An Intelligent Wireless Forensic Model (IWFM) for moving devices between wireless networks.

S.J. Ngobeni and H.S. Venter

I. INTRODUCTION

There are currently many different types of wireless crime investigation tools designed for different purposes in order to track down intruders of wireless crime, like Intrusion Detection Systems (IDSs), Wlan-Jack, HotSpotter, Monkey Jack, TULP 2G, MOBILedit! Forensic, and Cell Seizure [1, 2]. These tools were designed for different purposes, but their main objective was to minimize wireless crime, however these tools have their own challenges. The main challenge about these tools is that they were not designed for digital forensic purposes and none of them indicate the movement of devices between wireless networks during digital forensic investigations therefore the acquired electronic evidence by these tools can not be used in a court of law for prosecution of the wireless perpetrators. The essence of this study is to develop an Intelligent Wireless Forensic Model (IWFM) for acquiring data for forensic purposes in the event that a device has moved from one wireless network to another.

The rest of this paper is organized as follows: section 2, background on wireless networks and digital forensics, section 3, discussion of our proposed model, section 4, conclusion, and section 5, references.

II. BACKGROUND

This section introduces some background concepts on wireless networks and digital forensics.

A. WIRELESS NETWORKS

Wireless networks refers to any system of transmitters and receivers that sends radio signals over the air, such as Wireless Fidelity (Wi-FI), World Interoperability for Microwave Access (WiMAX), Cellular networks, and satellite networks [1]. The main focus of this work is on Wi-Fi technologies which covers short distance of up 100m, and in reality, Wi-Fi is a network that complies with the 802.11 standards. This work will show how to conduct a wireless forensic investigation in a series of 802.11 wireless networks for forensic evidence that is admissible in a court of law.

B. DIGITAL FORENSICS

Digital forensics can be described as the act of scientifically derived and proven technical methods and tools towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of after-the-fact digital information derived from digital sources for the purpose of facilitating or furthering the reconstruction of events as forensic evidence [2]. Some authors define digital forensics as the scientific methodical investigatory techniques to solve crime cases, and relate the investigated crime to the courts of law [3, 4]. The field of digital forensics is new and was started in USA when the FBI establishes the Computer Analysis and Response Team (CART) in 1984.

III. THE INTELLIGENT WIRELESS FORENSIC MODEL

The IWFM has been developed to assist in the detection of perpetrators that move from one wireless network to another. This model assumes that a threat has occurred on a wireless network but the suspect is not known. The evidence store will show the pattern that was followed by every mobile device. The following diagram depicts the IWFM.

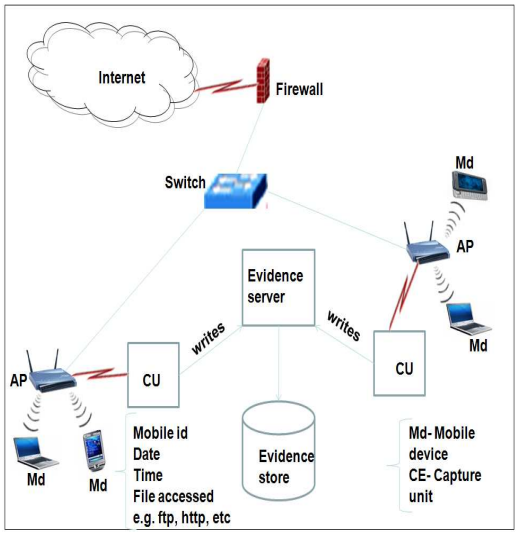

Fig.1. An Intelligent Wireless Forensic Model

The proposed model consists of three distinct components, which are:

- Capture Unit
- Evidence server
- Evidence store

A. CAPTURE UNIT

The purpose of this component is capturing the traffic from the access point, but for the purpose of this research we are only interested in the identity of the mobile device, the website that the mobile device had accessed, the date and time in which the incident occurred. Although the captured data is written to the evidence server, the captured unit must have its own storage to keep the acquired traffic so that it will be possible to trace back the original evidence [5].

There are two types of evidence acquisition methods according to Carrier [6], which are live and dead acquisitions. According to our model, live acquisition will occur when the capture unit acquires traffic when the mobile device is still connected to the Access Point (AP) or still online. For the purpose of dead acquisition, the forensic evidence will be acquired after the fact, when the machine is offline [7]. The evidence gathered through live acquisition is very descriptive however this type of evidence is known to have a lesser degree of trust associated with it. According to our proposed model, the capture unit works during live acquisition. Raya [8] proposed a system similar to the capture unit. This system is called DOMINO. It is used to detect greedy behaviour in IEEE 802.11hotspots. The following diagram depicts the DOMINO system.

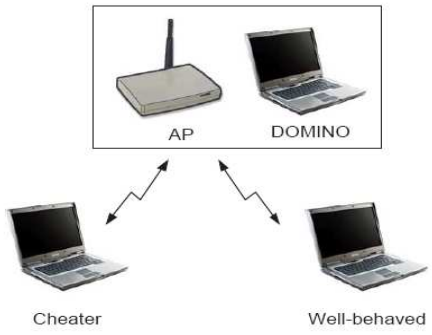

Fig.2. A DOMINO system for detecting greedy behaviour in IEEE 802.11 hotspots.

B. EVIDENCE SERVER

The purpose of the evidence sever is very simple. It sores the data acquired by the capture units from various APs. It classifies the data according to where it is coming from, i.e. from which capture unit belonging to which AP is the data coming from. It is of paramount importance that the data stored by the evidence server is immutable, in other words not a single file ever stored on the server may either be modified for it to be forensically sound. Another function of the evidence server is to do some comparing between the data coming from various APs to see if there is perhaps a match between this data. If any of the data matches, it means that each device was connected to one network and switched to another. This information is very important to be used in the court of law as forensic evidence.

C. EVIDENCE STORE

The evidence store act as a main database and keeps all data from the evidence server. The cyber inspectors will use this database to extract evidence that will be used in the court of law.

IV. CONCLUSION

The effective use of the evidence server to collect data from different capturing units belonging to different access points proves the positive benefits of this model to detect wireless devices that moves from one wireless network to another. The main drawback of this model is that, the capturing unit needs a large amount of storage to store all the traffic acquired from the access points and large storage may be expensive.

V. REFERENCES

[1]http://www.techweb.com/encyclopedia/define term.jhtml? term=wirelessnetwork

[2] B. Williamson, P. Apeldoorn, B. Cheam, M. McDonald, Forensic *Analysis of the Contents of Nokia Mobile Phones*, 2006, Pp 1-4.

[3] W.G. Kruse and J.G. Heiser, *Computer Forensics, Incident response essentials*, Addison-Wesley, Boston, 2001.

[4] M. Kohn, J.H.P. Eloff, M. Olivier, *Framework for a Digital Forensics Investigation*, Proceedings of the ISSA, from Insight to Foresight Conference, South Africa, July 2006.

[5] B. Carrier, *Defining Digital Forensics Examination & Analysis Tools*, Where Security & Business Intersect, 2002

[6] B.D. Carrier, *Risks of live digital forensic analysis*, Communication of the ACM, 2006, Pp 56-61.

[7] N. Adelstein, *Live Forensics: Diagnosing your system without killing it first*, Communication of the ACM, 2006, Pp 63-66.

[8] M. Raya, J.P. Hubaux, I. Aad, *DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots*, Laboratory of computer Communication Sciences and Applications (LCA), MobiSys '04, June 6-9, 2006