The Governance of Digital Forensic Investigation in Law Enforcement Agencies

Da-Yu Kao[a], Ni-Chen Wu[a], Fuching Tsai[b]

[a]Department of Information Management, Central Police University, Taiwan

[b]Department of Criminal Investigation, Central Police University, Taiwan

[b]**Corresponding Author: fctsai@mail.cpu.edu.tw**

***Abstract*—The volume of data for cybercrime investigation keeps growing at unprecedented rates and creating a quandary for law enforcement agencies. This brings a great challenge for law enforcement agencies. It requires the sincere examination of all available data volumes at crime scene or in lab to present digital evidence in a court of law. In order to maintain the integrity and validity of digital evidence, investigators must establish a process model that can provide a quick response at scene. This paper illustrates the novel TEAR-phase application of THOR dimensions to digital forensics. It facilitates the efficiency and effectiveness of constructing a clear investigation.**

Keywords—digital forensics, evidence triage, THOR dimensions, data network, Autopsy

I. INTRODUCTION

When investigators evaluate evidence, its reliability and accuracy are of grave importance both in the investigative and probative stages of a case. The digital forensic process is very time-consuming, because it requires the examination of available data volumes from the scene. The digital forensic process commences with any pieces of digital media. Every action taken has to adhere to the legitimacy rules so that the obtained digital evidence could be presented in the court. Conducting a digital forensics on the original evidence sources should be avoided if possible since the examination on forensic copies or images maintains the data integrity of digital evidence. However, evidence triage provides valuable quick intelligence without subjecting digital evidence to a full examination and determines if a media is worth to be examined under significant time constraints [10]. This quick intelligence can be used in the field to guide the search and seizure, and in the laboratory to determine if a media is worth to be examined.

The structure of this paper is organized as follows. Section 2 provides a review of evidence and principles in cybercrime investigation. Section 3 describes the proposed triangle strategy of digital forensic process. Section 4 demonstrates the discussions and analyses. Finally, the last section concludes the paper.

II. REVIEWS

A. Digital Evidence

Digital devices are everywhere and help people communicate locally and globally. Computers, cell phones and the Internet are valuable sources for digital evidence, and any piece of information technology can be used in a criminal way. Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device [4]. This evidence can be acquired when electronic devices are seized and secured for examination. Digital evidence is [3]:

1) Fragile: It can be altered, damaged or destroyed with little effort.

2) International: It can cross jurisdictional borders instantly and easily.

3) Latent: It is hidden like fingerprints or DNA evidence.

4) Volatile: It is volatile and sensitive.

B. Forensic Investigations in LEA

Crime scene investigation in Law Enforcement Agencies (LEAs) includes case analysis, report writing and legal presentation [9].

1) Case Analysis

Case analysis should be all independently reported by different experts.

2) Report Writing

Different reports from various experts involved in the case are called to give evidence explanations at the courtroom since the reports only have validity after being confirmed at the hearing.

3) Legal Presentation

Legal presentation in court is to give evidence explaining the relevance and the implications of their actions. Evidence is specific to his/her specialty so that forensic experts can be cross-examined and present their cases objectively without fear, uncertainty, or doubt.

III. PROPOSED TRIANGLE STRATEGY

The proposed triage strategy in digital forensic investigation is divided into three categories (Figure 1): principles, forensics, and governance.

A. Principles

Digital forensics is a branch of forensic science to encompass the investigation in digital devices. It focuses on the recovery and analysis of raw data in electronic devices. The required principles for digital evidence handling can be satisfied as follows [6]:

1) Sufficiency

An investigator needs to exhaust different methods, tools, and practices to identify, extract, and convert data to readable

evidence. There must be sufficient evidence to make the investigation convincing. Investigators should have taken into consideration that enough material has been gathered to prove somethings. Investigators should be able to decide how much and which material to collect or acquire at scene.

2) Relevance

The data value can assist the investigation of the particular incident. Investigators should be able to describe the followed procedures form auditing records and explain how the decision to collect each data was made. The relevancy of admissible data affects the weight and usefulness of the evidence. Time, efforts, and cost spent in investigation could be well controlled if investigators know what should be collected during the investigation. Then they can demonstrate that the acquired material is relevant to the investigation.

3) Reliability

Data extracting is not simply copying of data. All processes used in handling potential digital evidence should be auditable. Chain of custody should be preserved during collecting, examining, analysing, preserving, and transporting of data. If the evidence cannot be repudiated and rebutted, then the digital evidence would be reliable and admissible in a court of law.

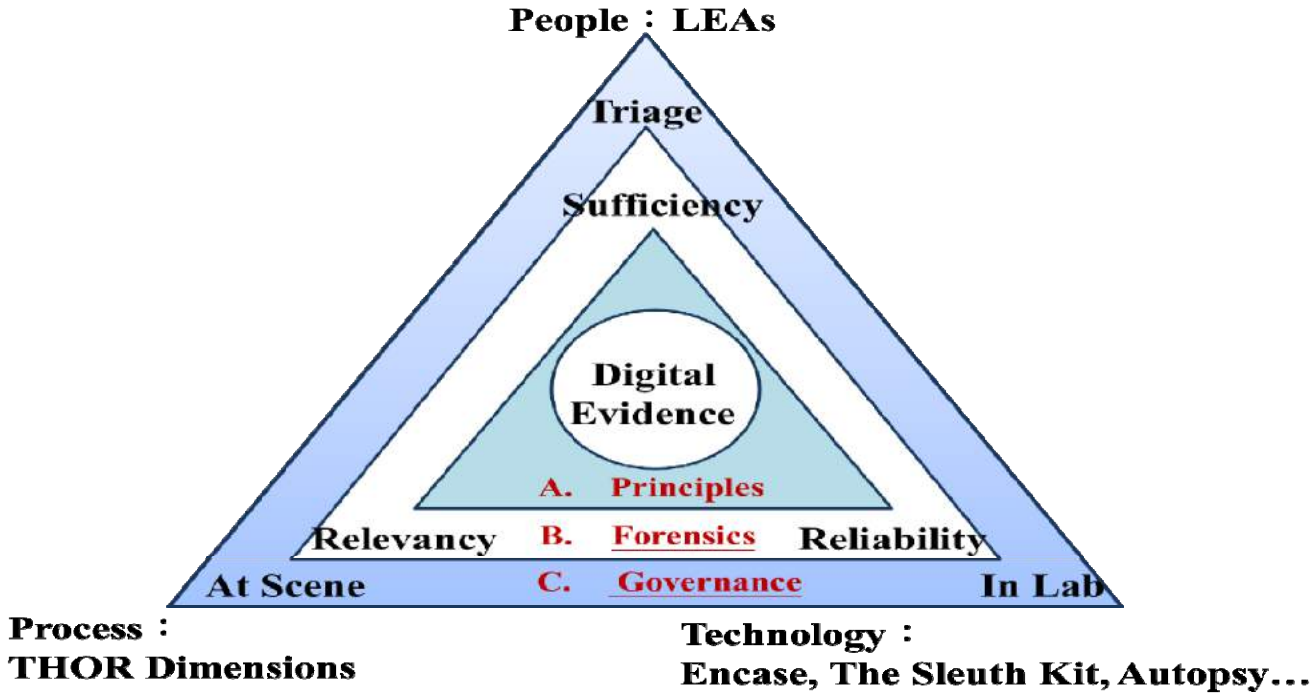

Figure 1. Triangle strategy of digital forensics process

B. Forensics

In Figure 1, there are three elements in our proposed triangle strategy. The detailed description is demonstrated in the following:

1) Triage

As the data loads increase exponentially, triage has become an increasingly important part of digital forensics. Triage aims to identify the most relevant data as quickly as possible. It helps carry out an investigation in a limited time. Some digital forensic tools meet this need by extracting the recently changed files from a computer.

2) At Scene

When investigators arrive at scene, they will look for all relevant evidence, explore some questions, and find the follow-up answers on whom, which, what, when, where, and how. Everything can be evidential to support or refute something.

3) In Lab

Due to the limitations of technology or knowledge, some evidence cannot be identified at scene and must be brought back to the laboratory for further examination.

C. Governance

1) People: LEAs

The dependence on using digital forensic tools or techniques brings about the detection and recovery of hidden data in LEAs. The trend of digital forensics implies the imperative need for governance on digital forensics. Investigators should persistently upgrade their skills, tools, and know-how to keep pace with changing technology. They should know how to extract the volatile evidence, use appropriate tools, and perform live investigative response [7]. It is no longer able to simply unplug a computer and expand the backlog as a mountain at lab.

2) Process: THOR Dimensions

The goal of the CAMINO (Comprehensive Approach to cyber roadMap coordINation and develOpment) project was to develop a comprehensive cybercrime and cyber terrorism

research agenda. THOR dimensions are the foundation of the CAMINO roadmap and address the following aspects [5]:

a) *(T)echnical*-related to technology, technological approaches and solutions.

b) *(H)uman*-related to human factors, behavioral aspects, privacy issues, as well as raising awareness and knowledge of society.

c) *(O)rganizational*-related to processes, procedures and policies within organizations, as well as cooperation between organizations.

d) *(R)egulatory*-related to law provisioning, standardization and forensics.

3) Technology: Digital Forensics Tools

The range of digital forensics includes personal devices, network servers, cloud systems, and mobile handsets. The following of digital forensic tools is designed for different types of examined targets.

a) *Computer Forensics: Autopsy, Encase, FTK, The Sleuth Kit*

b) *Memory Forensics: Volatility, Windows SCOPE*

c) *Mobile Device Forensics: Micro Systemation XRY/XACT*

IV. Discussions and Analyses

A. Reducing Digital Forensic Backlogs – Triage

As the prevalence of digital evidence in criminal, civil, or administrative cases becomes popular, backlogs in forensic labs continue to grow quickly [6]. Triage originally means that when medical resources are insufficient to deal with all injuries, they are classified, sorted, or selected to determine the priority order of emergency treatment. Then the injured can be treated efficiently and based on injury situation of the patients to determine the priority treatment process. Cybercrime investigators need to set up a series of digital triage processes to classify the various cases or scenes and to determine whether some devices need further examinations in lab. The purpose of digital triage is to rapidly prioritize the digital media and quickly obtain the quick intelligence. It is a solution to the problem of case backlogs. Digital triage is the investigative beginning of forensic examination. Figure 2 demonstrates two types of digital triage: live and dead. A triage assessment does not replace the forensic analysis. Some initial tasks can be performed at scene by non-digital evidence specialists to increase the efficiency of an investigation in a timely manner and to decrease the examination backlog in lab.

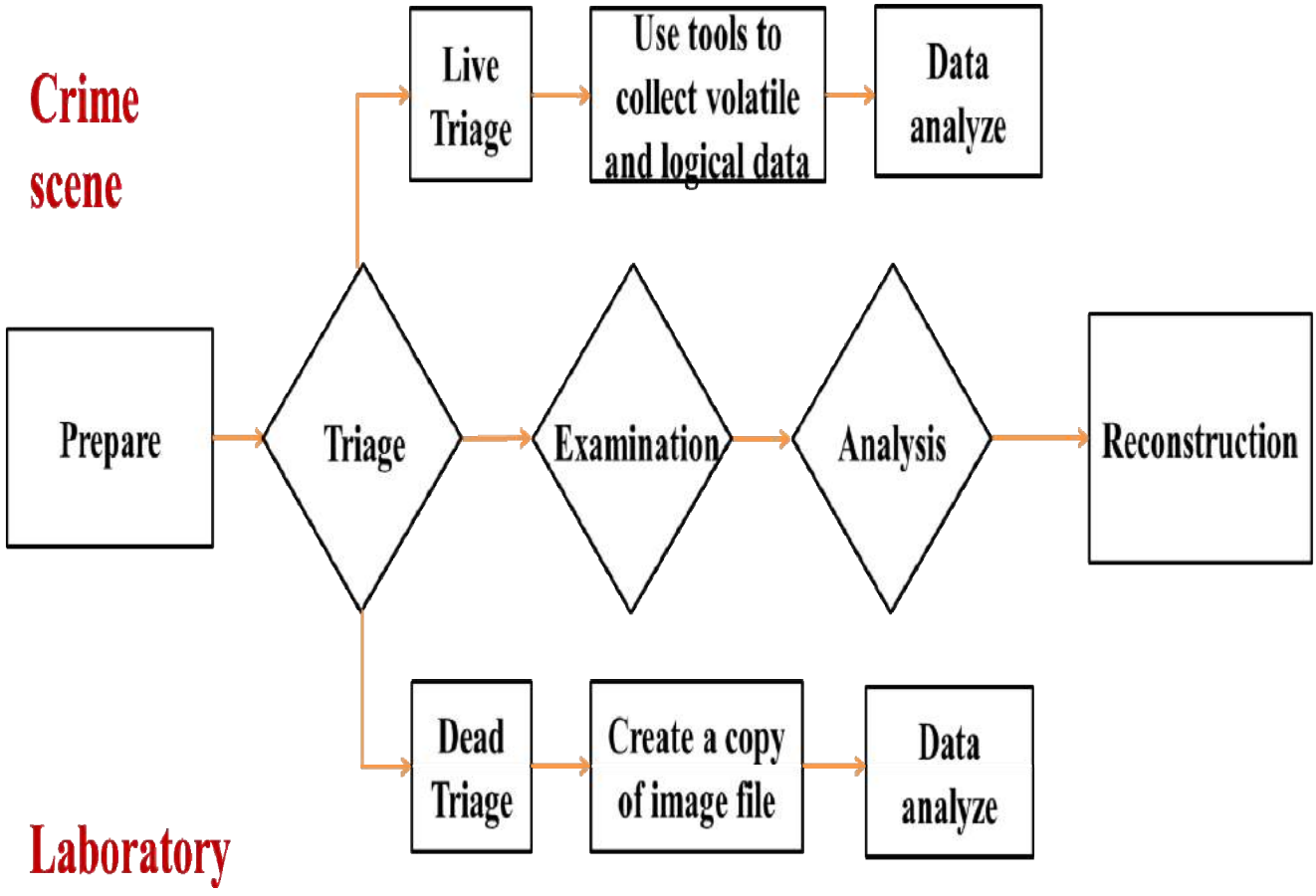

Figure 2. The TEAR evidence process

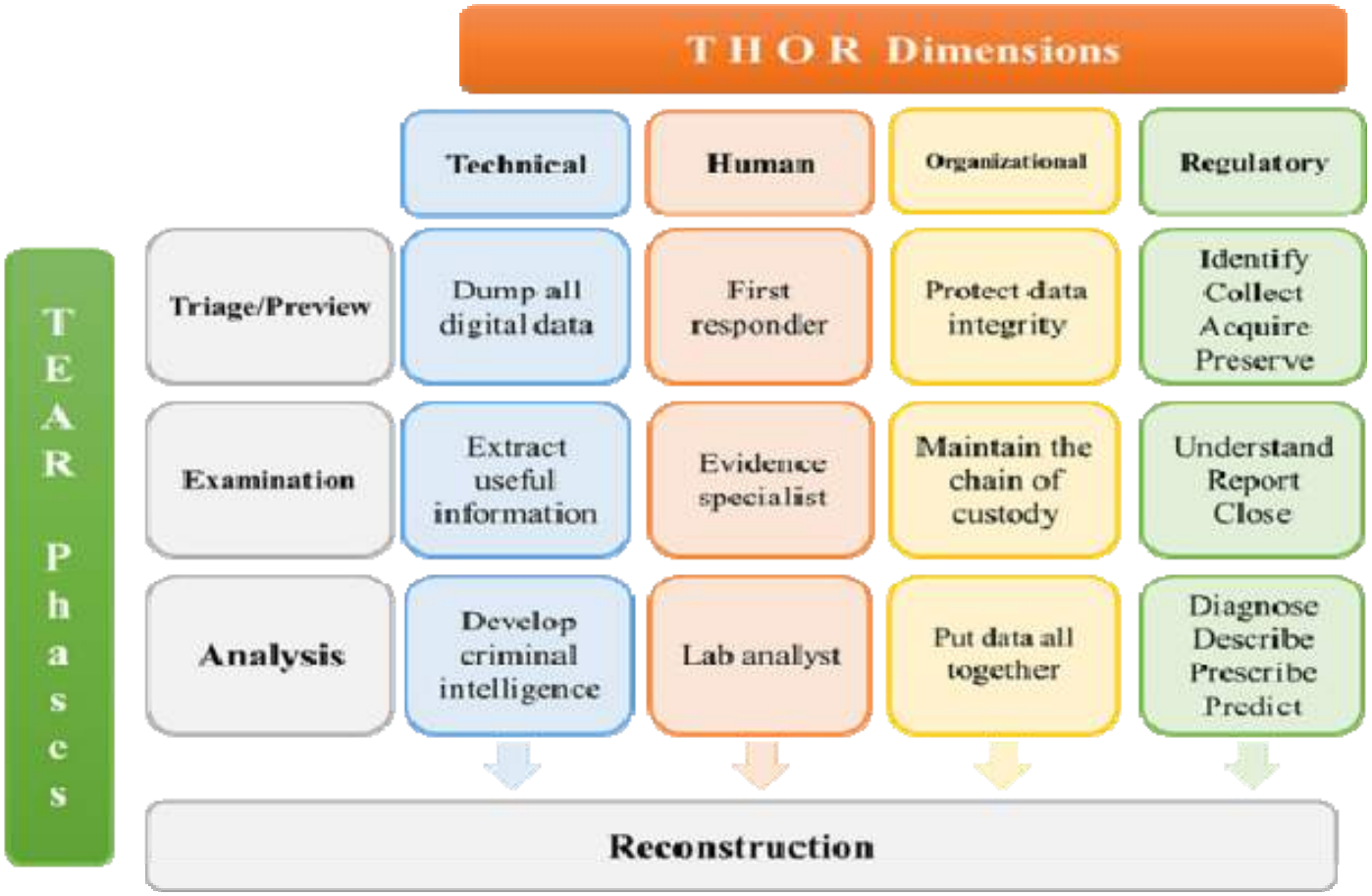

Figure 3. The multi-dimensional framework of digital forensics

1) Methods of Live Triage

The primary purpose of live triage is a rapid extraction of quick intelligence from the online sources. Live triage has the potential to quickly identify evidential data. Investigators need to find the following volatile and logic data from the power-on device.

a) Volatile Evidence: memory, network connections, running process, and open file.

b) Logical Data: operating system setting, network status, execution information, and system log records.

2) Methods of Dead Triage

Dead triage is conducted in lab for the possible existence of the relevant evidence. Some types of tools are [8]:

a) Acquiring a copy of image file.

b) Indexing, searching, cracking, and analyzing the digital contents in the digital media.

c) Presenting a forensic report

3) Scene Investigation

Scene investigation focuses on the dynamic evidence of the power-on status to detect and explore any possible answers of scenarios. At scene, under the power-on state, a live investigation of the primary memory content can be conducted to quickly collect the volatile evidence. The scene must be properly photographed or recorded. Turning off computer power is not the first thing to do at scene since immediately turning off the power of the computer will inevitably result in the loss of programs and data running in memory. Sometimes, it will destroy the valuable evidence.

4) Lab Forensics

Lab forensics, in the static evidence of shutdown status, focuses on identifying results. In lab, dead forensics analysis for digital storage media can be repeatedly verified for integrity. However, this time-consuming processing can result in excessive backlogs from a large amount of new cases.

B. THOR Components in Digital Forensics

In Figure 3, digital forensics is discussed in the following dimensions: Technical, Human, Organizational, and Regulatory. Each dimension is further distributed into 4 processes: Triage/Preview, Examination, Analysis and Reconstruction. The two axes represent perspectives and processes of digital forensic investigation. This proposed multi-dimensional framework helps law enforcement officers produce a quality report [6]. It also illustrates TEAR phases from the viewpoint of THOR dimensions to describe the best

practices for identifying, collecting, acquiring and preserving the digital data [9].

1) (T)riage/Preview

Investigators can use a triage tool to preview data at scene.

a) Technical: Using some tools dumps relevant data.

b) Human: Investigators provide assistance at scene.

c) Organizational: Evidence integrity refers to the preservation of evidence in its original form. The inspection process must be supervised or recorded.

d) Regulatory: ISO/IEC 27037:2012

Identify/ Collect/ Acquire/ Preserve

The guidelines for identification, collection, acquisition and preservation in handling potential digital evidence are required in an investigation to maintain the integrity of the digital evidence.

2) (E)xamination

Investigators extract useful data from digital devices, bring raw data to the lab, and maintain the chain of custody at the same time.

a) Technical

Investigators use tools to extract useful information from collected evidence.

b) Human

Investigators are responsible for documenting and preparing evidence once it arrives at scene.

c) Organizational

Investigators should comply with the chain of custody, which includes the documentation of physical and digital evidence.

d) Regulatory

The forensic examination aids the understanding of the evidence, reports the fact in issue, and assists the court to close the case.

3) (A)nalysis

Investigators should determine the processes necessary to complete the analysis.

a) Technical: Investigators should integrate the extracted data and develop an intelligence analysis platform.

b) Human: Forensics analysts who work at the lab combine relevant events into explore the fact.

c) Organizational: Investigators should put data all together to help the court make good decisions.

d) Regulatory: Investigators can use big data analytics to diagnose, describe, prescribe, or predict the case.

4) (R)econstruction

Reconstruction involves ordering the evidential associations from temporal, relational, and functional analysis. Crime reconstruction is the determination of the actions and events surrounding the commission of a crime. It can leverage a wide range of forensic methods to establish a hypothesis about the sequence of events and test whether the hypothesis is truth or not. If the hypothesis is confirmed, then one possible explanation can be identified. If it is refuted, then the explanation is not possible and other hypotheses will have to be considered [1].

C. Proposed Toolkits in Digital Forensic Investigations

Several tools for conducting cybercrime investigations in TEAR phases are briefly introduced below (Table 1)[10].

TABLE 1. USED TOOLS IN TEAR PHASES

Phases	Functions	Tool
Triage/Preview	Packet capture	Wireshark
	Make an image file create hashes of files Data recovery	FTK Imager
	Dump the memory	RAM Capturer
Examination	Browser information extraction	Dumpzilla
	capture the physical memory analyze artifacts in memory	Magnet RAM Capture
	Network sniffering	Network Miner
Analysis	Timeline Analysis Hash Filtering File System Analysis Keyword Searching	Autopsy and The Sleuth Kit
	extract applications data	Xplico
	Comprehensive analysis and forensics	EnCASE FTK TCT
Reconstructiom	Temporal Analysis Functional Analysis Relational Analysis	

1) Triage/Preview

a) *Wireshark:* It is a network capture and analyzer tool to investigate network related incident.

b) *FTK Imager:* FTK Imager is a data preview and imaging tool that allows investigators to create hashes of files and examine files and folders on local hard drives, network drives.

c) *RAM Capturer:* It is a free tool to dump the data from computer's volatile memory, which may contain encrypted volume's password and login credentials for web services.

2) Examination

a) *Dumpzilla:* It can analyze all exciting information from Firefox, Iceweasel and Seamonkey browser.

b) *Magnet RAM Capture:* It can capture the physical memory of a computer and analyze artifacts in memory.

c) *Network Miner:* It can detect OS, hostname, sessions and open ports through network packets.

3) Analysis

a) *Autopsy and The Sleuth Kit:* It is computer software that deploys many of the open source programs in The Sleuth Kit [2]. The Sleuth Kit (TSK) is a library and collection

of command line tools that allow investigators to investigate disk images or file system data.

b) *Xplico:* It aims to extract applications data from network traffic.

c) *HxD:* It is a hex editor that allows investigators to search, edit, or modify raw disk or memory.

V. CONCLUSION

Digital forensics is a continuous procedure. Each phase has a high impact on the relevance, reliability, and sufficiency of the evidence. Examination of digital sources should be completed empirically, logically, and systematically consistent with organizational policy. With the development of information technology, it is essential for investigators to get the evidence quickly and sufficiently. Crime scene is often the driving force behind a successful crime investigation. Properly collecting digital evidence is essential in cybercrime investigation. It is also critical to quickly assist the court in finding the root reasons of a case.

ACKNOWLEDGMENT

This research was partially supported by the Ministry of Science and Technology of the Republic of China under the Grants MOST 107-2221-E-015-002-.

REFERENCES

[1] Brooks, C. L., *CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide (1st Edition)*, McGraw-Hill Education, pp. 13-50, 2015.

[2] Carrier, B., "Autopsy," https://www.sleuthkit.org/autopsy/, 2018.

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

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

[5] Choraś, M. and Kozik, R., "CAMINO Roadmap (Research Agenda) for Fight against Cybercrime and Cyberterrorism," http://www.fp7-camino.eu/assets/files/Brochure-CAMINO_roadmap_250316.pdf

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

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

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

[9] Ubelaker, D. H., *The Global Practice of Forensic Science*, John Wiley & Sons Ltd, pp. 34-263, 2015.

[10] Stephenson, P., *Official (ISC)²® Guide to the Certified Cyber Forensics Professional (CCFP) Common Body of Knowledge (CBK)*, Auerbach Publications, pp. 293-404, 2014.

Dayu Kao is an Associate Professor at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. He is responsible for various recruitment efforts and training programs for Taiwan civil servants, police officers or ICT technicians. He has an extensive background in law enforcement and a strong interest in information security, ICT governance, technology-based investigation, cyber forensics, human resource development, and public sector globalization. He was a detective and forensic police officer at Taiwan's Criminal Investigation Bureau (under the National Police Administration). With a Master degree in Information Management and a PhD degree in Crime Prevention and Correction, he had led several investigations in cooperation with police agencies from other countries for the past 20 years. He can be reached at camel@mail.cpu.edu.tw.

Ni-Chen Wu is a student at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan.

Fu-Ching Tsai is a technical specialist in the Computer Center at Central Police University, Taiwan. He received his PhD degree in information management from National Cheng Kung University, Taiwan in 2013. His research interests include big data analysis, data mining, text mining, and artificial intelligence.