence was extracted, and matching those with the original hash values of each block as stored in the hashing storage. If the hash values match, it proves that the extracted digital evidence was in fact the original evidence, thus proving that the original evidence was not altered or tampered with.

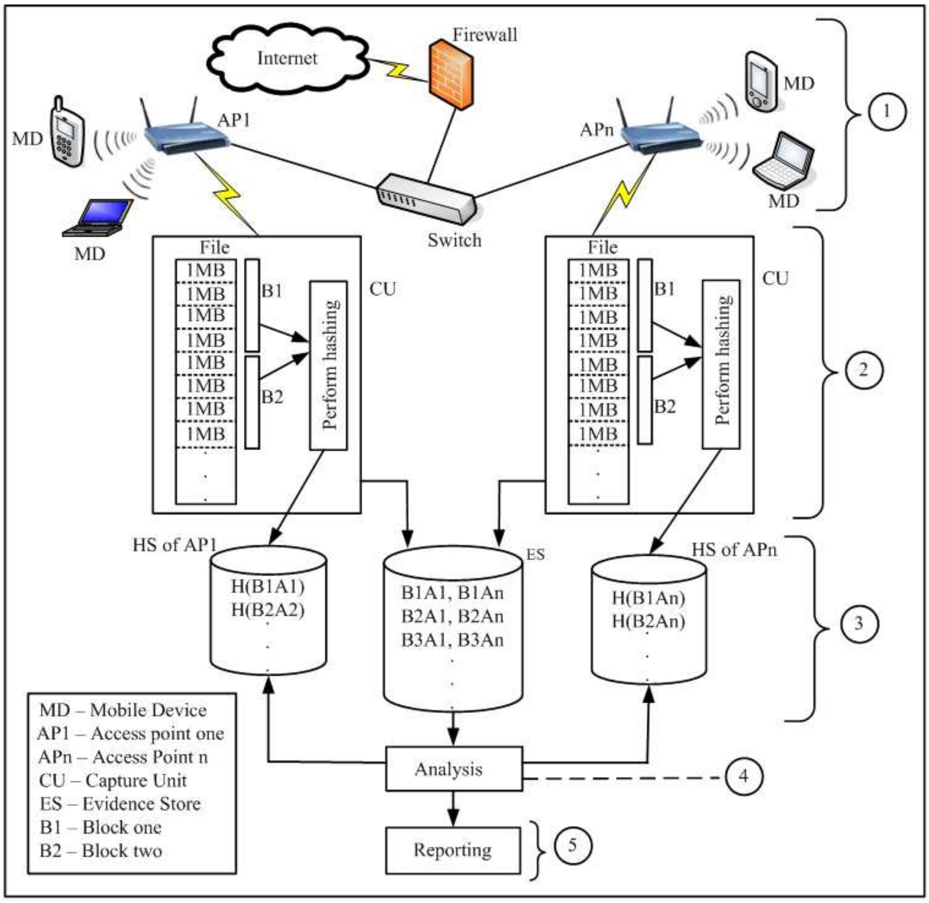

Internet
Firewall
MD
AP1
APn
MD
MD
MD
Switch
File
1MB
B1
B2
Perform hashing
CU
File
CU
HS of AP1
H(B1A1)
H(B2A2)
ES
B1A1, B1An
B2A1, B2An
B3A1, B3An
HS of APn
H(B1An)
H(B2An)
Analysis
Reporting
①
②
③
④
⑤
MD – Mobile Device
AP1 – Access point one
APn – Access Point n
CU – Capture Unit
ES – Evidence Store
B1 – Block one
B2 – Block two

Figure 9: The Wireless Digital Forensic Readiness Model

This section introduced the WDFRM in the form of a block diagram. The components of the WDFRM were initially presented separately, after which the proposed model, in which all the components were combined, was discussed. The next section presents a prototype of the WDFRM as a proof of concept.

6 WDFRM Prototype

This section presents the prototype of the WDFRM. It first gives an overview of the development environment and why the prototype was developed. The section proceeds to present the prototype development in detail.

6.1 Overview of the Prototype

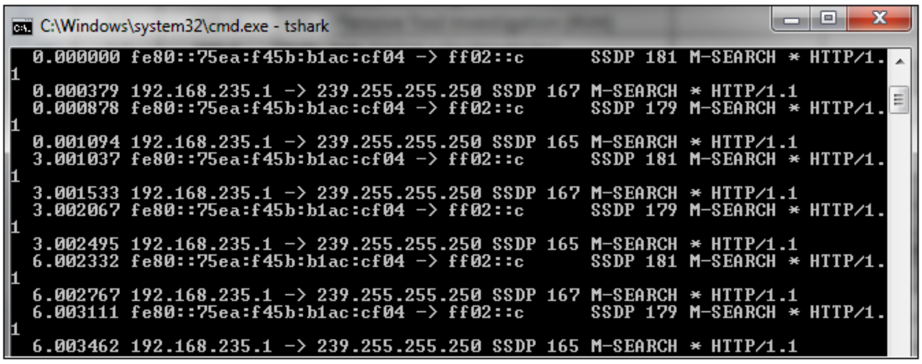
The WDFRM prototype was developed using Code::Blocks (version 10.06), which is an open source, cross platform, and free C++ Integrated Development Environment (IDE). Though it was designed for the C++ programming language, it uses plugins that enables it to support many other programming languages (Code::Blocks, 11). The prototype is developed to validate the use of the WDRFM for implementing digital forensic readiness in a WLAN environment.

6.2 Prototype Development

This section discusses how the live wireless network traffic was captured and stored in a forensically sound manner.

6.2.1 Tshark

The prototype uses Tshark [Tshark, 10] to capture raw packets as they traverse the live wireless network. This includes the source and destination address, source and destination ports, protocol used, packet size, as well as the message header of every packet. Figure 10 shows a sample Tshark dump in console. The general format of the Tshark output as extracted from line 2 of Figure 10 is explained as follows:
[TimeStamp: 0.00037] [MAC Sender: fe80::75ea:f45b:blac:cf04] [MAC Receiver: ff02::c] [Protocol: SSDP] [Size: 167] [TCP Message Header: M-SEARCH * HTTP/1]. It should be noted that though the source and destination address appears in Figure 10 they can be resolved to MAC addresses.

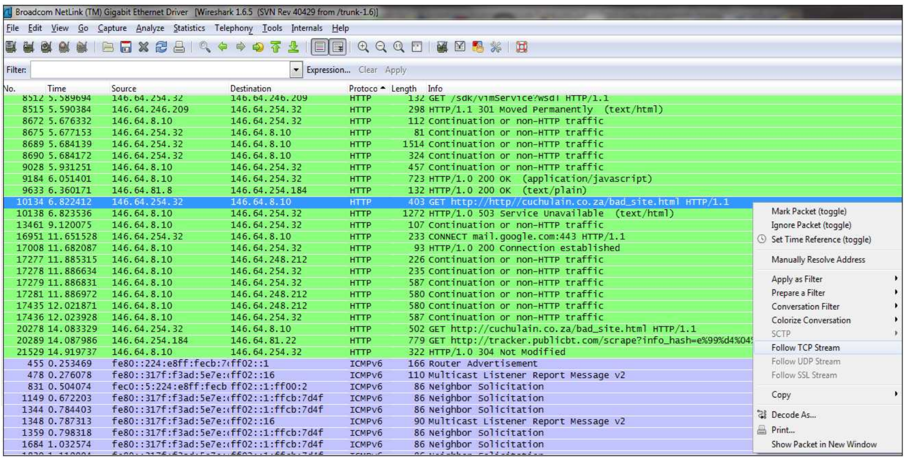


```
  0.000000 fe80::75ea:f45b:b1ac:cf04 -> ff02::c      SSDP 181 M-SEARCH * HTTP/1.
1
  0.000379 192.168.235.1 -> 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
  0.000878 fe80::75ea:f45b:b1ac:cf04 -> ff02::c      SSDP 179 M-SEARCH * HTTP/1.
1
  0.001094 192.168.235.1 -> 239.255.255.250 SSDP 165 M-SEARCH * HTTP/1.1
  3.001037 fe80::75ea:f45b:b1ac:cf04 -> ff02::c      SSDP 181 M-SEARCH * HTTP/1.
1
  3.001533 192.168.235.1 -> 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
  3.002067 fe80::75ea:f45b:b1ac:cf04 -> ff02::c      SSDP 179 M-SEARCH * HTTP/1.
1
  3.002495 192.168.235.1 -> 239.255.255.250 SSDP 165 M-SEARCH * HTTP/1.1
  6.002332 fe80::75ea:f45b:b1ac:cf04 -> ff02::c      SSDP 181 M-SEARCH * HTTP/1.
1
  6.002767 192.168.235.1 -> 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
  6.003111 fe80::75ea:f45b:b1ac:cf04 -> ff02::c      SSDP 179 M-SEARCH * HTTP/1.
1
  6.003462 192.168.235.1 -> 239.255.255.250 SSDP 165 M-SEARCH * HTTP/1.1
```

Figure 10: Sample Tshark dump in console

6.2.2 Pcap File

The Tshark output is written to a Pcap file. A Pcap file is a data file created by Tshark containing packet data created during a live network capture [Pcap, 12]. The Pcap file is set to have a maximum storage capacity of 4 MB (as specified by the model), by using the -a flag provided by Tshark. Once the Pcap file is filled with the 4 MB of traffic, Tshark stops writing into the current Pcap file and create a new file to be written to. Figure 11 shows a sample Pcap file opened in Wireshark [Wireshark, 12].


Broadcom NetLink (TM) Gigabit Ethernet Driver [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply
Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Decode As...
Print...
Show Packet in New Window

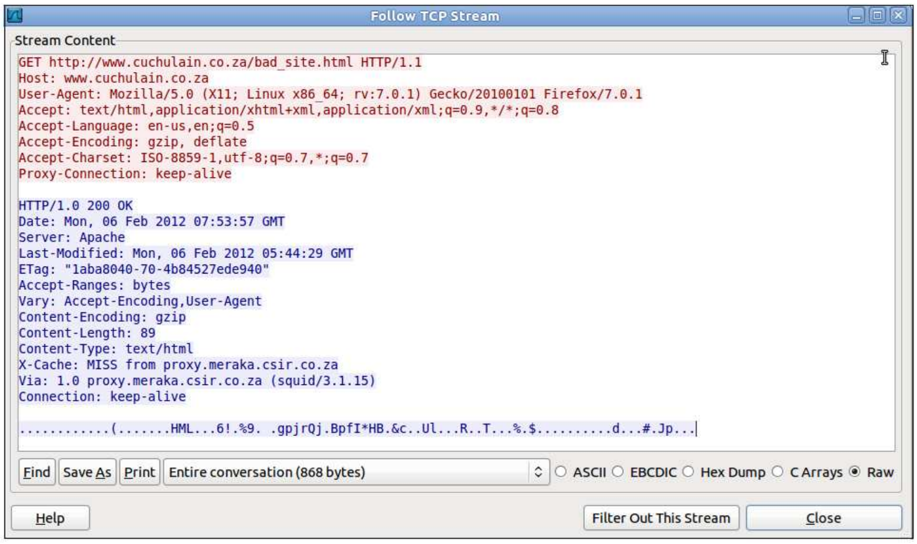
No.	Time	Source	Destination	Protoco	Length	Info
8512	5.589694	146.64.254.32	146.64.246.209	HTTP	132	GET /sdk/vimService?wsdl HTTP/1.1
8515	5.590384	146.64.246.209	146.64.254.32	HTTP	298	HTTP/1.1 301 Moved Permanently (text/html)
8672	5.676332	146.64.8.10	146.64.254.32	HTTP	112	Continuation or non-HTTP traffic
8675	5.677153	146.64.254.32	146.64.8.10	HTTP	81	Continuation or non-HTTP traffic
8689	5.684139	146.64.254.32	146.64.8.10	HTTP	1514	Continuation or non-HTTP traffic
8690	5.684172	146.64.254.32	146.64.8.10	HTTP	324	Continuation or non-HTTP traffic
9028	5.931251	146.64.8.10	146.64.254.32	HTTP	457	Continuation or non-HTTP traffic
9184	6.051401	146.64.8.10	146.64.254.32	HTTP	723	HTTP/1.0 200 OK (application/javascript)
9633	6.360171	146.64.81.8	146.64.254.184	HTTP	132	HTTP/1.0 200 OK (text/plain)
10134	6.822412	146.64.254.32	146.64.8.10	HTTP	403	GET http://http//cuchulain.co.za/bad_site.html HTTP/1.1
10138	6.823536	146.64.8.10	146.64.254.32	HTTP	1272	HTTP/1.0 503 Service Unavailable (text/html)
13461	9.120075	146.64.8.10	146.64.254.32	HTTP	107	Continuation or non-HTTP traffic
16951	11.651528	146.64.254.32	146.64.8.10	HTTP	233	CONNECT mail.google.com:443 HTTP/1.1
17008	11.682087	146.64.8.10	146.64.254.32	HTTP	93	HTTP/1.0 200 Connection established
17277	11.885315	146.64.8.10	146.64.248.212	HTTP	226	Continuation or non-HTTP traffic
17278	11.886634	146.64.8.10	146.64.254.32	HTTP	235	Continuation or non-HTTP traffic
17279	11.886831	146.64.8.10	146.64.254.32	HTTP	587	Continuation or non-HTTP traffic
17281	11.886972	146.64.8.10	146.64.248.212	HTTP	580	Continuation or non-HTTP traffic
17435	12.021871	146.64.8.10	146.64.248.212	HTTP	580	Continuation or non-HTTP traffic
17436	12.023928	146.64.8.10	146.64.254.32	HTTP	587	Continuation or non-HTTP traffic
20278	14.083329	146.64.254.32	146.64.8.10	HTTP	502	GET http://cuchulain.co.za/bad_site.html HTTP/1.1
20289	14.087986	146.64.254.184	146.64.81.22	HTTP	779	GET http://tracker.publicbt.com/scrape?info_hash=e%99%d4%04
21529	14.919737	146.64.8.10	146.64.254.32	HTTP	322	HTTP/1.0 304 Not Modified
455	0.253469	fe80::224:e8ff:fecb:7	ff02::1	ICMPv6	166	Router Advertisement
478	0.276078	fe80::317f:f3ad:5e7e:	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
831	0.504074	fec0::5:224:e8ff:fecb	ff02::1:ff00:2	ICMPv6	86	Neighbor Solicitation
1149	0.672203	fe80::317f:f3ad:5e7e:	ff02::1:ffcb:7d4f	ICMPv6	86	Neighbor Solicitation
1344	0.784403	fe80::317f:f3ad:5e7e:	ff02::1:ffcb:7d4f	ICMPv6	86	Neighbor Solicitation
1348	0.787313	fe80::317f:f3ad:5e7e:	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
1359	0.798318	fe80::317f:f3ad:5e7e:	ff02::1:ffcb:7d4f	ICMPv6	86	Neighbor Solicitation
1684	1.032574	fe80::317f:f3ad:5e7e:	ff02::1:ffcb:7d4f	ICMPv6	86	Neighbor Solicitation

Figure 11: Sample Pcap file opened in Wireshark

The reason for using Wireshark to open the Pcap file is to reproduce the raw packet in the Pcap file into a more readable format. For example, the information about each packet, that is, the source and destination address, port address, packet size and message header is reconstructed into a more meaningful way compared to the example in Figure 10.

It should be noted that, by following the Transmission Control Protocol (TCP) stream, one can uncover whom requested which site in the network and what content the server returned. Figure 12 shows TCP stream content as a result of right-clicking on the contents of the packets in Figure 11 and choosing the option “Follow TCP Stream”.

The red text in Figure 12 represents a client's request to an apache server indicated in blue text. The user makes an http GET request to the apache server. The server is located on the remote host www.cuchulani.co.za. In this example, the client uses a Firefox web browser as can be seen by referring to the user-agent string in Figure 12. The server sends an http acknowledgement with “200 Ok” meaning that it has received the client's request. All this information might be used as digital evidence to show that the particular client in this example did receive a certain request, should there be a need for such a digital forensic investigation. Similarly, any other digital evidence of potential investigative value can be extracted in this way.

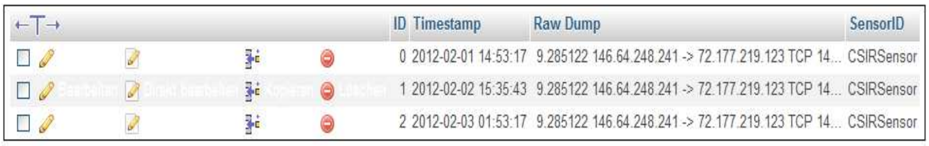


```
GET http://www.cuchulain.co.za/bad_site.html HTTP/1.1
Host: www.cuchulain.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:7.0.1) Gecko/20100101 Firefox/7.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Proxy-Connection: keep-alive

HTTP/1.0 200 OK
Date: Mon, 06 Feb 2012 07:53:57 GMT
Server: Apache
Last-Modified: Mon, 06 Feb 2012 05:44:29 GMT
ETag: "1aba8040-70-4b84527ede940"
Accept-Ranges: bytes
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 89
Content-Type: text/html
X-Cache: MISS from proxy.meraka.csir.co.za
Via: 1.0 proxy.meraka.csir.co.za (squid/3.1.15)
Connection: keep-alive

............(.......HML...6!.%9. .gpjrQj.BpfI*HB.&c..Ul...R..T...%.$.........d...#.Jp...
```

Figure 12: Follow TCP stream

6.2.3 The TCP Dump Log Table

The filled Pcap file is sent to a storage database called "TCP dump log table" through the network in a separate channel to prevent collision and duplication of data captured by the Tshark application. Figure 13 depicts the TCP dump log table with packets as they were captured from the live wireless network. It should be noted that this data will only be used for analysis purposes if an incident has been reported and a digital forensic investigation is required. The data in Figure 13 represents the same data as stored in the ES in Figure 9.

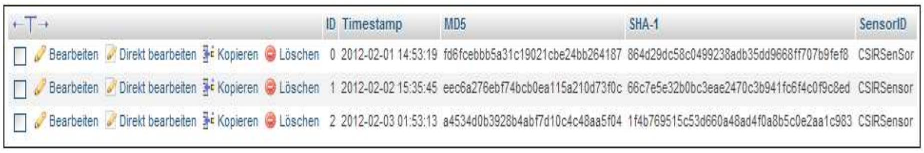


←T→	ID	Timestamp	Raw Dump	SensorID
☐	0	2012-02-01 14:53:17	9.285122 146.64.248.241 -> 72.177.219.123 TCP 14...	CSIRSensor
☐	1	2012-02-02 15:35:43	9.285122 146.64.248.241 -> 72.177.219.123 TCP 14...	CSIRSensor
☐	2	2012-02-03 01:53:17	9.285122 146.64.248.241 -> 72.177.219.123 TCP 14...	CSIRSensor

Figure 13: TCP dump log table

6.2.4 Hash Table with Both MD5 and SHA-1 Hashes of all TCP Dumps

The prototype also takes the same filled Pcap file of 1MB and creates MD5 and SHA-1 hash of it and saves the hash values in database called "Hash Table". Figure 14 depicts the hashing storage with hash values of the Pcap file. It should be noted that this is done to preserve the integrity of the captured wireless traffic. To verify the integrity of the data in the "TCP dump log table", we create MD5 and SHA-1 hashes of the data stored in the "TCP dump log table". If the output stream is the same as that of the hashes stored in the corresponding "Hash Table" entry, then it shows the data in the “TCP dump log table” was not tampered with. The data in Figure 14 represents the same data as stored in the HS in Figure 9.



	ID	Timestamp	MD5	SHA-1	SensorID
☐ Bearbeiten Direkt bearbeiten Kopieren Löschen	0	2012-02-01 14:53:19	fd6fcebbb5a31c19021cbe24bb264187	864d29dc58c0499238adb35dd9668ff707b9fef8	CSIRSenSor
☐ Bearbeiten Direkt bearbeiten Kopieren Löschen	1	2012-02-02 15:35:45	eec6a276ebf74bcb0ea115a210d73f0c	66c7e5e32b0bc3eae2470c3b941fc6f4c0f9c8ed	CSIRSensor
☐ Bearbeiten Direkt bearbeiten Kopieren Löschen	2	2012-02-03 01:53:13	a4534d0b3928b4abf7d10c4c48aa5f04	1f4b769515c53d660a48ad4f0a8b5c0e2aa1c983	CSIRSensor

Figure 14: Hash table of TCP dumps

While this section discussed the prototype development of the WDFRM to prove its viability for implementing forensic readiness in WLAN, the next section discusses pros and cons of the proposed model with regards to traffic monitoring.

7 Advantages and disadvantages of the WDFRM and legal issues pertaining to WLAN traffic monitoring

This section discusses the WDFRM by outlining its advantages and disadvantages. It then proceeds to a discussion of traffic-monitoring issues in a WLAN environment.

Once the traffic generated by the mobile devices that connect to a WLAN has been monitored and preserved, the data concerned is ready to be analysed and used by cyber forensic experts to conduct the actual digital forensic investigation. Seeing that this information is digitally ready and forensically sound, the cyber experts’ time and thus the cost of conducting the entire digital forensic investigation is considerably minimised. In fact, the information needed for the investigation has been made readily available and the first phases of the digital forensic process, i.e. the monitoring, logging and preservation, have been completed. A disadvantage of the WDFRM, however, may be the fact that the traffic monitored from the APs and captured by the CUs requires a large amount of storage, and this may prove to be expensive. However, we are not too concerned about this disadvantage since storage space becomes ever cheaper. Nevertheless, the authors are working on introducing compression on the WDFRM as a mechanism to minimise the amount of storage area required to log the entire stream of traffic that passes through the WLAN.

It was mentioned earlier that one of the functions of the WDFRM is to monitor wireless network traffic. Traffic monitoring may also be referred to as interception of communication as presented in the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICCA). Although the RICCA Act, Act No. 70 of 2002 [RICCA, 02], prohibits the interception of communication, section 6(2)(bb) makes provision for a person to intercept communication for the purpose of investigating or detecting unauthorised use of that communication system. Section 5(2)(a) states that the interception of communication may only take place if the entity that does the interception has received prior consent in writing from the applicable law enforcement authorities.

8 Conclusions

The proposed Wireless Digital Forensic Readiness Model helps address the twin challenges of intercepting and preserving all the communication generated by mobile devices in WLANs. In general, WLANs are not digital forensically prepared or equipped to gather digital evidence for use in ensuing digital forensic investigations. Our digital forensic readiness model therefore focuses on the monitoring, logging and preservation of wireless network traffic, as this covers the bulk of most digital forensic investigations. A prototype implementation of this model was presented as a proof of concept.

9 Future Work

Future research will focus on analysis of potentially large amounts of data gathered as a result of the application of the Wireless Digital Forensic Readiness Model (key issue). Other issues involve digital evidence management and the consideration of requirements in respect of infrastructure as well as the admissibility and retention of digital evidence.

Acknowledgements

This work was funded by the Council for Scientific and Industrial Research (CSIR) and University of Pretoria, South Africa. Special thanks goes to Prof. Hein Venter (University of Pretoria) and Ivan Burke (CSIR) for their continuous support and significant contribution towards the success of this work.

References

[Casey, 02] Casey, E.: Handbook of Computer Crime Investigation, Forensic Tools and Technology, Academic Press, San Diego, California, 29 January 2002.

[Cohen, 10] Cohen, F.B.: Fundamentals of Digital Evidence, 2007.

[Endicott-Popovsky, 02] Endicott-Popovsky, B., Frincke, D., Taylor, C.: A theoretical framework for organizational network forensic readiness, Journal of Computers, Vol. 2(3), May 2007, 1-11.

[Francia, 05] Francia, G., Clinton, K.: Computer forensics laboratory and tools, Journal of Computing Sciences in Colleges, Vol. 20(6), June 2005, 143-150.

[Ilyas, 05] Ilyas, M., Ahson, S.: Handbook of Wireless Local Area Networks, Applications, Technology, Security and Standards, Taylor and Francis Publication 2005, Boca Raton, Florida, USA, 25 May 2005.

[Mullet, 06] Mullet, G.J.: Wireless Telecommunications Systems and Networks, Thomson 2006, Springfield, MA, August 2006.

[Nguyen, 08] Nguyen, T.D.; Nguyen, D.H.M., Tran, B.N., Vu, H., Mittal, N.: A lightweight solution for defending against de-authentication/disassociation attacks on 802.11 networks, In Proc. Int. Conf. on Computer Communications and Networks (ICCCN), 3-7 August 2008.

[Newman, 07] Newman, R.: Computer Forensics: Evidence Collection and Management, Auerbach Publications, Boca Raton, Florida, 9 March 2007.

[Rowlingson, 04] Rowlingson, R.: A ten step process for forensic readiness, Int. Journal of Digital Evidence, Vol. 2(3), February 2004, 1-28.

[Siles, 10] Siles, R.: Wireless forensics: Tapping the air – Part one, Symantec Corporation, Mountain View, California, 2010, http://www.symantec.com/connect/articles/wireless-forensics-tapping-air-part-one

[Tan, 01] Tan, J.: Forensic readiness: Strategic thinking on incident response, Second Annual CanSecWest Conf., 30 March 2001.

[US.DOJ, 01] The U.S. Department of Justice, Electronic Crime Scene Investigation- A Guide for First Responders, July 2001, www.nwfia.org/NIJGuideforFirstResponders.pdf

[Velasco, 08] Velasco, E., Chen, W., Ji, P., Hsieh, R.: Wireless Forensics: A new radio frequency based location system, Intelligence and Security Informatics, 17 June 2008, 272-277.

[WLAN, 03] The New Mainstream Wireless LAN Standard, White Paper, IEEE 802.11g, 07 February 2003, http://www.dell.com/downloads/global/shared/broadcom_802_11_g.pdf

[Yang, 05] Yang, L., Zerfos, P., Sadot, E.: Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP), 16 November 2005, http://rfc-ref.org/RFC TEXTS/4118/index.html