



Research Repository UCD

Title	Efficiency of Network Event logs as Admissible Digital Evidence
Authors(s)	Al-Mahrouqi, Aadil, Abdalla, Sameh, Kechadi, Tahar
Publication date	2015-07-30
Publication information	Al-Mahrouqi, Aadil, Sameh Abdalla, and Tahar Kechadi. "Efficiency of Network Event Logs as Admissible Digital Evidence," July 30, 2015. https://doi.org/10.1109/SAI.2015.7237305 .
Conference details	2015 Science and Information Conference, London, United Kingdom, 28-30 July 2015
Item record/more information	http://hdl.handle.net/10197/6481
Publisher's statement	© © 2015 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
Publisher's version (DOI)	10.1109/SAI.2015.7237305

Downloaded 2025-12-04 23:06:21

The UCD community has made this article openly available. Please share how this access benefits you. Your story matters! (@ucd_oa)



© Some rights reserved. For more information

Efficiency of Network Event logs as Admissible Digital Evidence

Aadil Al-Mahrouqi
School of Computer Science and
Informatics
University College Dublin
Dublin, Ireland
Email: aadil.al-mahrouqi@ucdconnect.ie

Sameh Abdalla
School of Computer Science and
Informatics
University College Dublin
Dublin, Ireland
Email: sameh@ucd.ie

Tahar Kechadi
School of Computer Science and
Informatics
University College Dublin
Dublin, Ireland
Email: tahar.kechadi@ucd.ie

Abstract—The large number of event logs generated in a typical network is increasingly becoming an obstacle for forensic investigators to analyze and use to detect and verify malicious activities. Research in the area of network forensics is trying to address the challenge of using network logs to reconstruct attack scenarios by proposing events correlation models. In this paper we introduce and examine a new network forensics model that makes network event-logs admissible in the court of law. The idea of our model is to collect available logs from connected network devices and then apply Support Vectors Machine (SVMs) in order to filter out anomaly intrusion, and re-route these logs to a central repository where a event-logs management functions are applied.

Keywords—SVMs; Network Evidence Admissibility; Evidence Reliability; Authentication of Evidence; Best Evidence

I. INTRODUCTION

In a traditional computer network there exists, a large number of event-logs generated daily by network devices (e.g., servers, switches, routers). A network event log is a record of a network's alerts and notifications. Once a cybercrime occurs, these event-logs can significantly contribute to the forensics investigation in question. However, these event-logs are generated individually based on the time of occurrence. In addition, these logs are large and therefore, analyzing them is a time consuming task for network administrators. With this in mind, the secure exportation and storage of these log files and events is crucial. Being able to store data from multiple sources and monitoring systems on a secured centralized platform is the beginning of data forensic analysis. The centralized event-logs repository can be used to integrate the event-logs that have been generated from different network devices. The central event-logs repository plays an essential role during network incidents and criminal investigation.

In most cybercrime cases, a single alert log does not contain sufficient information about malicious actions background and invisible network attackers. The information for a particular malicious action or attacker is often distributed among multiple alert logs and among multiple network devices. In addition, a single network event often generates a redundancy of similar event-logs that belong to the same class within a short time intervals. The large amount of redundancy logs makes it difficult to manage them during forensics investigation. Also, there is no standard event-logs format. There are different event-logs format generated by numerous network devices.

A Forensic investigator's ability to detect malicious activities and reconstruct incident scenarios is very complex, considering the number as well as the quality of these event-logs. In many cases, the attacker aims to compromise internal computer machine and maybe will start sending a fake message to the network administrators showing a problem on the compromised machine. The network forensics investigators will spend their time investigating fake messages while the attacker tries to reach and attack other network assets.

Typically, courts ask if the obtained evidence is the same as the originally seized digital information when considering whether evidence is admissible [3]. To prove that evidence is trustworthy, it is usually vital to prove to the courts that it was acquired from a specific network device, that an accurate copy of digital evidence was acquired, and that it has continued unchanged since it was recovered. The reliability of digital evidence plays an essential role in the authentication process [4].

Appropriate chain of custody explains that evidence was acquired from a specific network device, and that it was continuously controlled since it was recovered [4]. Thus, proper chain of custody documentation enables the court to link the evidence to the cybercrime. Incomplete documentation can result in misunderstanding over where the evidence was obtained and can increase suspicion about the trustworthiness of the evidence. On the other hand, the objective of a court is to administer justice, and the duty of forensics investigators in this case is to show supporting realities [1]. As such, courts rely on the trustworthiness of investigators and their ability to show evidence accurately; it is their responsibility to show results in a realistic way [2]. Moreover, courts are worried about the authenticity of the evidence they provide.

Individuals processing evidence must verify that, in addition to being relevant, evidence should meet specific standards to be admitted [3], [4], [5], [6].

The Irish Rules of Evidence was established to help evaluate evidence. For example, before admitting evidence, a court will normally guarantee that it is relevant and will assess it to determine if it is what its proponent claims [4]. An inability to guarantee that the evidence is relevant to the case from beginning may lead to evidence being excluded, possibly resulting in losing the case [4]. Although some judgments evaluate all computer-generated data as business-records under

TABLE I: Forensics Effective Evaluation (FEE) Result

s/n	FEE (Xm)	Changeable Variable		Impact Variable			Value FEE (Xm) Vm(Xm)
		Numbers of Nodes to Victim	Network Security Zoon	C	I	A	
1	FEE (X1)	6	2	0	0	1	1
2	FEE (X2)	6	2	1	0	0	1
3	FEE (X3)	6	2	1	1	1	3
4	FEE (X4)	6	2	1	1	1	3

the hearsay-rule, this approach may be inappropriate when a person was not involved. In fact, computer-generated data may not be considered hearsay at all because they do not contain human statements and neither do they assert a fact but simply document an act.

The Irish-law describes the difference between evidence that is PC-generated against that which is PC-stored [4]. The difference hinges upon whether a computer or a human created the records contents [7]. Digitally stored documents refer to records that contain the writings of individual or group of persons and happen to be in automated form. As with any witness evidence containing human statements, digitally stored records must comply with the hearsay rule. Moreover, digitally generated records cover the output of programs, untouched by human-hands. Unlike digitally-stored records, computer-generated records do not contain human statements but only the output of a computer-program designed to process input following a defined algorithm.

The evidence issue is no longer whether a human out-of-court statement was accurate (a question of hearsay), but instead whether the computer-program that generated the record was functioning properly (a question of authenticity). However, information that is related to humans regarding their accuracy, such as entries in a database that result from data provided by an individual, are covered under the business-record exception if they meet the above description. The remaining parts of this paper is organized as follows, section 2 outlines previous work. Sections 3 cover the proposed methodology with the purpose of generating admissible digital evidence. In this section, we propose two models, Network Forensics Correlation Model and Forensics Effective Evaluation Model. Section 4 presents simulation of a typical network infrastructure environment with the help of Graphical Network Simulator (GNS3), Virtual Box and VMware workstation. Finally, section 5 deals with the conclusion and some perspectives as future works.

II. PREVIOUS WORK

The purpose of this literature review is to provide an overview of the most relevant, previous research done in the legal laws that focus in digital evidence. In addition, we will cover the tools and technologies that have been used in a case study like tools (GNS-3, Virtual Box and VMware) and technologies (Honey net and Honeypot). The legal review is mainly focused on different primary areas: the admissibility, reliability, authentic of digital evidence and I will focus mainly in the Irish law. Moreover, the aim is to cover the simulation approach to simulate attack in GNS3, investigation process model to virtualize the interesting evidence by using and an attack and evidence graph.

The idea of admissibility is a simple one. The court is required to define whether evidence is safe to put before a jury

and will help deliver a strong foundation for making a decision in the particular case [8]. In practice, admissibility refers to a set of lawful tests carried out by a judge for forensic ally assess the finding evidence [9], [6]. This valuation procedure can become complex and difficult, mainly when the evidence was not controlled correctly nor has traits that make it less trustworthy, less-reliable or more-harmful. Some authorities have rules relating for admissibility that are formal inflexible, while other authorities give judges more discretion [12].

For example, two parties present copies of event-logs that could not be authenticated correctly. The magistrate judge would not admit the event-logs, noticing that it is unauthenticated. event-logs are a form of digitally-generated evidence that posture evidential issues. The judge summarizes five issues that must be considered when evaluating whether evidence will be admitted:

- Not unduly prejudicial
- Best evidence
- Not hearsay or admissible hearsay
- Authenticity
- Relevance

Although some of these issues may not be appropriate in certain cases, each must be considered [13]. Other issues that may prevent investigators from being admitted by courts are incorrect handling seizure and search [14].

The Best Evidence in Irish Court, whenever dealing with the contents of photograph, writing, or recording, courts occasionally need the original evidence [19], [5]. The original-evidence drive of this rule was to confirm that decisions made in court were founded on the best available information. With the advent of technology that can generate efficiently identical copies records became acceptable in place of the original, unless a genuine question is raised as to the authenticity of the original or the accuracy of the copy or under the circumstances it would be unfair to admit the copy in instead of the original.

Because an exact copy of most forms of evidence can be made, a copy record is generally acceptable. In fact, offering a copy of evidence is typically more eligible because it helps to eliminate the possibility of hazard that the original will be unintentionally changed. Even a paper printout of a computer-document may be considered as valid as the original unless significant parts of the original are not visible in printed process.

For instance, a printout of a document from Microsoft-Word does not display all of the information embedded within the original file such as notes. Although courts have been slightly permissive in the past on inappropriate handling of

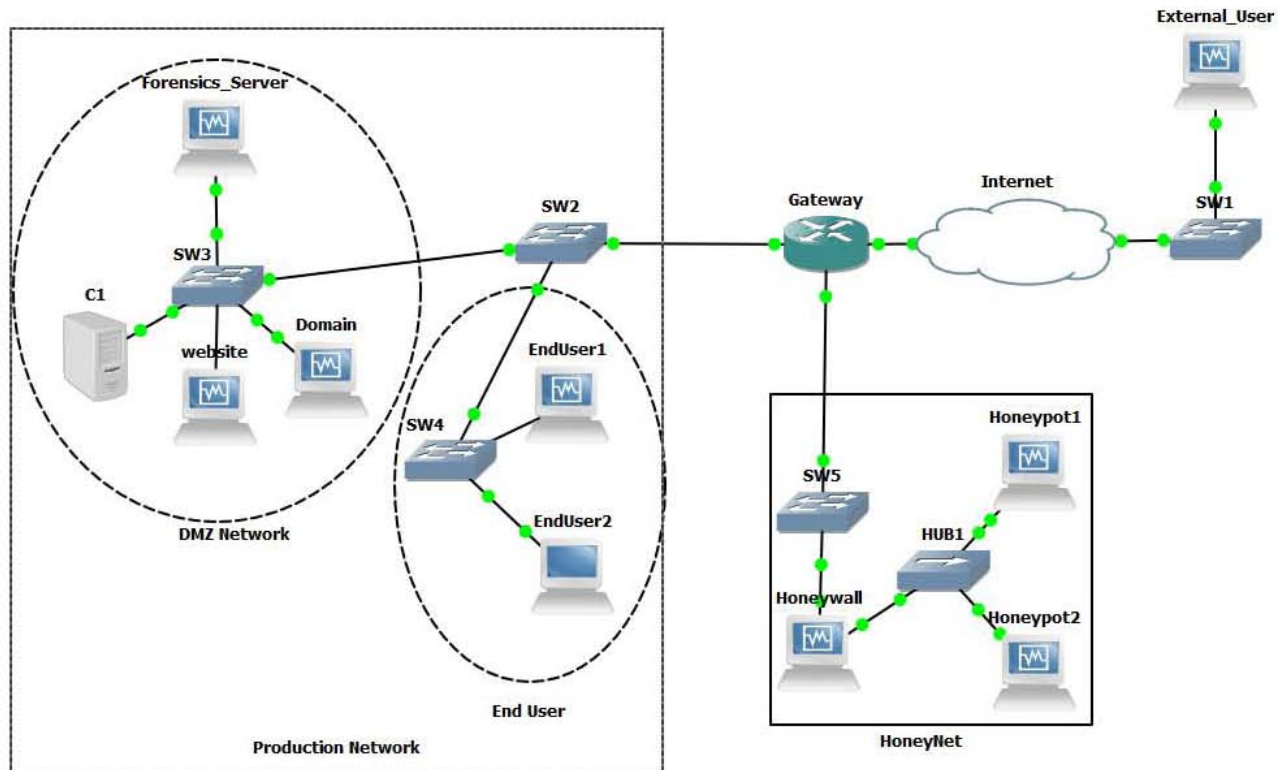


Fig. 1: Simulation Honeynet Network in GNS3

evidence, more challenges are being raised relating to evidence handling procedures as more lawyers become familiar with evidence. Courts are much less tolerant of unlawful seizure and search of evidence [15]. To authenticate evidence, it might also be essential to evaluate its reliability. There are two general methods to evaluating whether evidence can be trusted upon in court [16]. The first method is to focus on whether the device that generated the evidence was operative normally without any single issue, and the other method is to examine the actual evidence for manipulation [17].

In this research we simulated different cyber-attacks using GNS3 and other open source tools. In this attack scenario we used the idea of Honeynet network cyber-attacks trap. The Honeynet project is a non-profit volunteer organization of security professionals dedicated to computer security research and information sharing. They do this by deploying networks around the world to be hacked. In order to learn the tools, tactics, and motives of the blackhat community, and share the lessons learned. The goals of this project are to raise awareness of the threats that exist, to teach and inform about the threats, and to give organizations the capabilities to learn more on their own. The group informally began in April 1999 as the Wargames maillist. Over time, the group has grown, officially becoming the Honeynet Project in June 2000. The value of the project is totally Open Source, sharing all of their work, research and findings. Everything they capture is happening in the wild (there is no theory), made up of security professionals from around the world; they have no agenda, no employees, nor any product or service to sell [22].

The Honeynet is high interaction honeypot; it is an ar-

chitecture, not a product or software. Honeypot is a security resource who is value lies in being probed, attacked or compromised. Honeypots have a very simple design that brings with it many advantages. The real advantage of honeypots though is that they are designed to only interact with attackers. This way honeypots collect smaller set of data with a very high value. In addition, they can detect any new tools or technologies used by attackers. The most important and useful advantage is its simplicity, i.e. requires minimal resources. However, with advantages come disadvantages, and like all technologies, honeypots have a few. It can only track activity that interact with it. As other security technologies, honeypots are also at risk of being taken over by attackers and used to harm other systems. There are two types of honeypots, low interaction and high interaction. The main difference between the two is their complexity and interaction they allow an attacker. low interaction honeypots do not give attackers much control by emulating operating systems and other services. The main advantage of this is their simplicity that allows easy deployment and maintenance plus the low risk factor because they do not work with real production system. High-interaction honeypots differ in that they involve real operating system and applications. Unlike low-interaction, nothing is emulated. The advantage of this is that by giving attackers real systems to work with; they can capture a wide range of information and learn new techniques being used [22].

On the other hand, digital Forensics uses software tools to get the results and gain data bit-by-bit from memory dumps. A prerequisite forensics examination is necessary and for this process we will be using a selection of tools such as EnCase

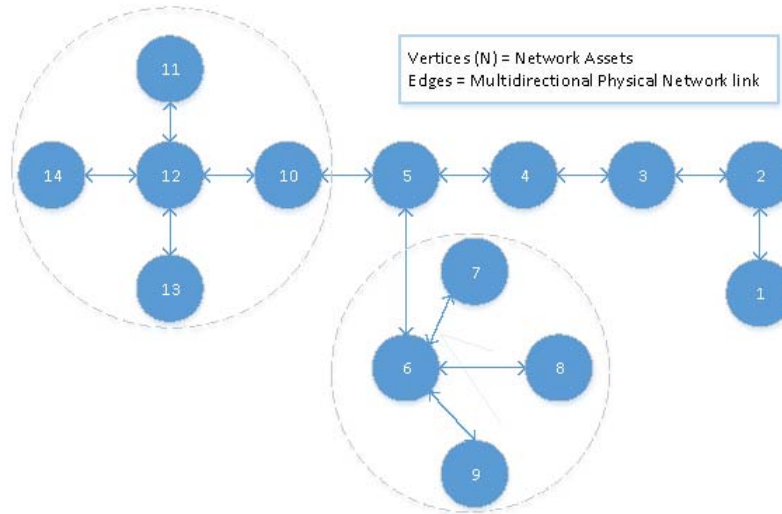


Fig. 2: Building Node Relationship

and Forensic Toolkit (FTK) to extract and integrate information for the investigation of the illegal activities using network infrastructure.

Acquisition of data imaging from the target network is both important and challenging. Procedures and standards must be verified during acquisition: acquisition of digital evidence, by its very nature, is fragile and can be alerted, damaged, or destroyed by improper handling or examination [24]. When data is identified from the network devices for acquisition purpose, the network forensics investigation should be conducted in a proper way in order to avoid any volatile information lost, network device locking or network power loss. The acquisition process in the network forensics different than other digital forensics laboratory, because forensics investigators dealing with volatile data.

TABLE II: Computer Security Threats

S/N	Symbol	Attack Name
1	FEE (X1)	Denial of Service (DOS)
2	FEE (X2)	Eavesdropping
3	FEE (X3)	Role Bypass
4	FEE (X4)	Authentication Bypass

Network forensics investigators deal with live devices in most investigation cases [25], and therefore network investigators can not power off network devices and bring them to a laboratory. Anti-forensics is defined as any attempt at compromising or destroying digital evidence according to the two forensics analysis methods [26]. Anti-forensics approaches are classified into several groups based on various techniques and tools. Dr. Marcus Rogers [27] proposed the most accepted subcategories of anti-forensics: data hiding, artifact wiping, trail obfuscation and attacks against the computer forensics processes and tools. After the illegal actions and attack activities, most of the professional attackers used anti-forensics to prevent proper digital forensics investigation processes that might be conducted. In addition, anti-forensics for networks have created major challenges. They use stealth and masking

for hiding any digital evidence from the victim network device. The memory in most network devices like routers and switches, contain volatile information that requires continuous power to retain.

The integrity of the data image must be examined during image processing of the victim devices. A hash function, such as md5sum or shasum for Linux, is the most common technique that is used to check the data integrity of the examined file. A hash function is a function that takes a relatively arbitrary amount of input and produces an output of fixed size [28]. The hash will change if any modifications occurs to the examined file. Consequently, hash functions are used to verify that no modifications have taken place acquiring the data.

We used different open source tools in order to built our network environment like GNS3, VirtualBox, VMware and other open source tools. GNS3 is a simulation tool and stand for Graphical Network simulators. GNS3 allows us to connect to VirtualBox virtual machines that are used to emulate different operating systems, e.g. Linux and Microsoft Windows. In addition, GNS3 allows the emulation of Cisco IOSs.

Rahman et al [21], proposed Developing Forensics Readiness Secure Network Architecture for wireless Body Area Network (WBAN). They used Additive Value Function (AVF) equation to validate their proposed architecture. In our research, we are explained the methodology that has been used in Forensics Effective Evaluation (FEE).

Wang et al proposed two anomaly intrusion detectors which are based on one-class SVM learning algorithm and kernel methods [30]. The experimental results shows that the proposed methods give better accuracy rate than Markov Chain anomaly and STIDE. Leandros [31] and all proposed a different approach to detect anomaly intrusion detection using one-class support vector machine (OCSVM). They proposed an integrated one-class support vector machine mechanism distributed in a supervisory control and data acquisition

(SCADA) network. The proposed model used to read the network data traffic, split traffic based on the source of the network packets and eventually creates a cluster of OCSVM models.

III. METHODOLOGY

Figure 4 shows Network Forensics Readiness and Security Awareness Framework. This framework contains fifteen different software and database blocks, these blocks work as single unit in order to forensically process and normalize the captured event-logs that have been discussed in [17]. In order to be able to generate an admissible forensics report to the court of Justice we have to clean our event-logs repository from any duplication and irrelevant information.

Figure 5 shows an update design of Admissible Network Forensics Correlation Model (ANFCM). The old version of this model has been discussed in [16]. The new update will focus on generating only admissible digital evidence. ANFCM is used to clean our evidence from any noise and un-wanted information. There are two important processes in this model, format standardization and redundancy management. The format standardization process aims to unify different event-logs format into one format, while the redundancy management process aims to reduce the duplication of the single event. The analysis data Engine has two functions format standardization and redundancy management. The proposed Admissible Network Forensics Correlation Model consists of all the processes and components required as listed in Table III.

In order to evaluate the development of the Network Forensics Readiness and Security Awareness Framework shown in figure /reffigure3 we used Additive Value Function (AVF). The AVF will convert all qualitative data generated from FIA, to quantitative data. After that, the quantitative data will be used to quantify the Network Security Effective Level (NSEL). The NSEL will be used to evaluate the development of impact level for the Network Forensics Readiness and Security Awareness Framework.

TABLE III: Admissible Network Forensics Correlation Requirement

No	Process	Component
1	Network Traffic Monitoring	Syslog, Nagios
2	logging the changing on Network	RANCID, Syslog
3	Preservation of Logs	Evidence Repository
4	Produce Report	Admissible Forensics Report

A. Forensics Effective Evaluation (FEE)

The Forensics Effective Evaluation (FEE) is a Network Forensics analysis mechanism to test and evaluate the influence of different attack threats. Basically, FIA experimental tests means to try different network attacks in target victim network systems. A set of the most popular network security threats were selected in these experiments. It shows four computer security threats. The FEE (Xm), FEE (X1), FEE (X2), FEE (X3), FEE (X4) refers to Attack, Denial of Service (DOS), Eavesdropping, Role Bypass and Authentication Bypass, respectively. Table IV shows the impact variables that have been used in FEE experiments.

B. Additive Value Function (AVF)

Rahman proposed Additive Value Function (AVF) used to convert all qualitative data that has generated from FEE forensics experimental testing to quantitative data. In 2009, a value-based software testing process was launched as a grading model to determine software testing priority ranking [18]. We used AVF in our research to determine which network malicious software testing processes are deemed as the most effective based on Quality Forensics Risk (QFR), testing costs and business importance set as variables [18]. In order to quantify the security impact level computer network, the (AVF) equation as shown in Equation 1 has been used in this research in order to quantify the security impact level on network:

$$V(X) = W_m x V_m(Ax) \quad (1)$$

- V(X) is the AVF
- V_m(Ax) is the total score of FEE (Ax)
- W_m, are a set of a positive weighting factor

As discussed earlier that the FEE have generated multiple inputs values. Consequently the AVF will be modified into additive multiple-objectives values function to include multiple variables, therefore:

$$V(X) = [W_1 X V_1(X_1)] + [W_2 X(X_2)] + [W_3 X V_3(X_3)] + [W_4 X V_4(X_4)] \quad (2)$$

Consequently, we get Equation 3:

$$V(X) = \sum [W_m x V_m(X_m)] \quad (3)$$

C. Forensics Impact Level (FIL)

In this section we presented the FIL. The FIL results consists of a set of attack experiments results that have been conducted in the target victims (network systems). The calculation of (FIL) for each FEE (X_m) presented in Table V.

D. Weighting Factor

According Qi Li and Ezell have a different approach of deciding the value for the weighting factor W_m [20]. However, in this research, the weighting factor W_m will be derived from the changeable variable measured during the FEE procedures. The changeable variables that have taken place are two, number of nodes between (attacker and victim) and the network security zone where the victim machine located.

IV. CASE STUDY

This section presents a simulated sandbox that allows us to perform experiment from our real assets and at low cost and risk. We proposed earlier Simulation SQL Injection Cyberattack using GNS3 [23]. Figure 1 shows the simulation of Honeynet Network and SQL injection attack. The idea of the case study is to examine the website that has been compromised by an SQL injection. We focus to forensically analysis and examine event-logs in order to reconstruct a cybercrime scenario that was previously observed. The aims

Fig. 3: Admissible Network Forensics Correlation Model

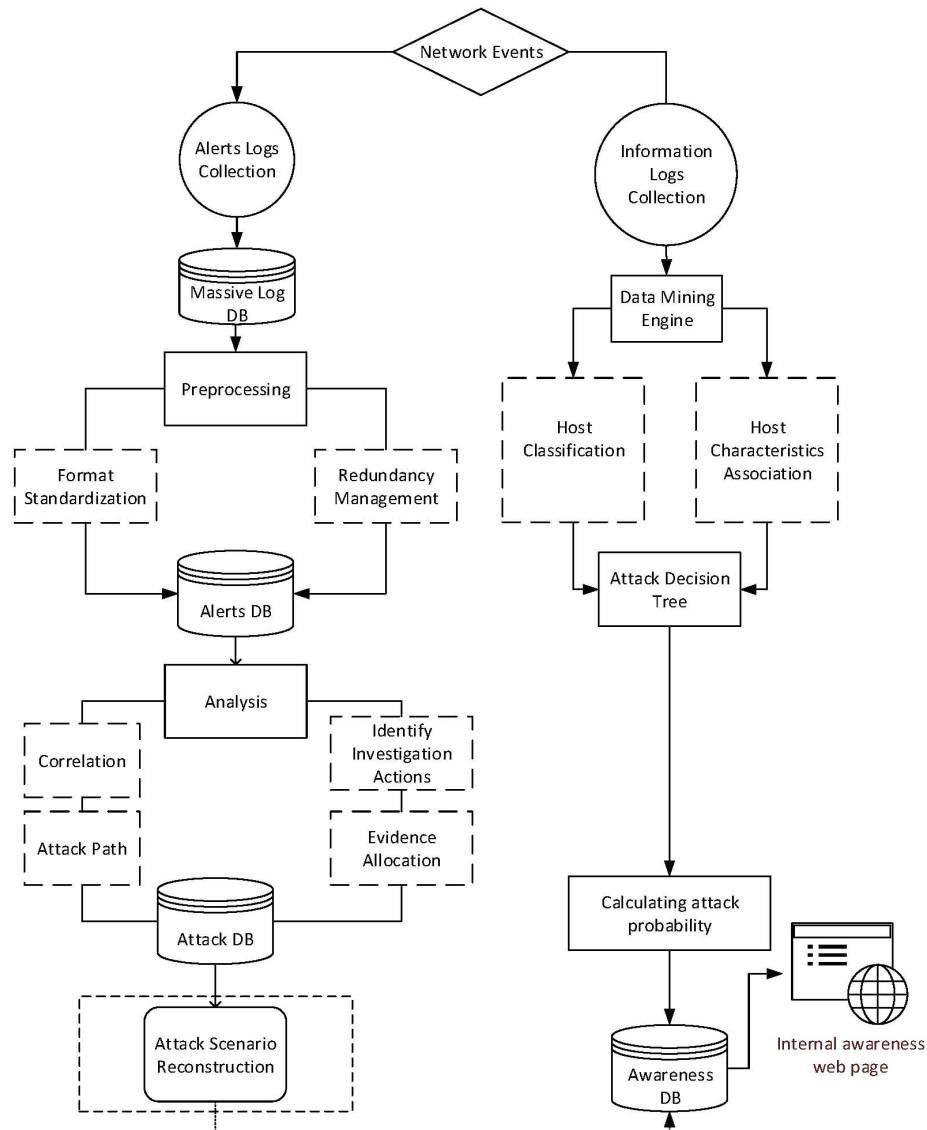


Fig. 4: Network Forensics Readiness and Security Awareness Framework

of this experiment is to graphically simulate an attack for low enforcement for instance court, jury and investigators. In addition, the simulation methodology tries to simplify the complicated attack scenario in the complex network topology. The outcome of this experiment can be used as a recommendation in a real IT infrastructure.

The case study discuss a network security incidence. International Bank website (<http://192.168.71.129>) has been compromised by an unknown attacker. The attacker used different techniques and tools to compromise the victim website such as SQL injection, XSS, Cach Breaking, Directory Traversal and breaking the local authentication login to the server. The question is how to plan and excute an investigation of such case? We used Graphical Network Simulator (GNS3) for simulate and configure a network environment based on

the case study, includes DMZ, Switches, Routers, etc. Also we used VirtualBox and VMware for simulates operating systems such as windows 2000, Backtrack, Kali, etc. Finally, we used wireshark forensics tool to detect criminal activity from network layer (OSI Layer 3). Also, we used two open sources tools(RANCID and Syslog).

RANCID (Really Awesome New Cisco Conflg Differ) is a network management application released under a BSD-style license. RANCID can monitor a network router's configuration files (hardware and software). RANCID does the following functions:

- 1- RANCID can access and monitor all network devices that have been listed in the router table (router.db).
- 2- It can email any configuration change to the forensics

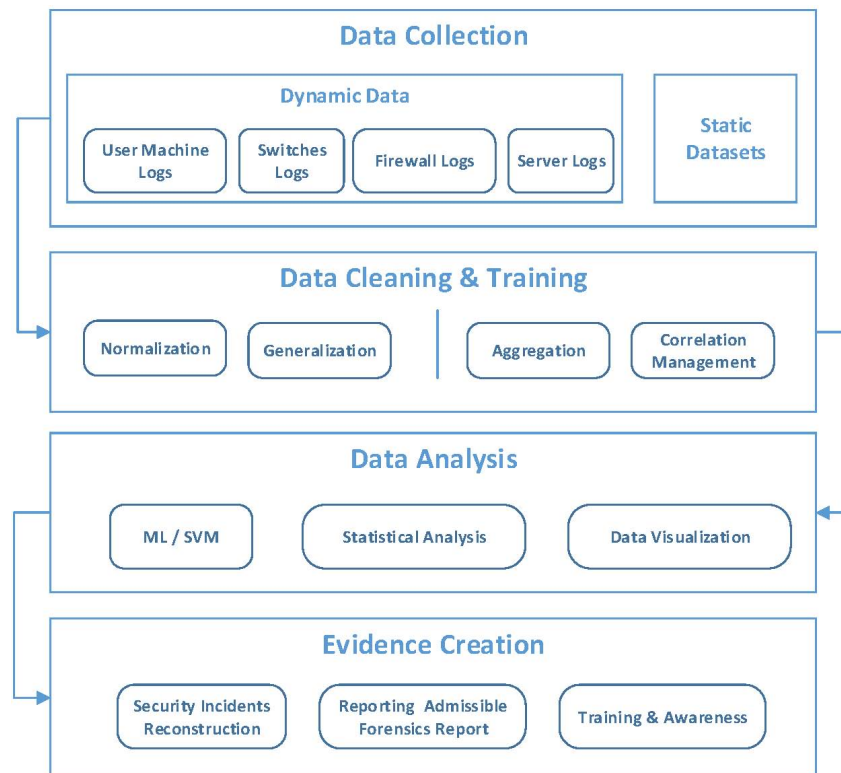


Fig. 5: Admissible Network Forensics Correlation Model

investigators or network administrators.

Syslog server is used to send event-logs to a logging server. It use the syslog protocol to send the event-logs. Syslog protocol is supported by many technologies from wide range of devices like (routers, switches, printers, etc.). The main difference between syslog server and SNMP, SNMP has abilities to ask a network device for information like available disk space. That is not possible in the syslog server scenario instead the network devices send logs entries to the centralized syslog server when events are triggered.

In short, there is no silver bullet solution. It is possible to safely store this data by restricting access with Access Control Lists (ACLs). Allows only certain trusted IPs ranges to log into the secure syslogs server via dedicated port numbers. The syslog uses the port number 514 so; we recommended to change the default port number to give more secure for login into syslog server. Furthermore, secure remote access to the server by using Secure Socket Layer (SSL) to encrypt the link between a server and client.

Figure 2 shows nodes relationship for the given case study scenario. After building the Network topology we will create an Adjacency Matrix based on the nodes relationship. The ones in the Adjacency Matrix shows the direct links between nodes while zero indicates no direct link between nodes in the network. The second stage of this approach is to create a Network Union Matrix. Network Union Matrix will try to substitute all zero values in the Adjacency Matrix with distances between one node to another [Source - Distance (link(n))] for example, [7- 1 (link(6))] and [1-2 (link(1))]. The third stage of this

approach is to create an Attack Pathway Detection. Sometimes the network investigators face difficulties in understanding the network infrastructure and the relationship between the victim node and others. The Attack Pathway Detection will try to utilise the Network Union Matrix as a road map for the investigation process to trace the source of the attack. The Network Union Matrix will list all distances between the victims node and other nodes. This will help examining all suspected nodes. The final step is recovering the remains from the suspected nodes which can be used as evidence.

V. CONCLUSION

This research proposed a full forensics methodology that is able to generate and obtains admissible digital evidence. The proposed models used to process and normalize the captured network event-logs. The output of the proposed model will store in the central event-logs repository. The main point of designing the model is to find a forensically way to collect and normalize the network event-logs that can be admissible in the court of justice.

The basis of any case relating evidence is appropriate evidence management. So, the practice of evaluating, saving and grabbing evidence must be routine. Courts might also consider whether evidence was changed before, during, or after gathering, and whether the procedure that produced the evidence is reliable enough. Methods to help formalize the procedure by which investigators allocate a level of certainty to conclusions that are based on evidence. Investigators might be requested to verify the reliability of the original evidence and the collection and examination procedures, and to assert that

TABLE IV: Attack Impact Variables

Impacts Variable	Security Three Pillars	Details
C	Confidentiality	The data only accessible by authorized users
I	Integrity	Protect the data accuracy, authenticity, reliability and completeness
A	Availability	The authorized user should able to access to the data when required.

TABLE V: The Final Result of Forensics Impact Level

s/n	PIA (Xm)	Changeable Variables		Vm (Xm)	Wm	Impact Level of FAA (Xm) V(Xm)
		Nodes to Victim	Network Security Zone			
1	FEE (X1)	6	2	1	4	$V(X1) = [W1 \times (X1)] = 4 \times 1 = 4$
2	FEE (X2)	6	2	1	4	$V(X1) = [W1 \times (X1)] = 4 \times 1 = 4$
3	FEE (X3)	6	2	3	4	$V(X1) = [W1 \times (X1)] = 4 \times 3 = 12$
4	FEE (X4)	6	2	3	4	$V(X1) = [W1 \times (X1)] = 4 \times 3 = 12$

they personally established the forensically preserved information and chain of custody. A realizing of direct versus indirect evidence, hearsay, and technical-evidence is essential to implement reliable conclusions and to protect those conclusions and the related evidence on the stand. An inability to understand these ideas can undermine an investigator testimony. Finally, investigators must prepare their conclusions to be used in court by non-specialist spectators.

The future work, to design and develop an automated tool to enable us to build an Adjacency Matrix that help digital investigators to better understand and visualize the structure of the victim network. In addition, this automated tool enable generate build a Forensics Investigators Graph that can summarize and document the procedures and steps carried out by forensics investigators based on the chain of custody.

ACKNOWLEDGMENT

The authors would like to acknowledge the support done by the Insight Centre for Data Analytics and UCD Centre for Cybersecurity and Cybercrime Investigation.

REFERENCES

- [1] Abbell, M. (2010). Obtaining Evidence Abroad in Criminal Cases 2010. Leiden: BRILL.
- [2] McIntyre O'Brien, R. (2014). The Current Status of Computer Hacking Offences in Ireland and their Application to the Internet. Master of Law. University College Cork.
- [3] Rishstatutebook.ie, (2014). Criminal Evidence Act, 1992. [online] Available at: <http://www.irishstatutebook.ie/1992/en/act/pub/0012/print.html> [Accessed 8 Dec. 2014].
- [4] McGuinness, C., T. P., McAuley, F., Shanley, M., O'Donnell, D., Byrne, R., Campbell, C., Drislane, S., Ni Chaoimh, G., Suibhne, B., Grady, J., Sadlier, G., Spooner, J., Eur, F. and Eur, C. (2014). Documentary and Electronic Evidence. 1st ed. [ebook] Dublin: law Reform Commission, pp.7-197. Available at: <http://www.lawreform.ie> [Accessed 8 Dec. 2014].
- [5] MC GRATH, P. (2014). WHITE COLLAR CRIME THE TRIAL PROCESS PROPOSALS FOR REFORM. [online] Dublin: The Constitution of Ireland, pp.3-20. Available at: https://www.dppireland.ie/filestore/documents/PAPER_-_Patrick_McGrath_BL_280511.pdf [Accessed 8 Dec. 2014].
- [6] Crime-scene-investigator.net, (2014). The Admissibility of Digital Evidence in Criminal Prosecutions. [online] Available at: <http://www.crime-scene-investigator.net/admissibilitydigitalevidencecriminalprosecutions.html> [Accessed 8 Dec. 2014].
- [7] INSA, F., Lazaro, C. and D'Inyestigation, E. (2014). The Admissibility of Electronic Evidence in Court. 1st ed. [ebook] Barcelona: Cybex, pp.25-42. Available at: <https://www.itu.int> [Accessed 8 Dec. 2014].
- [8] Marie Daly, Y. (2014). Unconstitutionally Obtained Evidence in Ireland: Protectionism, Deterrence and the Winds of Change. 1st ed. [ebook] Dublin: DCU Online Research Access Service, pp.1-19. Available at: http://doras.dcu.ie/4559/1/iclj_19_2_doras.pdf [Accessed 8 Dec. 2014].
- [9] Oireachtasdebates.oireachtas.ie, (2014). Seanad Eireann - 10/Dec/2008 Criminal law (Admissibility of Evidence) Bill 2008: Second Stage.. [online] Available at: <http://oireachtasdebates.oireachtas.ie> [Accessed 8 Dec. 2014].
- [11] Heffernan, L. (2014). POLICE ACCOUNTABILITY AND THE IRISH law OF EVIDENCE. 1st ed. [ebook] Dublin: Trinity College Dublin, pp.1-13. Available at: <http://www.tara.tcd.ie> [Accessed 8 Dec. 2014].
- [12] Peiris, C. (2014). The Admissibility of Evidence Obtained Illegally: A Comparative Analysis. 1st ed. [ebook] Sir Lanka: University of Colombo, Sir Lanka, pp.309-344. Available at: http://file:///C:/Users/cisco/Downloads/v13n2_G.L.%20Peiris.pdf [Accessed 8 Dec. 2014].
- [13] Awreform.ie. (2000). THE RULE AGAINST HEARSAY. CHAPTER 1 THE PRESENT law. one (1), P 1-248
- [14] rishbarrister.com, (2014). [online] Available at: <http://irishbarrister.com/defamation.html> [Accessed 8 Dec. 2014].
- [15] Ni Shuilleabhain, M. (2014). Legalisation of Public Documents within the EU Member States. 1st ed. [ebook] Dublin: University College Dublin, pp.1-47. Available at: http://ec.europa.eu/civiljustice/news/docs/study_public_docs_ireland.pdf [Accessed 8 Dec. 2014].
- [16] A. S. Al-Mahrouqi, S. Abdalla and T. Kechadi, e-Government Network Forensics Correlation Model, QScience , Doha, Qatar, 2014.
- [17] A. S. Al-Mahrouqi, S. Abdalla and T. Kechadi, Network Forensics Readiness and Security Awareness Framework, Annaba, Algeria, 2014.
- [18] Q.Li, "Using Additive Multiple Objective Value Function for Value Based Software Testing Prioritization". University of Southern California Computer Science Department. (2009), URL: <http://css.usc.edu/csse/TECHRPTS/2009/usc../usc-csse-2009-516.pdf>.
- [19] B. C. Ezell, "Infrastructure Vulnerability Assessment Model (I-VAM), (2007), URL: <http://create.usc.edu/assets/pdf/51834.pdf>.
- [20] A. F. A. Rahman and R. Ahmad, Hybrid Method to Measure Vulnerability in Wireless Body Area Network, Proceedings of the 6th International Conference on Sensor AsiaSense, (2013) August 23-25, Malacca, Malaysia
- [21] A. F. A. Rahman and R. Ahmed, "Developing Forensic Readiness secure Network Architecture for Wireless Body Area Network (WBAN)", International Journal of Security and its Applications, Vol.8., No.5, page 403-420.
- [22] J. Haas and L. Spitzner, "The Honeynet Project Latest Advances", URL: <http://www.honeynet.org>
- [23] A. S. Al-Mahrouqi, S. Abdalla and T. Kechadi, Simulating SQL-Injection Cyberattacks using GNS3, International Journal of Computer Theory and Engineering, ISSN:1793-8201, www.ijcte.org, 2015.
- [24] J. Ashcroft, D. J. Daniels, and S. V. Hart. Forensics examination of digital evidence: Guide for law enforcement. In U.S. Department of Justice, 1999.
- [25] A. E.-C. W. Group and 7safe. Good practice guide for computer-based electronic evidence. In England Wales and N Ireland, 2007.

- [26] R. Harris. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. In *The International Journal of Digital Forensics and Incident Response*, pages (44-49), 2006.
- [27] M. Rogers. Anti-forensics. In presented at Lockheed Martin, San Diego, pages (221-224), 2005.
- [28] J. E. Silva. *Giac security essentials practical*. In SANS Institute InfoSec Reading Room, 2003.
- [30] Wang, Y.; Wong, J.; Miner, A., Anomaly intrusion detection using one class SVM, *Information Assurance Workshop*, 2004. Proceedings from the Fifth Annual IEEE SMC , vol., no., pp.(358-364), 10-11 June 2004.
- [31] Mahlaras, leandros A., Jianmin Jiang, and Tiago Cruz. "Integrated OCSVM mechanism for intrusion detection in SCADA systems. *Electronics Letters* 50.25 (2014): 1935-1936.