THE DESIGN OF A WIRELESS FORENSIC READINESS MODEL (WFRM)

SJ Ngobeni[1] and HS Venter[2]

Information and Computer Security Architecture Research Group (ICSA),
University of Pretoria, Pretoria, South Africa

[1]sngobeni@csir.co.za, 012 841 4410

[2]hventer@cs.up.ac.za, 012 420 3654

ABSTRACT

The proliferation of wireless mobile communication technology has emerged and this has resulted in the increase of the wireless users. On the other hand, cyber crime in WLANs has appeared to be gradually increasing world wide. Wireless network forensics is seen as not only a counterproposal but as a solution to the rapid increase of cyber crime in WLANs. However, the key issues impacting wireless network forensics are, firstly, it is an enormous challenge to monitor and collect all the communications generated by the communicating mobile devices and conduct a proper digital forensic investigation. Secondly, network traffic only exists for split seconds, and because of its large volume, it may be retained for a limited time before storage space is depleted. Therefore this suggests that WLANs are not forensically ready to gather enough evidence that can be used for subsequent forensic purposes. In an attempt to address this issue, this paper proposes a Wireless Forensic Readiness Model (WFRM) with the capabilities of monitoring, preserving and analysing wireless network traffic.

KEY WORDS

WLANs, forensic readiness, traffic, Access Point

THE DESIGN OF A WIRELESS FORENSIC READINESS MODEL (WFRM)

1 INTRODUCTION

The proliferation of mobile devices that connect to Wireless Local Area Networks (WLANs) has ushered in an era of pervasive computing [1]. The most important function of a WLAN is to provide wireless broadband connectivity at public locations like airports, railway stations, conference centres and hotels. The high broadband connectivity allows people to access and share services like data, voice and video through their mobile devices. However, cyber criminals are always making it their mission to access these services in an unauthorised way and pilfer valuable information.

Investigative techniques, forensic tools and network-based forensic techniques have rapidly evolved to track down the rapid increase in cyber crime [2]. However, one of the most noteworthy challenges of investigating criminal activity in a WLAN environment is obtaining all necessary evidence related to the crime [1]. This challenge is as a result of the fact that, firstly, all devices participating in a WLAN environment are mobile. This suggests that they are not always connected to the network; therefore it becomes difficult to monitor and collect information about the communications generated by these devices and investigate it. Secondly, network traffic only exists for split seconds, and because of its large volume, it may be retained only for a limited time before storage space is depleted. It stands to a reason, therefore, that WLANs are not forensically ready to gather enough evidence that can be used for subsequent forensic purposes.

To attend to this problem, this study proposes a Wireless Forensic Readiness Model (WFRM) with the capability of monitoring, preserving and analysing wireless network traffic in order to come up with credible evidence that can associate a security breach with a suspected mobile device. The concept of wireless forensic readiness arose in this study as a recommendation for improving the efficiency of a digital forensic investigation [3]. Further explanation on digital forensic readiness is provided in the background section of this paper. Traffic monitoring in a wireless network is mandated by law in many countries [5]. The most significant function of the proposed model is to monitor wireless network traffic and log information about this traffic for later analysis in case a security breach has occurred and a digital forensic investigation is warranted. For the purpose of the proposed model, all traffic that passes through the Access Points (APs) will be intercepted.

The remainder of this paper is structured as follows: Section 2 provides background information about WLANs, the digital forensic processes and digital forensic readiness. This paper proceeds to present the proposed model in Section 3. How the model is integrated and a discussion thereof is presented in Section 4. Section 5 concludes the paper and discusses future work.

2 BACKGROUND

This section discusses some background concepts regarding WLANs, digital forensic processes and digital forensic readiness. Each concept is described in a separate section, starting with a definition of the concept, followed by its challenges, and finally its role in the proposed model.

2.1 Wireless Local Area Networks

By definition, a Wireless Local Area Network (WLAN) is a network that links two or more computers without any physical connection [6]. The lack of physical connection between wireless networks makes it discreet, since its participating mobile devices are potentially far removed. This is indeed an issue to be considered when evidence is identified and collected within a digital forensic investigation that may involve wireless traffic. When a digital forensic investigation is conducted, the lack of physical connection between communicating wireless devices may cause the identification of such devices to be problematic. There is consequently a good chance that some of these devices may be left undiscovered [7]. WLANs utilise spread spectrum technology based on radio waves to enable communication between devices in a limited area. This gives users the mobility to move around within a broader coverage, for example WiMAX, GPRS/HSDPA, and still be connected to the network [8].

For home users, wireless networks have become popular owing to ease of installation and location freedom that results from the increased popularity of laptops and PDAs. For business, public businesses such as coffee shops and malls have begun to offer wireless access to their customers. Some services are even provided free of charge. Large wireless network projects are set up in many major cities. For instance, Google is providing a free service to Mountain View in the US, and California has entered a bid to do the same for San Francisco. New York City has also launched a pilot programme to cover all five municipalities of the city with wireless Internet access [8]. In South Africa, a number of soccer fields are currently being constructed for the 2010 Soccer World Cup. A large number of people will be attracted internationally to come and watch the 2010 World Cup games. Therefore, it is planned that wireless networks be deployed at these soccer stadiums so that people will be able to access and share services like voice, video and data through their mobile devices while watching a soccer match.

As WLANs are more widely deployed, wireless security is becoming a serious concern for an increasing number of organisations [9]. It is therefore essential that a forensic readiness mechanism with the capability to combat the unrelenting increase of cyber crime should be put in place without any further delay.

2.2 Forensic readiness

Digital forensic readiness claims that the effort to perform a digital forensic investigation should decrease while at the same time maintaining the level of credibility for the digital evidence being collected [4]. The decrease in effort referred to here is the time and cost required for an incident response during a digital forensic investigation. For example, if an organisation is forensically prepared, then there will be no huge difference between the amount of time spent by the intruder to launch the attack and the amount of time required by the cyber forensic experts to respond to the attack. In general, reducing the time to respond to an incident during a digital forensic investigation will definitely reduce the cost required to respond to that particular incident.

Dave Dittrich [10] – head of the honeynet project – discusses an incident that took an intruder a period of about two hours to launch an attack, but it took the cyber forensic experts a period of about 40 billable hours to respond to that incident. The reason why it took so long to respond to this incident is that, the organisation that was investigated was not forensically prepared for any such incident. This paper therefore claims that organisations, which deploy WLANs that are of high risk to cyber attack, should be forensically ready to collect any digital evidence in advance so that, in the event of a crime being committed over a WLAN, such collected data is ready to be used for subsequent digital forensic investigations.

2.3 Digital forensic process

A digital forensic process is defined as a procedure that is followed to investigate a particular digital criminal activity and that procedure must be acceptable in a court of law [11]. Digital forensics is hard work; therefore the cyber forensic experts need some tools to assist them in conducting the digital forensic investigation. Every digital forensic investigation need to follow the digital forensic process. The following phases represent the general digital forensic process [11]:

1. Define the scope and goals of the investigation
2. Determine the work and materials
3. Acquire images of the devices to be examined
4. Perform the digital forensic analysis
5. Prepare the report

The most popular tools used in digital forensic investigations are Encase [14] and FTK [15]. The phases of the digital forensic process for Encase include preview, imaging or acquisition, verification, recovery and analysis, and restoration, while the phases of the digital forensic process for FTK include detection, identification, analysing, preservation and reporting. Table 1 present a comparison between the phases of Encase, FTK and the phases of the model proposed in this paper, called the Wireless Forensic Readiness Model (WFRM).

Table 1. Digital forensic phases for the FTK, Encase and WFRM

Digital forensic process		
Encase	**FTK**	**WFRM**
1. Preview 2. Imaging/Acquisition 3. Verification 4. Recovery and analysis 5. Restoration 6. Archiving	1. Detection 2. Identification 3. Analysis 4. Preservation 5. Reporting	1. Monitoring 2. Logging 3. Preservation 4. Analysis 5. Reporting

Table 1 indicates that only the analysis phase of the digital forensic process is common to Encase, FTK and the WFRM model. Both the preservation and analysis phases are common to the FTK and the proposed model. However, it is worth noting that the digital forensic process for FTK and Encase is more or less the same when relating them to the general digital forensic process. This also suggests that the phases of the digital forensic tools also co-relate although they are named differently. The reason for the inconsistent naming of the phases between the various tools is because the digital forensic process has not been standardised yet. The digital forensic process, however, as taken from [11], is one that the authors assume as an acceptable general digital forensic process as used in this paper.

3 THE COMPONENTS OF THE PROPOSED MODEL

This section presents the Wireless Forensic Readiness Model (WFRM). This section starts by presenting an overview of the WFRM as a black-box. This is followed by a detailed discussion of the components that constitute the proposed model. Lastly the proposed model and all its components are presented. The complete depiction of the WFRM appears in Figure 6, but its components are discussed in separate sections below.

3.1 Overview of the WFRM

The principal concept addressed by the WFRM is that it monitors wireless network traffic from various Access Points (APs). The monitored traffic is logged in a log file, and then preserved to maintain its integrity. Thus the information needed by the cyber forensic experts is rendered readily available should it be necessary to conduct a digital forensic investigation. The availability of this digital information may maximise chances of using it as evidence and reduce the cost of conducting the entire digital forensic investigation. This is because a part of the digital forensic process (i.e. the monitoring, logging and preservation) has already been conducted. Figure 1 indicates a block diagram of the WFRM. The block diagram shows how the components of the model interact with each other. The shaded area in the block diagrams from Figure 2 up to Figure 5 represents the component that is described in each particular subsection that follows.

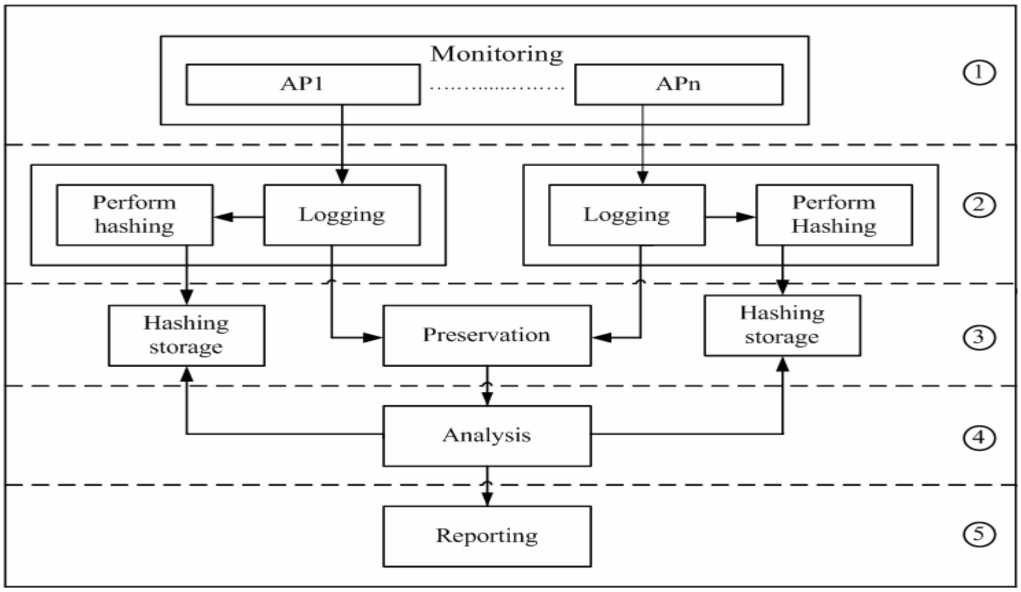

Figure 1. A block diagram for the WFRM

The numbers from 1 to 5, represented with circles in figure 1, demonstrates the phases of the digital forensic process of the WFRM as shown in Table 1. Number 1 represent the monitoring phase, number 2 represents the logging phase, number 3 represents the preservation phase, number 4 represents the analysis phase and number 5 represents the reporting phase.

3.2 Traffic monitoring

Figure 2 demonstrates the traffic monitoring component whereby Mobile Devices (MDs) are connected to a WLAN through various Access Points (APs). This can be denoted by 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, which connects to each AP. 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 can not detect all the misconduct of the WLAN since some other MDs may obscure their identities and will appear as if they are legitimate users of the network – therefore the proposed model employs another component called the Capture Unit (CU) that logs all the monitored traffic. The CU is discussed in detail in the next section.

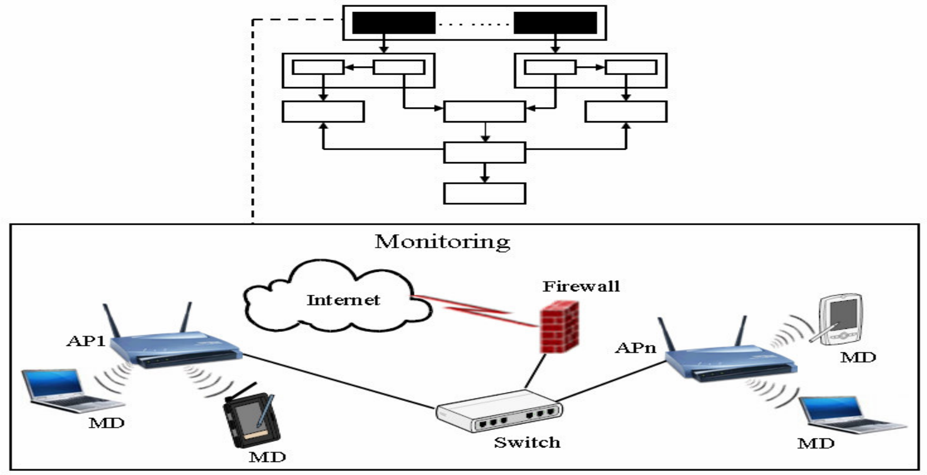

Figure 2. Traffic monitoring component

3.3 Logging

The CU component logs all the traffic monitored by the APs. Each AP has its own associated CU that logs the traffic passing through the AP. The CU logs the traffic in a log file as represented in figure 3. The log file is divided into separate storage areas with each storage area consisting of, for example, 1 Megabyte (1MB) of data. As traffic is being monitored from the AP and stored in a log file, the storage area of the log file becomes limited. Therefore, this component creates a block of data per several MBs, i.e. B1 in Figure 3 represents a block of data consisting of 4MBs, for example. A block is a fixed-size unit of data that is transferred together to permanent storage space, as described in the next section. For the purpose of this model, the logged traffic is the packets. Therefore, whenever this study refers to 'traffic', it means all the packets passing through the APs. Finally, the CU then send the accumulated blocks of data to the Evidence Store (ES) for analysis purposes and creates a hash per each block of data that is sent to the hashing storage for preservation purposes, as explained in the next section.

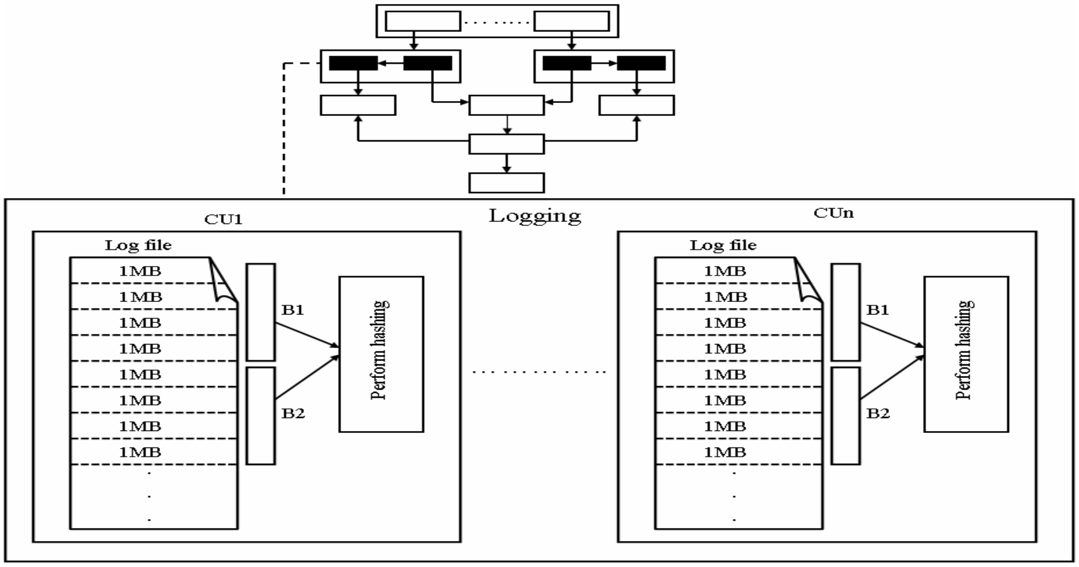

Figure 3. Logging component

3.4 Preservation of Logs

The primary goal of evidence preservation in WLANs is to ensure that absolutely no changes to the logged data have taken place since the data was collected [12]. Figure 4 demonstrates how the logs are being preserved in the proposed model. The Evidence Server (ES), as represented in figure 4, store all the blocks of data received from various CUs. In general, the ES act as a central storage of all the data monitored from 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 nth AP.

It is worth noting that, the data stored in the ES is needed only for analysis purposes. The 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 then transferred to the hashing storages represented as “HS of AP1” (Hashing Storage of AP1) and “HS of APn” (Hashing storage of APn) as represented in figure 4. There is a hashing storage for each AP on the WLAN. The H(B1AP1) in HS of AP1 shown in Figure 4 represents the hash value of the first block from the first AP, and H(B1APn) in HS of APn represents the hash of the first block from the nth AP and so on. The proposed model adopts the MD5 hashing technique. The MD5 hashing technique is not addressed in to detail in this paper since the focus is on forensic readiness, however, a detailed discussion of the MD5 hashing technique can be obtained in [12]. Hashing is described as a mathematical function that creates a unique fixed-length string from a message of any length [12]. 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, during a digital forensic investigation, the logged data on the ES has not been altered. This is a requirement of the digital forensic process [11].

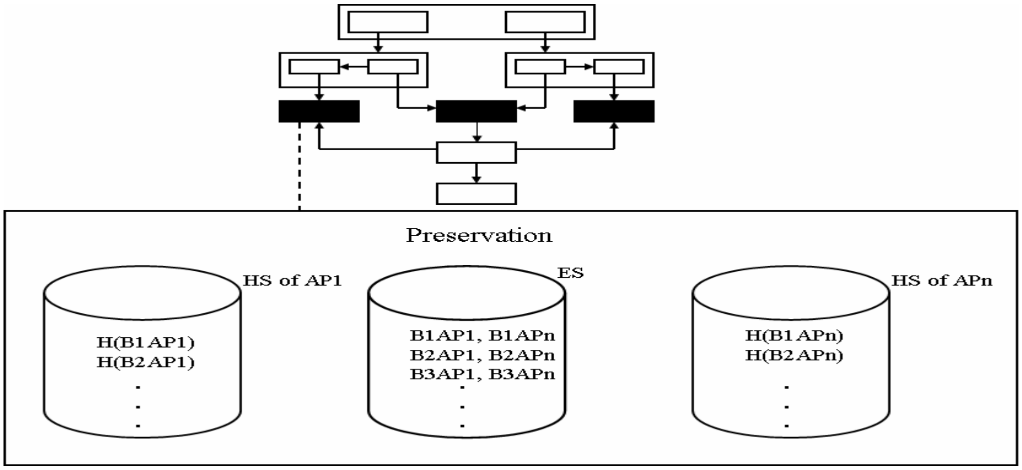

Figure 4. Preservation component

3.5 Analysis and reporting of logs

The main purpose of the analysis and reporting component is to mine and extract the data from the ES to come up with evidence that can associate a particular adversary with a criminal activity committed on the WLAN. The analysis component is the one responsible for mining data from the ES; however, it is not within the scope of this study to discuss data mining into details, but the use of data mining techniques should not be overlooked during the process of conducting a digital forensic investigation. The analysed data will then be passed to the reporting component.

The reporting component contains the final evidence of the entire digital forensic investigation. It is used by the cyber forensic experts when testifying in a court of law that an intruder was found to be guilty due to the evidence they posses from the investigation. It is then the decision of the prosecutor within a court to decide whether the intruder is guilty or not based on the evidence presented by the cyber forensic experts.

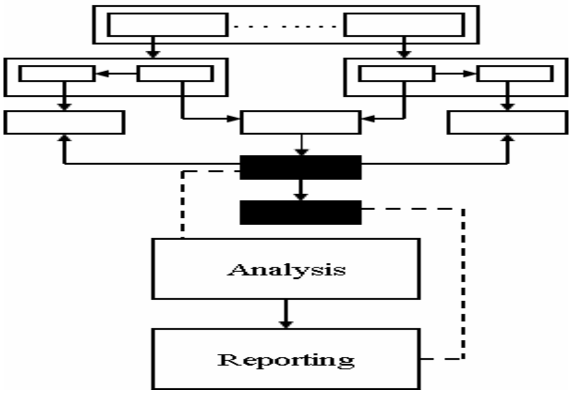

Figure 5. Analysis and reporting components

4 THE WFRM – PUTTING IT ALL TOGETHER

This section is devoted to the integration of the proposed model. The WFRM (see Figure 6) is depicted with all its components as explained above. These components show how wireless traffic is monitored in the WLAN, how the monitored traffic is logged, preserved and how it is stored for analysis purposes in order to render information that is forensically ready to be used by forensic experts. This section starts by providing a presentation where by all the components of the WFRM are integrated together. A detailed discussion of the proposed model is then presented, and lastly a discussion on the interception of communication or traffic monitoring related issued is presented.

The numbers from one to five represented with circles in figure 6 depicts the phases of the digital forensic processes.

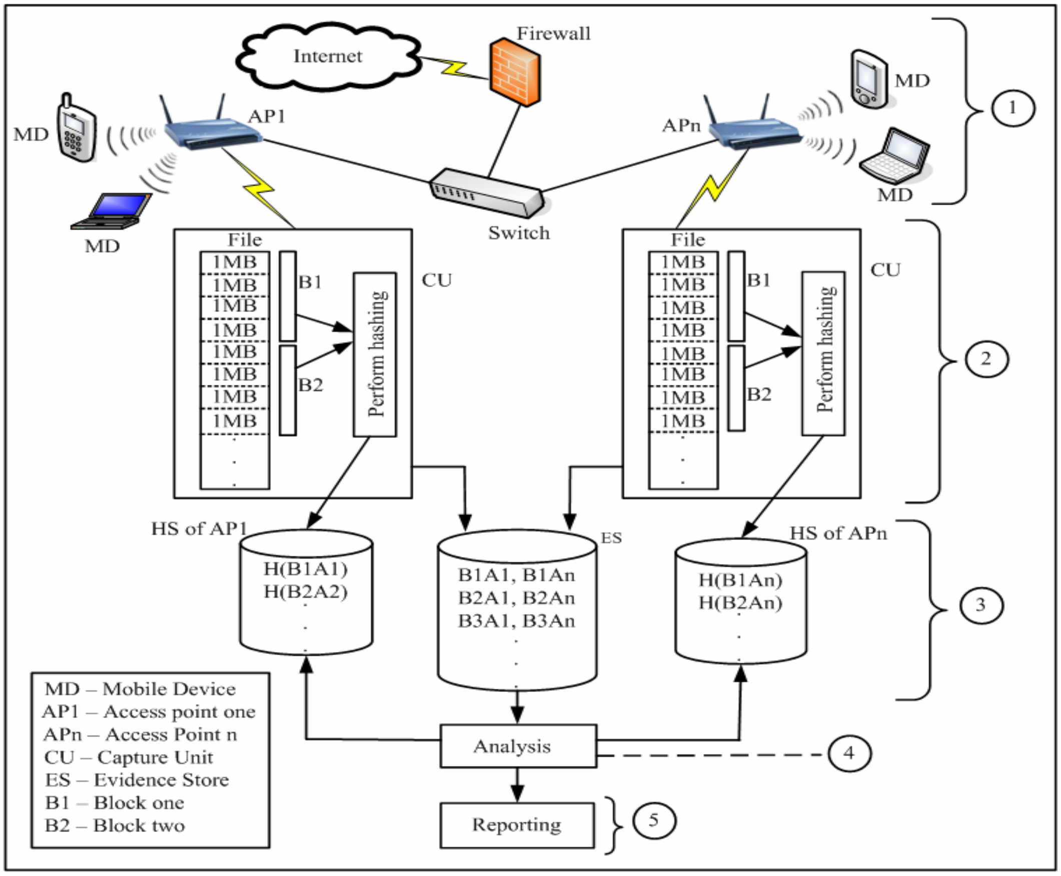

Figure 6. The Wireless Forensic Readiness Model (WFRM)

4.1 Integrating the WFRM components

Figure 6 shows all the components of the WFRM. The monitoring component indicates four mobile devices and two APs. Two of the MDs are connected to each AP. These MDs might be busy with internet access in a particular WLAN. This study assumes that the proposed model depicts a particular device deployed closer to the WLAN. This device has the capabilities of monitoring wireless traffic, logging the monitored traffic, preserving the traffic, and analysing the traffic. The component which 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 storage units of, say, 1MB. As the log file accumulates data, every fourth block, for example, are associated as a block of data. These blocks are then first transferred to the ES component. This study assumes that the ES is a sufficiently large mass storage device. Secondly, hashes of each of these blocks are created and transferred to the hashing storage. In this way the integrity of the data that flows through the WLAN is preserved.

Let's 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 just extract the data from the ES and do the analysis. The integrity of the analysed data can be proven by simply creating hash values of each block from where the evidence was extracted, and match that with the original hash values of each block as stored in the hashing storage. If the hashes match, it proves that the extracted evidence was, in fact, the original evidence, proving that the original evidence was not tampered with or manufactured.

4.2 Discussion of the WFRM

This section discusses the WFRM by outlining its advantages and disadvantages. This section then proceeds to discuss the traffic monitoring issues in a WLAN environment.

Once the traffic generated by the devices that connect to a WLAN has been monitored and preserved, it is ready to be analysed and used by cyber forensic experts to conduct the actual digital forensic investigation. Seeing that this information is forensically ready and forensically sound**,** the cyber experts' time and cost for 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 part of the digital forensic process, i.e. the monitoring, logging and preservation phases, have been completed. A disadvantage of the WFRM, however, may be the fact that the traffic monitored from the APs requires a large amount of storage, and this may prove to be expensive. However, the authors are not too concerned about this disadvantage since storage space becomes ever cheaper. Nevertheless, the authors are working on introducing compression on the WFRM as a mechanism to minimise the amount of storage required to log the entire stream of traffic that passes through the network.

It was mentioned earlier that one of the functions of the WFRM 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). The RICCA act, act No. 70 of 2002 [13], prohibits the interception of communication, however section 6(2)(bb) makes a provision that a person may intercept communication only for the purpose of investigation 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 given a prior consent in writing to the applicable law enforcement authorities.

Lastly, the authors are aware that the digital forensic process for FTK, EnCase and the WFRM as presented in Table 1 are logically more or less the same; however, this paper puts more emphasis on the design of a readiness model for wireless forensic purposes which comprise the somewhat different digital forensic phases of our model. Thus, the practical implementation if the digital forensic process employed by the proposed model is much different from that of conventional digital forensic process models of, for example, FTK and EnCase.

5 CONCLUSION

The most important issue addressed is this paper is that it is quite a challenge to conduct a digital forensic investigation in a WLAN environment. This is due to the fact that all the devices that participate in such an environment are mobile – therefore it becomes an enormous challenge to monitor and collect all the communications generated by these mobile devices and conduct a proper digital forensic investigation. WLANs are not forensically ready, as was suggested in this paper. In an attempt to solve this problem, this study proposed a WFRM that has the capability to monitor wireless traffic while these mobile devices are still connected to the wireless network. As discussed in this study, the monitoring, logging and preservation of the traffic was proposed.

Whilst the development of the proposed model, as a proof of concept, is still in an early stage, there are a number of areas that still need to be addressed as future work. The first of these is the effective storage constraints of the log files. As traffic is monitored from the APs and stored on the log files, the storage space of the log files will eventually be depleted, however, as mentioned in section 4.2, the authors proposed that, compressing the blocks of data while maintaining the integrity of the data might be a solution to this problem. The second area of future research includes that of analysis. It is understood that several approaches exists for analysing digital data in order to determine evidence for forensic purposes, however, a new approach still needs to be identified specifically to cater for the analysis of the potential large amounts of data gathered by the model proposed in this study. Lastly, this research will also investigate issues like infrastructure requirements as one of the requirements for forensic readiness, evidence admissibility requirements and evidence management with regards to the retention period of information logged by the ES.

6 REFERENCES

[1] Newman, R. (2007). *Computer Forensics, Evidence Collection and Management.* Auerbach Publications.

[2] Arthur, K., Olivier, M. & Venter, H.S. (2007). *Applying the Biba Integrity Model to Evidence Management*. IFIP International Conference on Digital Forensics.

[3] Rowlingson, R. (2004). *A Ten Step Process for Forensic Readiness*. International Journal of Digital Evidence, Vol. 2, Issue 3, pp1-5.

[4] Endicott-Popovsky, E., Frincke, D.A. & Taylor, C.A. (2007). *A Theoritical Framework for Organizational Network Forensic Readiness*. Journal of Computers, Vol.2, NO.3, pp1-11.

[5] ITU-T, (6 May 2008). *Technical Aspects of Lawful Interception*. Available from: http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000060001PDFE. (Accessed 26 November 2008).

[6] Peikari, C. & Fogie, S. (2003). *Wireless Maximum Security*. Sams Publishing, Indianapolis, Indiana, USA.

[7] Turnbull, B. & Slay, J. (2007). *Wireless Forensic Analysis Tools for use in the Electronic Evidence Collection Process*. Proceedings of the 40th Annual Hawaii International Conference on Systems Sciences (HICSS'07).

[8] Wireless LANs, (15 March 2004). *What is a Wireless LAN?*. Available from: http://www.wirelesslans.org/, (Accessed 20 October 2008).

[9] He, C. & Mitchell, J.C. (2005). *Security Analysis and Improvements for IEEE 802.11i*. The 12th Annual Network and Distributed Systems Security Symposium (NDSS'05), pp 90-110

[10] Tan, J. (2001). *Forensic Readiness*. The CanSecWest Computer Security Conference.

[11] Casey, E. (2007). *Handbook of Computer Crime Investigation, Forensic Tools and Technology*. Elsevier Academic Press, San Diego USA.

[12] Solomon, M.G., Barrett, D. & Broom, N. (2005). *Computer forensics, The Best First Step towards a Career in Computer Forensics*. SYBEX Inc, San Francisco, London.

[13] RICCA Act, (22 January 2002). *Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002*. Order No. 24286. Available from: http://www.info.gov.za/acts/2002/a70-02/, (Accessed 15 March 2009).

[14] Encase. (18 August 2008). The *Industry leading eDiscovery Solution*. Available from: http://www.guidancesoftware.com/ediscovery/index.aspx, (Accessed 05 April 2009).

[15] Forensic Toolkit. (10 July 2008). *Access Data, A pioneer in digital investigations since 1987*. Available from: http://www.accessdata.com/forensictoolkit.html, (Accessed 05 April 2009).