A Digital Triage Forensics Framework of Window Malware Forensic Toolkit

Based on ISO/IEC 27037:2012

Da-Yu Kao*
Department of Information Management,
Central Police University, Taoyuan City, Taiwan 33304
*Corresponding author: camel@mail.cpu.edu.tw

Guan-Jie Wu
Department of Information Management,
Central Police University, Taoyuan City, Taiwan 33304

***Abstract*—The rise of malware attack and data leakage is putting the Internet at a higher risk. Digital forensic examiners responsible for cyber security incident need to continually update their processes, knowledge and tools due to changing technology. These attack activities can be investigated by means of Digital Triage Forensics (DTF) methodologies. DTF is a procedural model for the crime scene investigation of digital forensic applications. It takes place as a way of gathering quick intelligence, and presents methods of conducting pre/post-blast investigations. A DTF framework of Window malware forensic toolkit is further proposed. It is also based on ISO/IEC 27037: 2012 - guidelines for specific activities in the handling of digital evidence. The argument is made for a careful use of digital forensic investigations to improve the overall quality of expert examiners. This solution may improve the speed and quality of pre/post-blast investigations. By considering how triage solutions are being implemented into digital investigations, this study presents a critical analysis of malware forensics. The analysis serves as feedback for integrating digital forensic considerations, and specifies directions for further standardization efforts.**

Keywords—digital forensics; digital triage forensics; ISO/IEC 27037; cybercrime; malware, hacker (key words)

I. INTRODUCTION

Malware is short for malicious software, which broadly provide unauthorized access or perform unauthorized actions on a system. Security breaches become a part of life nowadays. As society becomes increasingly digitalized, it also becomes necessary to optimize the forensic examination process. Hackers have often destroyed evidence by modifying logs, overwriting files, or encrypting incriminating data. Examiners, such as system administrators, incident response specialists, and forensic laboratory managers, are rarely presented with a perfect incident scene. They are called to an incident after a victim has taken steps to remediate an incident [1]. This creates investigative difficulty and legal challenges to prove the evidence is authentic and reliable. In order to ensure that the evidence is admissible in court, examiners should closely follow some rigorous procedures or recommendations. Forensics is intangible by nature. It is essential for digital examiners to develop appropriate skills. Forensics is heterogeneous and digital forensics is no exception to this. Certifications are a good way to develop examiners' skills.

The growing need of digital forensics has sparked heated debates about tools, terminology, definitions, standards, and other aspects. It should come as no surprise that this study reflects the issue of access original data in the terminology debate. Examiners need quick examination or analysis within a short period of time. Investigating the entire computer is impossible in limited hours [4]. An organization may have lots of computer and other digital devices. Lots of information is stored on a single computer. There are simply too much computers and information. In some circumstances, the following traditional digital forensics approaches are no longer appropriate [18]: seizing a media, transporting it to the lab, making a forensic image, and searching the entire system for potential evidence.

This study is organized as follows. Studies of digital forensics, Digital Triage Forensics (DTF), ISO/IEC 27037:2012 and its follow-up ISO/IEC 27043:2015 are discussed in Section 2. The proposed three stages and periods in DTF framework, which is based on ISO/IEC 27037:2012, are presented in Section 3 and Section 4. Three periods in DTF framework are also analyzed from the viewpoints of people, process, and technology. The Window malware forensic toolkit of DTF framework is further discussed and analyzed in Section 5. Future research is presented in Section 6. Conclusions are given in Section 7.

II. REVIEWS

A. Digital Forensics and DTF

1) Digital Forensics

Digital forensics is a branch of forensic science to encompass the investigation of data in digital devices [14]. It focuses on the recovery and analysis of raw data in electronic devices. It is a maturing science that needs to be continuously held to higher standards [16]. Digital forensics is separated by dead forensics and live forensics, which identify that the system is power-on or power-off at that time. If the system is boot then it called live forensics. Dead forensics may lose data or information due to shutdown of digital device or removal the plug [5]. Current attitudes towards the process of digital forensic investigations are examined to improve the speed of pre/post-blast investigations. Once the initial incident scene examination is concluded, the media can be transported back to a lab for a detailed examination.

2) Destructive Challenge in Digital Forensics

The tests of DNA or fingerprint are destructive. Traditional forensic disciplines of DNA or fingerprint analysis show that measure of forensic soundness does not require the original to be left unaltered. Despite the changes that occur in data processing, these methods are considered forensically sound. DNA evidence is regularly admitted as evidence [6]. Some practitioners of digital forensics think that a method of preserving or examining digital evidence is only forensically sound if it does not alter the original evidence source in any way [5]. However, preserving everything but change nothing is almost impossible in malware, cloud or mobile forensics. Postulating the above unaltered principle as a best practice only opens digital evidence to criticisms. It is also impossible to conform to such a principle at the incident scene. The main reasons are [5, 6, 7]: (1) many cases are handled at the same period for law enforcement agents; (2) many computers are found at the incident scene; (3) the time is limited in data processing; (4) the man-power is limited in forensic lab; (5) less information can be recorded from the first responder; (6) inconsistent principles are listed with other forensic disciplines (i.e., fingerprint process or DNA analysis); (7) some volatile data will be lost in some circumstances; (8) The backlog of digital evidence processing is obvious in a legal context.

3) The Gathering Quick Intelligence Need for DTF

As digital forensics is still an immature science, scientific processes are integrated into investigations in order to make digital evidence acceptable in court. Digital Triage Forensics (DTF) is a procedural model of digital forensic applications for the initial assessment of an incident. DTF determines its severity, prioritizes resources and sets the direction for further action of crime investigation [15]. By considering how the solution of DTF can be implemented into digital investigations, this study presents a critical review of gathering quick intelligence in the proposed DTF framework. With the rise of challenges in the forensic investigation field, some problems interesting are looming on the horizon for both victims and examiners. Digital forensics is the science of recovering digital evidence from a digital source under forensically sound conditions using scientifically derived and proven methods [8]. It is no longer sufficient to collect the non-volatile data of digital evidence when examiners pull the plug and take the computer back to the lab. Different approaches and tools are required, depending on the state of the device [11]. The appearance of DTF meets this need.

B. ISO/IEC 27037:2012 and Its Follow-up ISO/IEC 27043:2015

Many digital forensics tools have been designed to resolve the existing challenges of forensic investigation. The purpose of this study is to compare the performance of the popular tools, which follow with the criteria of ISO/IEC 27037:2012 [9]. It mainly involves the identification, collection, acquisition, and presentation of digital evidence processing (Fig. 1). The scope of this International Standard relates only to the core handling process of digital evidence although the complete digital evidence handling activities in ISO/IEC 27043:2015 include plan, prepare, respond, identify, collect, acquire, preserve, understand, report, and close [10]. These standards are intended to give fundamental principles or guidance on the investigation of information security incidents, and to ensure that tools, techniques, and methods can be selected appropriately.

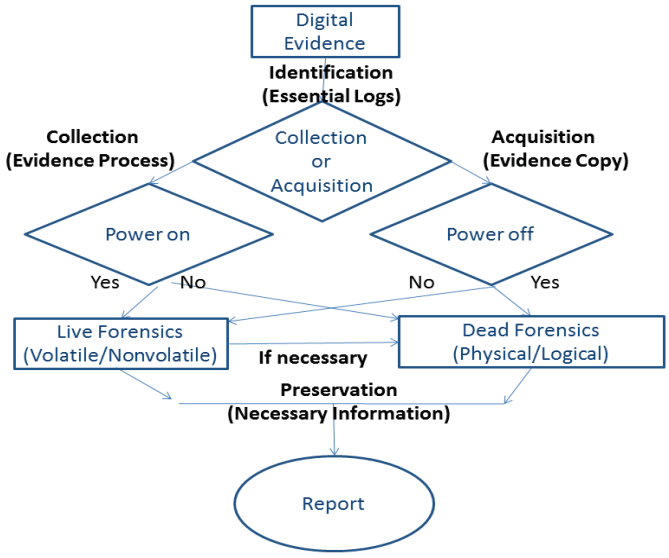

Fig. 1. Core Processes in ISO/IEC 27037:2012

1) Identification: Essential Logs

The identification process involves the recognition of digital evidence. It identifies electronic storage devices, which may contain digital evidence in an incident. As far as the digital forensics process is concerned, some elemental sources of auditing logs (e.g. IP address, date-time stamp, digital action, and response message) should be identified.

2) Collection: Evidence Process

The collection process includes documenting the handling approach and packaging mobile phones, laptops and other ICT devices [12]. The evidence of collecting digital evidence at the incident scene is a topic constantly under debate, and no single right answer exists.

3) Acquisition: Evidence Copy

The acquisition process involves producing a digital evidence copy (e.g. complete hard disk, partition, or selected files) and documenting the decision for using a particular method, appropriate tool or performed activities. The examiner should adopt a suitable acquisition method based on the situation, cost and time.

4) Preservation: Necessary Information

The preservation process involves the safeguarding of digital devices and their evidence. When first responders evaluate the scene, they should [12]: (1) leave all electronic devices off if they are already turned off; (2) ensure no unauthorized person has access to any electronic devices at the scene; (3) secure all electronic devices.

III. PROPOSED THREE STAGES IN DTF FRAMEWORK

Reconstructing an event is a necessary process in forensics investigations [13]. This section shows some ways in advance, at scene and in lab to support or refute that certain actions took

place on a computer system. The proposed DTF framework is divided into three stages which are highlighted below (Fig. 2): prepare tools in advance, perform investigation at scene, and analyze evidence in lab.

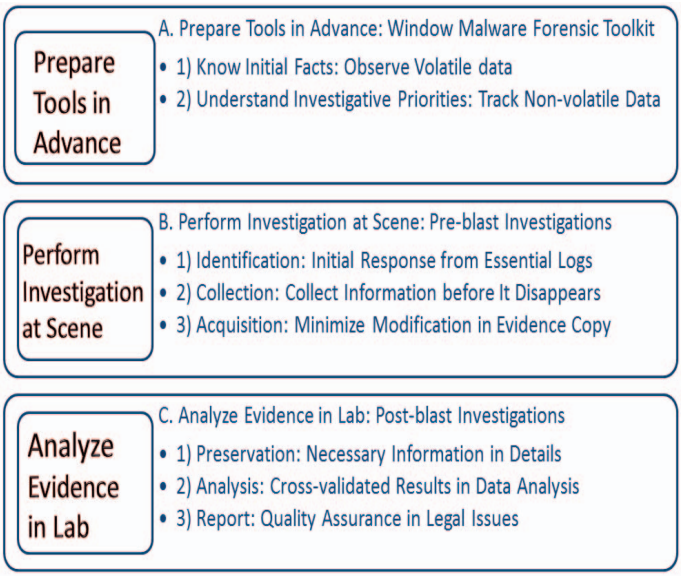

Fig. 2. Proposed Three Stages in DTF Framework

A. Prepare Tools in Advance: Window Malware Forensic Toolkit

Various forms of digital evidence have become crucial to solving a cybercrime. Examiners can match up the certain characteristic of known sample (suspicious malware) and unknown sample (at scene) [13]. The collected information of volatile or non-volatile data meets this need. Window malware forensic toolkit can be prepared in advance for digital evidence collection and investigations of cyber activities [17].

1) Know Initial Facts: Observe Volatile data

The list of connected users to a computer system may be disconnected at any single time. The volatile data of a victim computer contains significant information that helps examiners determine the 'who' and 'how' of the incident. To help answer these questions, examiners can collect data from the following areas on the victim machine (Table I) [1, 13]: date-time stamp, network status, opening port, running process, login user, auto run, and routing table information.

2) Understand Investigative Priorities: Non-volatile Data

Non-volatile data is less likely to change, and can be collected later. Examiners can collect non-volatile data from the following areas on the victim machine (Table II) [1, 13]: IP configuration, system configuration, system file, used log, and cache view.

B. Perform Investigation at Scene: Pre-blast Investigations

The following processes can be conducted at scene [9]: identification, collection, and acquisition. It allows examiners to direct contact with the suspect.

1) Identification: Initial Response from Essential Logs

The identification process is essential in the scope of legal authority. Some paperwork is necessary to take photos, take notes, tag evidence items and document the taken steps at scene.

TABLE I. VOLATILE DATA IN WINDOW MALWARE FORENSIC TOOLKIT

Date Type	Tool's Command
Date-time Stamps	date /t, time /t
Network Status	Tcpvcon, netstat –an, net view, net session, net use, NetResView /stext, Psfile, net share, net file, OpenedFilesView /stext
Opening Port	fport –p, getport, cports /stext
Running Process	Pslist, Psservice config, Handle, listdlls, psgetsid, pulist
Login User	Whoami, net accounts, userdump, net user, net localgroup, psloggedon, Joa, UserProfilesView /stext
Autorun	Autorunsc, net start, WhatInStartup /stext
Table Information	route print -4, route print -6, arp –a

TABLE II. NON-VOLATILE DATA IN WINDOW MALWARE FORENSIC TOOLKIT

Data Type	Tool's Command
IP Configuration	Hostname, ipconfig/all
System Configuration	Systeminfo, net config, psinfo, awatch /stext
System File	myuninst /stext, dir /t:c /s %windir%, dir /t:c /s "C:\Program Files (x86)\", dir /t:c /s "C:\Program Files\"
Used Log	recentfilesview /stext, usbdeview /stext, auditpol, Psloglist, faview /stext, schtasks /Query SkypeLogView /stext, mzcv /stext, Mozillahistoryview /stext, MyLastSearch /stext, browsinghistoryview /stext, iehv /stext
Cache View	insideClipboard /stext, chromecacheview /stext, Mozillacacheview /stext, IECacheView /stext, OperaCacheView /stext

2) Collection: Collect Information before It Disappears

Collecting initial facts of volatile data includes underlying operating state of the system, and plays a vital role during system examinations [18]. It helps understand the impacts of the running system and network process. To demonstrate information in volatile data, three tools in Table I are capable of capturing digital evidence. Examiners should start with the most unstable data and proceed toward stable data. This will be less likely to miss valuable information before it disappears [7].

3) Acquisition: Minimize Modification in Evidence Copy

Examiners should minimize modification when conducting forensics. However, network-based evidence is often highly volatile and must be collected through active means that inherently modify the evidence status [4]. In cases where the data acquisition is impossible without changing the configuration of the device, the procedure and the changes must be tested, validated, and documented [19].

C. Analyze Evidence in Lab: Post-blast Investigations

1) Preservation: Necessary Information in Details

Digital evidence is subject to strict rules regarding its admissibility in the court record. Examiners should take time to preserve it properly for a court trial. They should consider the initial response to preserve the integrity and admissibility of the essential logs [7].

2) Analysis: Cross-validated Results in Data Analysis

A third-party forensic tool evolution is needed to facilitate malware analysis [7]. The analysis process evaluates potential digital evidence and assesses its relevance to the investigation [10]. The analysis should describe tool version numbers, techniques and their results, and the results can be cross-validated by another examiner. Enough information is crucial for another examiner to confirm/dispute the findings.

3) Report: Quality Assurance in Legal Issues

The report should be written in simple language and should be clear, concise, unambiguous and understandable for a wide audience in its statements [10]. Examiners need to focus on what they can do, why they do it and what they have found. They can offer opinions and conclusions in court within their areas of expertise.

IV. Proposed Three Periods in DTF Framework

As the cybercrime increases in the modern society, there is an urgent need to set up a standard of evidence collection [4]. Live forensics is complementary to dead forensics in the modern era of computing. Live forensics primarily targets the volatile data which can only be collected from a running system, and which cannot be extracted from a dead system whose power cord is pulled out [2]. When a computer is involved in an incident, there are several choices to proceed during an investigation. Three periods in DTF framework are discussed below (Table III): prelusion, incident, and aftermath periods. Each period should be performed in order, and be analyzed from the viewpoints of people, process, and technology. This section provides a framework for directing and managing a digital forensic job [16].

A. Prelusion Period: System Administrators Collect Evidence for Security Management

Prelusion period includes identifying where the incident begins and how system administrators find an incident at the very beginning.

TABLE III. PROPOSED THREE PERIODS IN DTF FRAMEWORK

Period	Stage	People	Process	Technology
Prelusion	Prepare Tools in Advance	System Administrators	Evidence Collection	Security Management
Incident	Perform Investigation at Scene	Incident Response Specialists	Live Forensics	Fact Finding
Aftermath	Analyze Evidence in Lab	Forensic Laboratory Managers	Dead Forensics	Forensic Conclusion

1) People: System Administrators

System administrators are responsible for the reliable operation and security maintenance of computer systems. They seek to ensure the performance of the computers can quickly recover from a security incident. Administrators often know when a program is running exceptionally slow, or when there is something odd.

2) Process: Evidence Collection

Numerous mistyped commands or unsuccessful login attempts can be signs of SQL injection or brute-force intrusion attempts. These signs can indicate a potential area of concern. The toolkits in Table I and Table II can be valuable in helping system administrators conduct ongoing assessments of network status, and distinguish between normal and abnormal activities over a given period.

3) Technology: Security Management

Sometimes administrators cannot afford to remove the computer from the network, and a traditional forensic duplication cannot be acquired in its place. Immediate attention and proper preparation can facilitate smooth execution and include [12]: (1) establish an information security policy to ensure available services; (2) maintain an approach to handle an incident; (3) collect the related information to detect hackers; (4) report an incident to the authority.

B. Incident Period: Incident Response Specialists Perform Live Forensics for Fact Finding

1) People: Incident Response Specialists

If first responder specialists find it necessary to access the original data on a computer or on storage media, they must be competent to do so and be able to explain the relevance and the implications of their actions [2]. However, every operation may modify the computer status and can impede the forensic analysis. Changing the system as little as possible is standard practice.

2) Process: Live Forensics

The process of live forensics becomes an important issue in a security breach. It is impossible to ignore the volatile data of computer memory in performing digital evidence collection and acquisition. Live forensics allows recovering and analyzing memory content, processes and data without shutting down the system [15, 17]. Live forensics can be considered as the first step towards an incident response scenario [16]. This live forensic methodology can extract volatile data, system running processes, cached processes, network connections, and opened ports.

3) Technology: Fact Finding

If victims have filled complaints to prosecute hackers, examiners should document all the steps and hash the acquired data to vouch for the validity of the collected data.

C. Aftermath Period: Forensic Laboratory Managers Perform Dead Forensics for Forensic Conclusion

Aftermath period includes identifying how to recover from the incident, and how to get back to normal business sooner.

1) People: Forensic Laboratory Managers

If first responders forward all media on to lab without any exploitation attempts at scene, and make the forensic laboratory managers responsible for all processing, it becomes back logged very quickly by the sheer volume of data that must be analyzed. This backlog can be completely erased by implementing the DTF procedures [15].

2) Process: Dead Forensics

In dead forensics, it is much easier for examiners to minimize system modification when working with a copy of a write-protected drive.

3) Technology: Forensic Conclusion

The conclusions of the investigation must be fairly supported by the fair and reasonable depiction of what the overall evidence will show [19]. Each incident response team had to evolve the truth from a mass of confused evidence. Examiners should always offer objective opinions and conclusions that are supported by facts, and facts alone.

V. Discussions and Analyses in Window Malware Forensic Toolkit

Defending against malware has focused on intrusion detection, content filtering, detecting and blocking malware, and other reactive technologies. The Window malware forensic toolkit of DTF framework is discussed and analyzed below [1, 3, 6, 11, 12].

A. Characteristics in Malware Forensic Toolkit

The analysis of malware forensic toolkit can put some information all together and analyze the following two characteristics: class and individual. Class and individual characteristics can be found in Table I and Table II.

1) Class Characteristics

Class characteristics help the examiners narrow the pattern down to specific malware patterns. It is impossible to be familiar with every kind of malware in all of its various forms [1]. Better investigative efforts include a comparison of unknown malware with known samples in their patterns or behaviors.

2) Individual Characteristics

Individual characteristics may establish the uniqueness of an object. When individual characteristics are determined, the malware can be identified. With the help of the collected data on the target computer, the examiners are able to determine if a sample of malicious code or code pattern is consistent with the unknown sample found at the scene.

B. Command Line Interface in Malware Forensic Toolkit

Examiners need to continually perform digital evidence analysis using various tools. Digital forensic tools generally fall into one of two categories: Command Line Interface (CLI) and Graphical User Interface (GUI). A GUI is a human-computer interface that uses windows, icons and menus by a mouse. On the other hand, a CLI uses only text by a keyboard. To have a simple and easy way in collecting batch information, this study presents a malware forensic toolkit in CLI tools (Table I and Table II). Some tools use '/stext' parameter to export the retrieved data to a text file. Multi-operations can be performed much faster than in GUI tools.

1) Implement Trusted Toolkit

If hackers have broken in and achieved administrator rights, examiners must prepare some trusted tools to quickly analyze the compromised machine. Examiners should never trust the compromised computer. Because the examined system has been potentially compromised, the native programs may be modified. When they conduct live forensics it is essential to implement trusted toolkits and linked libraries to acquire data from the examined system. Incident period includes identifying potential evidence. Hackers often look for known weaknesses or exploits in the Operating System or any application programs. At the start of any investigation, several questions must be answered by first responders and system administrators immediately. Are there any file deletion activities? If so, incident response specialists must pull the power cable out of the wall. This will freeze the computer and its network [6, 12]. Let the forensic laboratory managers to obtain potential evidence later. The entire scenario usually dictates the next steps an examiner takes.

2) Volatile and Non-volatile Data in Malware Forensic Toolkit

This proposed toolkit presents a malware forensic toolkit to capture evidence from computer memory. When the collection tools are stored on a CD-ROM, the collected information of volatile and non-volatile data can be recorded in other removable disk. The collected data consists of two main subsets: volatile and non-volatile data. This volatile data would lose if examiners were to rely on the traditional analysis methods of forensic duplications. The volatile data will not be present if examiners shut down a computer.

C. Malware Forensic Toolkit in Digital Forensics

1) Case-oriented Difference

As hacker attacks become sophisticated, malware continues to advance and automate effective attack techniques. The impact of malware ranges from minor system performance issues to remote control of a system by an attacker. As ICT devices continue to update, examiners must adopt new principles, methods or tools to keep in good status of handling cybercrime issues [11]. This is applicable especially in malware investigation. It is problematic that the accused can use this malware defense strategy to camouflage his/her crimes. Every case may differ from each other. The collected evidences may vary in their time, relationship or function. When the modification of digital data is unavoidable, the procedure and the changes must be documented [19]. Examiners can use video, photography, notes or sketches to help convey or reconstruct the details of the scene later [12].

2) Put Data All Together

Volatile or non-volatile data are often putted together in a batch file to get a picture of what happened after examiners sincerely parse the stored data, analyze the relevant information, and interpret their relationship. Those data can provide certain action indications which were performed by malware or a user. Mutual comparison among different evidential sources becomes an essential part to support or refute a malware defense.

3) Need for Malware Forensic Toolkit

A malware forensic toolkit is essential to collect information from the Windows system for volatile and non-volatile data (Table I and Table II). That toolkit can [3]: (1) acquire memory contents for forensic analysis; (2) parse data from the physical memory; (3) reduce data size; (4) look into

the large volumes of data for analysis; (5) monitor the running program.

VI. Future Research

Digital evidence can be fragile in nature. It may be altered, tampered with or destroyed through improper handling or examination. Some symptoms can be creased by different approaches. While attackers can lunch their attacks on various platforms, this framework is not powerful enough to detect various OSes (such as Windows, Unix family, iOS) or various devices (such as desktops, smartphones, embedded devices). In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions [2]. Digital forensic investigators should be competent to manage the follow-up consequences when dealing with digital evidence. While emulators or virtual environments become more prevalent as an analysis tool in digital forensic investigations, they may allow digital forensic investigators to observe the malware activities and their various processes. It can reduce the risk of damaging evidences. While this work represents an important initial exploration into the use of digital triage forensics framework for malware identification, there is still a need for further experimentation to keep the integrity of digital evidences across different OSes and various devices. Future research will take these mechanisms into account so that it can make the life of an investigator easier. Then the evidences can be accepted by a court.

VII. Conclusion

The malware incident response process has become a technique for collecting and analyzing forensically sound evidence. The data currently in memory may be the only evidence of the incident. A live forensic process contains information such as the current network connections, running processes, and open files. The proposed Window malware forensic toolkit can collect relevant data from the target computer to confirm whether an incident has occurred. The data is collected by running a series of commands. Each command produces data in an easily readable format. The nature of this framework suggests substantial benefits from using ISO/IEC 27037:2012 approach as a critical reference for system administrators, incident response specialists and forensic laboratory managers. The purpose of this theoretical framework is to provide selection with an entire view of Window malware forensic toolkit. It is vital to recover possible evidence from a digital source in a forensically sound manner. Examiners can look at a piece of digital evidence in an investigation, gather more information, and try to explain what happened during an incident. They should only make conclusions based upon what the science can show, but cannot overstate the conclusions from the discovered electronic evidence.

Acknowledgment

This research was partially supported by the Henry C. Lee Forensic Science Foundation and the Ministry of Science and Technology of the Republic of China under the Grants MOST 103-2221-E-015-003-.

References

[1] Aquilina, J. M., Casey, E., and Malin, C. H., "Malware Forensics: Investigating and Analyzing Malicious Code," Burlington, MA: Elsevier Inc., pp. 93-282, 2008.

[2] Association of Chief Police Officers (ACPO), "ACPO Good Practice Guide for Digital Evidence, Version 5," pp.6-12, March 2012.

[3] Andress, J., Winterfeld, S., and Ablon, L., "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners (2nd Edition)," Burlington, MA: Elsevier Inc., pp. 181-192, 2014.

[4] Bashir, M. S. and Khan M. N. A., "Triage in Live Digital Forensic Analysis," The International Journal of Forensic Computer Science (IJOFCS), vol. 1, no. 1, pp. 35-44, 2013.

[5] Casey, E., "Handbook of Digital Forensics and Investigation," Burlington, MA: Elsevier Inc., pp. 21-208, 2010.

[6] Casey, E., "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd Edition)," Waltham, MA: Elsevier Inc., pp. 187-306, 2011.

[7] Flandrin, F., Buchanan, W. J., Macfarlane, R., Ramsay, B., and Smales, A., "Evaluating Digital Forensic Tools (DFTs)," 7th International Conference : Cybercrime Forensics Education & Training, Canterbury, September 2014.

[8] Hosseinkhani, J., Koochakzaei, M., and Keikhaee, S., "Detecting Suspicion Information on the Web Using Crime Data Mining Techniques," International Journal of Advanced Computer Science and Information Technology (IJACSIT), vol. 3, no. 1, pp. 32-41, 2014.

[9] International Organization for Standardization (ISO), "ISO/IEC 27037:2012 - Information Technology: Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence," Switzerland: ISO Office, 2012.

[10] International Organization for Standardization (ISO), "ISO/IEC 27043:2015 Information Technology - Security Techniques - Incident Investigation Principles and Processes," Switzerland: ISO Office, 2015.

[11] Jingle, D. J. and Rajsingh, E. B., "ColShield: An Effective and Collaborative Protection Shield for the Detection and Prevention of Collaborative Flooding of DDOS Attacks in Wireless Mesh Networks," Human-centric Computing and Information Sciences, vol. 4, no. 8., 2014.

[12] Johnson, L., "Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response," Burlington, MA: Elsevier Inc., pp. 97-184, 2013.

[13] Ligh, M. H., Case, A., Levy, J., and Walters, A., "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory," Indianapolis. IN: John Wiley & Sons, Inc., 2014.

[14] Marshall, A. M., "Standards, Professionalization and Quality in Digital Forensics," Digital Investigation, vol. 8, no. 2., pp. 141-144, 2011.

[15] Pearson, S. and Watson, R., "Digital Triage Forensics: Processing the Digital Crime Scene," Elsevier Inc., MA: Burlington, 2010.

[16] Raghavan, S., "A Framework for Identifying Associations in Digital Evidence Using Metadata," Brisbane: Queensland University of Technology Dissertation, pp. 73-124, 2014.

[17] Roger, A. E. and Achille, M. M., "Multi-Perspective Cybercrime Investigation Process Modeling," International Journal of Applied Information Systems (IJAIS), Foundation of Computer Science FCS, New York, USA, vol. 2, no.2, June 2012.

[18] Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., and Debrota, S., "Computer Forensics Field Triage Process Model," Journal of Digital Forensics, Security and Law, vol. 1, no. 2., 2006.

[19] Stephenson, P., "Official (ISC)2® Guide to the CCFP CBK," Boca Raton, FL: Auerbach Publications, pp. 293-404, 2014.