Guidelines for Procedures of a Harmonised Digital Forensic Process in Network Forensics

George Sibiya
Meraka Institute
Council for Scientific and Industrial Research (CSIR)
Pretoria, RSA
gsibiya@csir.co.za

H.S. Venter
Department of Computer Science
University of Pretoria
Pretoria, South Africa
hsventer@cs.up.ac.za

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

Thomas Fogwill
Meraka Institute
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
tfogwill@csir.co.za

***Abstract* — Cloud computing is a new computing paradigm that presents fresh research issues in the field of digital forensics. Cloud computing builds upon virtualisation technologies and is distributed in nature. Depending on its implementation, the cloud can span across numerous countries. Its distributed nature and virtualisation introduces digital forensic research issues that include among others difficulty in identifying and collecting forensically sound evidence. Even if the evidence may be identified and essential tools for collecting the evidence are acquired, it may be illegal to access computer data residing beyond the jurisdiction of a forensic investigator. The investigator needs to acquire a search warrant that can be executed in a specific foreign country – which may not be a single country due to the distributed nature of the cloud. Obtaining warrants for numerous countries at once may be costly and time consuming. Some countries may also fail to comply with the demands of cloud forensics. Since the field of digital forensics is itself still in its infancy, it lacks standardised forensic processes and procedures. Thus, digital forensic investigators are able to collect evidence, but often fail in following a valid investigation process that is acceptable in a court of law. In addressing digital forensic issues such as the above, the authors are writing a series of papers that are aimed at providing guidelines for digital forensic procedures in a cloud environment. Live forensics and network forensics constitute an integral part of cloud forensics. A paper that deals with guidelines for digital forensic procedures in live forensics was submitted elsewhere. The current paper is therefore the second in a series where the authors propose and present guidelines for digital forensic procedures in network forensics. The authors eventually aim to have guidelines for digital forensic procedures in a cloud environment as the last paper in the series.**

Keywords*: component; network forensics; procedures and processes; cloud computing*

I. INTRODUCTION

Computer crime has been a challenge since the dawn of the Internet. In most cases perpetrators are successful in breaking security, it is impossible for a system to be 100% secure. All systems are prone to security breach, no matter how strong the security mechanisms that are in place. Whenever such incidences occur, the services of digital forensic investigators are required. The ability of digital forensic investigators to perform their function is heavily reliant on their ability to acquire digital evidence from computer systems and network devices. Unfortunately, computer system technologies are changing constantly, which has a direct impact on the ability of forensic investigators to identify and acquire digital evidence.

This problem arises from the fact that new technologies in computer systems come with new data storage formats and storage locations that differ from the ordinary formats and locations with which digital forensic investigators have been accustomed. Criminals are constantly studying systems and developing new techniques to break into the latest systems, software products and patches. Digital forensic investigators, on the other hand, struggle to keep up with new developments in technology.

This paper is one of a series of papers that aim to provide guidelines for digital forensic procedures in the cloud. The first paper that focuses on live digital forensics has been completed and submitted. The current paper focuses on digital forensic procedures in network forensics.

The paper is organised as follows: Section II provides a brief background on network forensics, followed by a discussion of the harmonised digital forensic process and challenges that exist in network forensics. In Section III the authors present the proposed digital forensic procedures for network forensics. Section IV concludes the paper and also presents future work.

II. BACKGROUND

The authors' ultimate goal is to study digital forensics in a cloud computing environment. Cloud computing is a new computing paradigm that builds upon virtualisation technology to provide infrastructure, platform and software as services [1–3]. Cloud computing presents challenges to digital forensic investigators due to its virtualised and distributed nature. The goal therefore is to provide guidelines for digital forensic procedures and to provide a digital forensic solution in the cloud. The current paper focuses on digital forensic procedures for a network environment. Network forensic procedures form part of the procedures that need to be carried out in a cloud environment.

In this section, the authors present a brief background on network forensics and network forensic challenges. The

authors also present the harmonised digital forensic process on which the procedures presented in this paper are based.

A. Network Forensics

A number of different network types exist these days, but they all originate from two basic ones: Local Area Networks (LANs) and Wide Area Networks (WANs) [4]. These networks can also be deployed as wireless networks (e.g. WLAN), wired networks (e.g. Ethernet) and virtual networks (e.g. connection among virtual machines). In the context of cloud forensics, the network layer is a fertile ground from which digital evidence can be collected as all communications with cloud services occur via a local network or a wide area network (e.g. Internet). Digital evidence or data that can be obtained from the network may include the source and destination address of any communication, as well as the data (Internet Protocol (IP) packets) that is transmitted during the communication session itself.

There are various key locations in the network from which such data can be captured and stored. These locations include network routers, firewalls and even workstations or network accessing devices. Information collected from these locations can be used for subsequent digital forensic purposes, if there exists a case.

The field of network forensics, one of the forensics fields, is still in the limelight as a new emerging area of academic interest. Traditional computer forensics generally involves data acquisition from a storage medium such as a hard drive, while network forensics encompasses the capture, recording and analysis of network traffic that can be used for digital forensics purposes [5]. To conduct network forensics, especially in a cloud computing environment, one would need to follow a standardised digital forensic procedure; however, currently there is no such procedure. It is for this reason that the authors propose guidelines for a harmonised digital forensic process that would be applicable in the cloud computing environment.

B. Network Forensic Challenges

Network forensics presents a number of challenges. One common identifiable challenge is that generally there is only one opportunity to collect network traffic as it traverses the network. Hence, inadequate digital evidence collection may result in the loss of vital digital evidence that may not be recoverable. Also, since networks communicate data before transmission takes place, it becomes a challenge to reconstruct the large number of packet pieces to obtain its original form. Furthermore, network traffic comprises of various protocols and media types, which in turn add complexity to the already complicated source of digital evidence [6].

Fortunately, quite a number of tools have been designed to capture and analyse network traffic. As most of them were intended for network troubleshooting and identifying problems in a network instead of digital evidence processing, they have specific shortcomings from a network forensics point of view [7].

Another challenge that face forensic investigator while carrying out forensic investigations in a network environment is a lack of standardised procedures. There are efforts by other researchers [8–10] aimed at standardising network forensic procedures but they leave a lot to be desired. In the next section we present a harmonised digital forensic process on which the procedures proposed in this paper are based.

C. Harmonised digital forensics process

The harmonised digital forensics process is presented in ISO/IEC 27043 draft standard [11]. It comprises of eleven phases, i.e. planning; preparation; incident detection; first response; incident scene documentation; potential evidence identification; evidence collection; evidence storage; analysis, and presentation. In addition to the eleven phases shown in Figure 1, six actions run in parallel with these phases, namely obtaining authorisation, documentation, information flow, preserving the chain of evidence and interaction with physical evidence.

In variance to the harmonised digital forensics procedures for network forensics proposed in [11], we consider and adjust only the first ten phases of the process in this paper. The presentation phase (the last phase) does not differ in network forensics and can be carried out as described in [11].

In the next section the authors present in detail the procedures that need to be carried out when conducting a digital forensics investigation in a network.

III. NETWORK FORENSIC PROCEDURES

Procedures presented in this paper are a sequence of activities that need to be carried out in their presented order to accomplish each phase of the digital forensic process. A lack of standardised forensic procedures leads to lack of confidence in an investigation being carried out [12]. In a worst-case scenario this increases the chances of evidence being thrown out of court or being not admissible at a hearing. We therefore address this issue by proposing procedures that can be used to conduct a successful investigation in a network environment. The procedures are depicted in Figure 1 as well as presented in the sections that follow. Each subsection contains a brief description of a harmonised digital forensics process phase. This is then followed by a bulleted list of the more specific digital forensic procedures.

D. Incident detection phase

This phase deals with the actual occurrence of an incident that requires forensic investigation. It comprises only one action, namely the reporting of an incident.

- **Incident reporting.** This action involves notifying the forensic team of the incident. Network engineers are usually the ones who first observe or receive notifications from network tools such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). They then relay the message to a forensic team. Network engineers may also be trained and authorised to perform the first response actions of an investigation.

E. First response phase

This phase deals with the restoration of a system or a network to an operational state while preventing future attacks [13]. The first group of people to respond to the scene is the incident handlers in a forensic team [9]. Mechanisms are also put in place by means of which evidence can be collected while the network is operational.

- **Enable secure logging.** It is very important that all the actions performed in an incident scene should be securely logged. The default logging systems in a network may not be standardised and therefore may be hard to read. Default logs are also vulnerable to being manipulated during an attack. These issues can be averted by investigators having their own standardised secure logging mechanisms.
- **Attack classification.** This action deals with categorising the type of attack in the incident scene. Categorisation may include whether it is an on-going attack or whether it has halted. Attacks can also be classified as passive, active or intrusive active attacks [14]. A passive attack is when an attacker eavesdrops a communication between two network nodes. In an active attack the attacker impersonates one of the active nodes on a network, while in an intrusive active attack the attacker gains unauthorised access to resources in a network. Each of these attack categories requires specific actions to be taken at an incident scene. Attacks may also be classified as presented in [15].

F. Planning phase

In an organisation this phase may be initiated by the executive establishing a digital forensics team. If the forensic services are outsourced, an already existing digital forensics team(s) may already be in place. The activities carried out in the planning phases are as follows:

- **Forensic Team Organisation.** As proposed in [9], the forensic team should comprise of investigators, IT professionals and incident handlers. Incident handlers are the first to respond when an incident has occurred. They are the ones who carry out the initial activities of an investigation such as categorising the type of attack. Investigators in the forensic team may comprise of legal advisors and members of the human resources department. The investigators usually oversee the investigation process – from when the suspected criminal incident occurred through to the conclusion of the case. They use different forensic tools and techniques to carry out their duties. IT professionals assist the investigators by using appropriate tools and sometimes their privileges on the systems being investigated to acquire evidence.
- **Identification of state-of-the-art network types.** In each network implementation, network devices vary. Hence, the locations from which evidence can be collected also vary. An advantage with computer networks is that they do not evolve as often as computer systems. That is, computer networks usually outlive the devices and computer systems (e.g. Operating Systems) connected to them. This means that forensic tools and techniques used for computer networks can be used for longer periods than the forensic tools used for other types of forensics, such as RAM forensics. After a forensic team has been established, there is still a need for the team to do research on existing network types and implementations.
- **Identification of potential sources of evidence in each network type.** The location of potential evidence may vary with each network type and implementation. In a private virtual network (VPN), an edge router can be the key point for collecting evidence as it can be configured to log all communications or to forward packets to a server to be dumped [16]. If a computer is connected through a modem to a wireless internet service provider, locations from where potential evidence can be collected differ widely. After categorising network types and implementations, it is therefore important that the digital forensic team should identify such locations and technologies used from where potential evidence can be collected.
- **Development of specifications or requirements for evidence collection tools.** For each network type and implementation there are specific requirements for forensic tools that can be used to acquire evidence. These specifications are informed by the technologies used in those networks. If, for example, a network cannot be reached physically (such as virtual networks), a forensic tool used needs to support remote connectivity. These specifications can be developed after a careful study of existing networks and locations (virtual routers, virtual switches, etc.) from which evidence can be collected.

G. Preparation phase

In this phase the forensic team prepares for the occurrence of an incident that would require a forensic investigation. It comprises of three activities to be performed, namely the development of forensic policies, the acquisition of digital forensic tools and/or the design and development of digital forensic tools.

- **Forensic policies and guidelines development.** Forensic policies deal mainly with the responsibilities of a forensic team, such as what aspect(s) of a forensic investigation should be handled by which personnel. Not everyone in the forensics team may be allowed to monitor communications in an organisation [9]. Data transmitted over a network includes confidential information such as passwords and banking information. Such information needs to be handled carefully and protected at all costs, so that it does not land in unsafe hands. Based on the information gathered in the planning phase (such as evidence location and type of evidence that may be contained), the policies are developed and responsibilities for aspects of the evidence allocated.
- **Digital forensic tools acquisition.** Based on the requirements specified in the planning phase, a set of tools that meet the requirements is acquired. These tools may include the ones that the forensic team may already have in

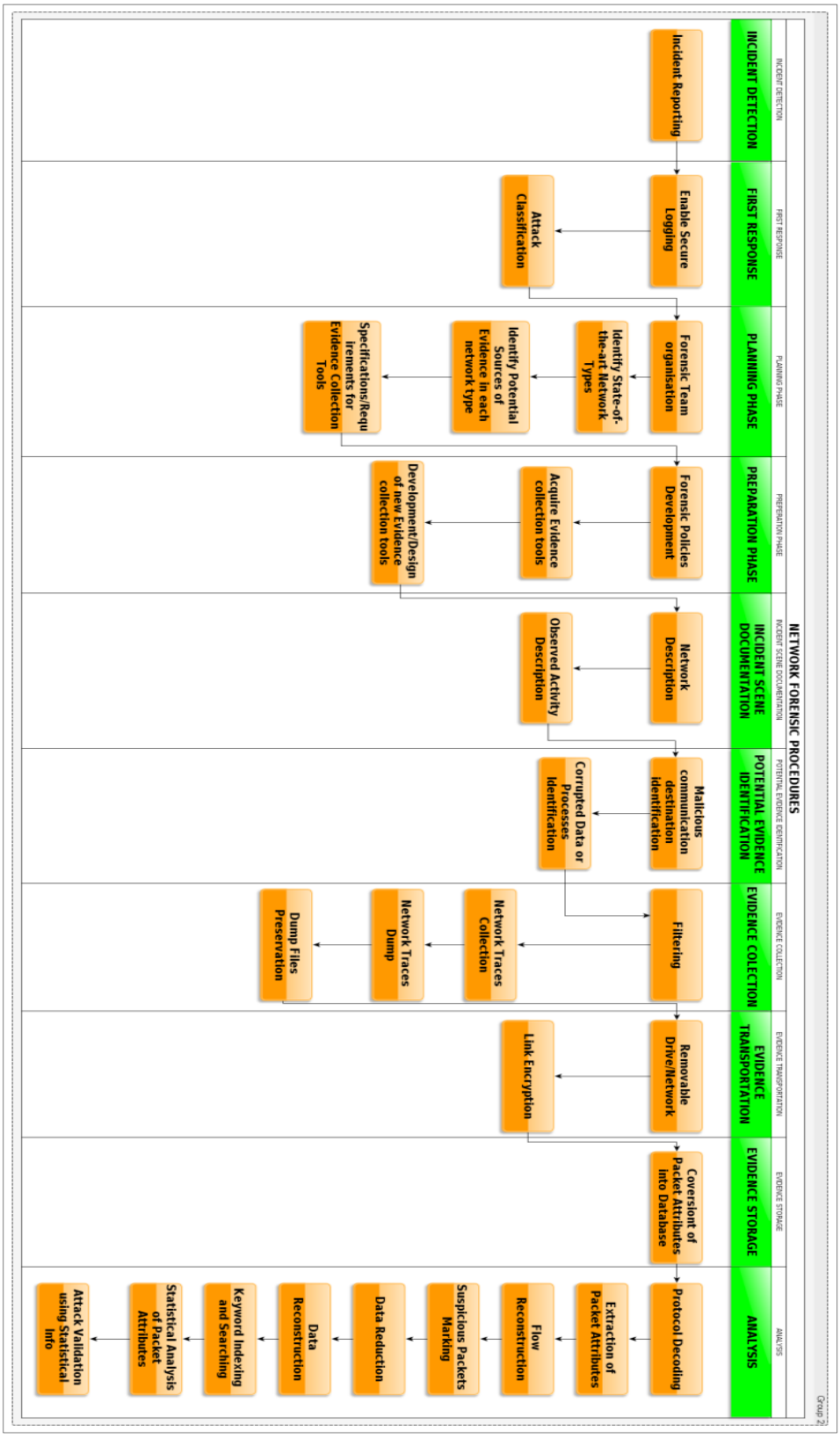

Figure 1: Harmonised digital forensics process in network forensics

their collection. Those not in their collection yet may be purchased.

- **Development/Design of new digital forensic tools.** Digital forensic tools that meet requirements may be neither available in the collections of the forensic teams nor for purchase. If that is the case, the forensic team needs to make use of its IT professionals to design and develop new tools. Such services may be outsourced with requirements specified.

H. Incident scene documentation

This phase deals with documentation of the incident scene. The documented information will include description of the topology and tools used in the network that has been attacked or under attack. This can be achieved with assistance of a network engineer from the organisation being investigated. If the attack is on-going, other information to be documented is the observed network behaviour that is raising suspicions.

- **Describing the network.** Unlike other incident scenes that may be photographed as part of documentation, a network cannot be photographed. The documentation may only contain transcripts such as a description of the network topology and the network tools and technologies used in the network. Even though in most cases incident scene documentation is useful in the final phases of an investigation, it can also be used in the evidence identification phases. This is because information documented include the network structure and network devices used, which may contain evidence.
- **Describing observed activity.** This involves describing the observed suspicious activity in the network. The descriptions include reports sent by IDS and IPS, and the network congestions observed by network administrators.

I. Potential evidence identification

Since data in transit in a network may be extremely large, it is important that key points and segments of the network that are of interest to the investigators be identified. This helps in minimising the amount of data to be handled by focusing only on the relevant data. Identification of potential evidence may be informed by the information gathered in the planning phase.

- **Malicious communication destination.** An attack in a network involves communications that are destined to a local host or a number of local hosts. These destination hosts are a rich source of evidence.
- **Corrupted data or processes.** After identifying the hosts, the corrupted data or running processes that result from the attack have to be identified.

J. Evidence collection

This phase deals with the actual collection of evidence from an incident scene and other locations that may be linked to an activity being investigated in a crime scene. Best practice [17] needs to be ensured. The three procedural actions taken in network forensics are as follows:

- **Filtering.** Traffic generated in a network involves a very large amount of data. If all such data would be collected by forensic investigators, it would be very hard to store and analyse. Filtering involves the examination of the data to decide which can be used as evidence [9]. This action may also help identify other locations of interest from which evidence can be acquired.
- **Network traces collection.** This action involves the application of forensic tools and techniques to carve network traces from identified locations. If the incident scene involves an on-going attack, this action may include monitoring network communications and dumping the IP packets using available tools.
- **Dump files preservation**. This action involves calculating the HASH signatures as a means to preserve their integrity. The signatures may be verified in each subsequent phase of the digital forensic investigation.

K. Evidence transportation

Once the evidence has been collected, it has to be transported. The transportation media may be over a secured network link. If the evidence were to be saved in physical storage media, the transportation procedure would be as described by Mukasey et al. in [18]. The action performed here involves deciding whether to transport the evidence through a removable storage device or network and whether to encrypt the transportation link.

- **Removable drive/Network.** The decision on the media to use in evidence transportation is informed by the stipulated policies in the preparation phase.
- **Link encryption.** If the transportation occurs via a network, the links need to be encrypted. This will prevent packet sniffers and eavesdroppers from accessing the evidence.

L. Evidence storage

Evidence always has to be transported form the incident scene to a more secure environment where it cannot be interfered with. In this section, the authors present ways in which evidence can be stored.

- **Conversion of packet attributes into database.** This action involves extraction of IP and ICMP attributes from IP packets [10] and their storing in a database. The attributes may be helpful in the analysis phases for easier identification of IP addresses that were involved in a communication.
- **Storage.** If the evidence has been transported through physical storage media, it has to be stored according to how it is presented in [10]. If evidence is stored online, the environment needs to be secure with highly restricted remote access.

M. *Evidence analysis*

One of the most crucial phases of a digital forensics process is the analysis phase. In this phase the digital forensics teams use different forensic tools and techniques to make sense of the collected evidence. The analysis phase helps the investigators to validate or dispute allegations of computer misuse. Here it is important that investigators should adhere to the basic principle that analysis should be performed of copies of the evidence. The procedures below must not necessarily be followed in their presented order. The different actions may be assigned as tasks to different forensic team members for easier and faster analysis.

- **Protocol decoding.** Protocol decoding [19], [20] deals with the analysis of elements of a protocol. This is a technique applied by intrusion detection systems where elements of a protocol (e.g. IP, ICMP) are decoded and rules are applied to detect any violations. According to Vacca in [20], this technique allows investigators to detect unknown attacks as it can correlate an exploit with a pattern.
- **Extraction of packet attributes.** The attributes that can be extracted from an IP packet include among others the source IP address, destination IP address, source port, destination port, etc. [21]. These attributes may also be obtained from the database as they were entered in the evidence storage phase. They can help in attack recognition and for tools that help in identifying the source of the attack.
- **Marking of suspicious packets**. The attributes that are identified as being violated in the protocol decoding and extraction of packet attributes are used to identify suspicious packets in network traffic. Such packets are marked as suspicious and are kept separate. This helps in reducing the amount of data that needs to be analysed, as the main focus will be on the marked packets [10]. This action needs to occur in parallel with the protocol decoding and packet extraction actions.
- **Flow reconstruction.** The purpose of network flow reconstruction is to obtain a logical representation of the network structure from which and on which an attack occurred [22]. This activity assists in identifying the perpetrator and also in mitigating the attack.
- **Data reduction.** Based on the marked packets, the evidence can be classified in order of relevancy. Evidence with most suspicious packets will be prioritised in the analysis phase and so reduce the data to be analysed [10]. It should be noted that analysis of the prioritised evidence may eventually lead to a need to analyse evidence that has not been prioritised.
- **Data reconstruction.** The purpose of this action is to reconstruct human-readable information from the network traffic. Text files, images and videos can be reconstructed from IP packets that were captured from the network as evidence. Algorithms such as presented by Batenburg in [23] and implemented by various digital forensic tools are used to reconstruct human-readable data from the network flow. Images, files and video files may be used to substantiate cases of for example child pornography.
- **Keyword indexing and searching.** This action involves searching for specific keywords or phrases of interest through the dumped network files. The searched key words can assist in eliminating hits that are not relevant to an investigation [24]. If a keyword of interest is an IP address, data that is associated with hits on that address may be isolated for further scrutinising. •
- **Statistical analysis of packet attributes.** Kaushik et al. in [10] present an algorithm for generating statistical data from IP packet attributes. In [10], it is argued that such statistical data can be used to validate the attack.
- **Attack validation using statistical information.** By using the statistical information gathered in the statistical analysis of packet attributes action, and also from the data base can be used to validate an attack [10]. Amran et al. in [14] present an approach that uses the Common Vulnerability Scoring System (CVSS) to validate an attack. The scoring approach also ensures the credibility of the evidence.

IV. CONCLUSION AND FUTURE WORK

In this paper, the authors presented digital forensic procedures on the basis of which digital forensics can be carried out in a network environment. The procedures presented follow the digital forensic processes presented in line with the draft international standards in [11], [25]. This paper is one in a series of papers aimed at standardising digital forensic procedures in a cloud environment. The papers are based on RAM forensics and network forensics as both constitute an integral part of cloud forensics. The next paper will planned will deal with complete digital forensic procedures in cloud computing. Further research work includes validation of the procedures presented in this paper.

REFERENCES

[1] G. E. Mathew, “Cloud Computing,” *SETLabs Briefing*, vol. 7, no. 7, 2009.

[2] T. B. Winans and J. S. Brown, “Cloud Computing: A collection of working papers.” 2009.

[3] L.-H. Schubert, “The future of cloud computing: Opportunities for European Cloud Computing beyond 2010,” 2010.

[4] B. A. Forouzan and D. College, *Data Communication and Networking, 3/e*, 3rd ed. 2004.

[5] C. Y. Cho, S. Y. Lee, C. P. Tan, and Y. T. Tan, “Network Forensics on packet fingerprint,” in *21st*

IFIP Information Security Conference (SEC 2006), 2006.

[6] E. Casey, "Network traffic as a source of evidence: tool strengths, weaknesses, and future needs," *Digital Investigation*, vol. 1, no. 1, pp. 28-43, Feb. 2004.

[7] B. Turnbull and J. Slay, "Wireless Forensic Analysis tools for Use in the Electronic Evidence Collection Process," in *Proceddings of the 40 Hawaii International Conference on System Science (HICSS'07)*, 2007.

[8] R. F. Erbacher, M. Ieee, K. Christiansen, and A. Sundberg, "Visual Network Forensic Techniques and Processes," *Current*.

[9] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *Nist Special Publication*, 2006.

[10] A. K. Kaushik and R. C. Joshi, "Network Forensic System for ICMP Attacks," *International Journal of Computer Applications*, vol. 2, no. 3, pp. 14-21, May 2010.

[11] "Information Technology- Security techniques- Investigation principles and processes," U.S. Patent ISO/IEC WD 270432012.

[12] R. Leigland, "A Formalization of Digital Forensics," *International Journal of Digital Evidence*, vol. 3, no. 2, pp. 1-32, 2004.

[13] K. Mandia, C. Prosise, and M. Pepe, *Incident Response & Computer Forensics*. McGraw-Hill/Osborne, 2003, p. 507.

[14] A. R. Amran, R. C. Phan, and D. J. Parish, "Metrics for Network Forensics Conviction Evidence," *Analysis*. Institute of Electrical and Electronics Engineers, 2009.

[15] Y.-D. Shin, "New Digital Forensics Investigation Procedure Model," *2008 Fourth International Conference on Networked Computing and Advanced Information Management*, pp. 528-531, Sep. 2008.

[16] I. Dlamini, M. Olivier, and S. Sibiya, "Pattern-Based Approach for Logical Traffic Isolation Forensic Modelling," *2009 20th International Workshop on Database and Expert Systems Application*, pp. 145-149, 2009.

[17] "Guidelines for Best Practice in the Forensic Examination of Digital Technology," *International Organization on Computer Evidence*, 2012. [Online]. Available: http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html.

[18] M. B. Mukasey, J. L. Sedgwick, and D. W. Hagy, "Electronic Crime Scene Investigation : A Guide for First Responders , Second Edition," Washinton, DC, 2008.

[19] J. Long, *Storage Networking Protocol Fundamentals*. Cisco Press, 2006, p. 552.

[20] J. R. Vacca, *Computer and Information Security Handbook (The Morgan Kaufmann Series in Computer Security)*. Morgan Kaufmann, 2009.

[21] W. Fan and Wu, *Advances in Web-Age Information Management, 6th International Conference, WAIM 2005, Hangzhou, China, October 11-13, 2005, Proceedings*, vol. 3739. Springer, 2005.

[22] O. Demir, "A scalable agent-based system for network flow reconstructio with applicatios to determining the structure and dynamics of distributed denial of service attacks.," City University of New York, 2010.

[23] K. J. Batenburg, "A Network Flow Algorithm for Binary Image Reconstruction from Few Projections," LNCS 4245., Berlin Heidelburg: Springer-Verlag, 2006, pp. 86-97.

[24] Forentech, "Forensic Lifecycle: An effective and repeatable process for computer forensic investigation." 2005.

[25] "Information technology - Security techniques - Guidelines for identification, collection and acquisition and preservation of digital evidence.," U.S. Patent ISO/IEC DIS 270372011.