# A Triage Triangle Strategy for Law Enforcement to Reduce Digital Forensic Backlogs

Da-Yu Kao*, Ni-Chen Wu*, Fuching Tsai**

*Department of Information Management, Central Police University, Taiwan

**Department of Criminal Investigation, Central Police University, Taiwan

**dayukao@gmail.com, niniwu841223@gmail.com, fctsai@mail.cpu.edu.tw**

***Abstract*—The explosive growth of computer technologies creates many electronic data and produces much digital evidence of people's lives. As technology has improved, the volume of data for cybercrime investigation keeps growing at unprecedented rates and creating a quandary for Law Enforcement Agencies (LEAs). This study discusses the rise of digital evidence and the triage needs in digital forensic processing. It requires the sincere examination of all available data volumes at the scene or in the lab to present digital evidence in a court of law. In order to maintain the relevance, reliability, and sufficiency of digital evidence, investigators must establish a process model that can provide a quick response at the scene. This study proposes the novel triage triangle strategy of digital forensic components and illustrates TEAR phases from the viewpoint of THOR dimensions to describe the proper practices for identifying, collecting, acquiring, and preserving the digital data. It facilitates the efficiency and effectiveness of reducing digital forensic backlogs for LEAs.**

***Keyword*—Digital Evidence, Digital Triage Forensics, THOR dimensions, Data Network, Law Enforcement**

## I. INTRODUCTION

The digital forensic process commences with any piece 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. When investigators evaluate evidence, its relevance, reliability, and sufficiency are of grave importance both in the investigative and probative stages of a case. Digital forensics addresses the collection, examination, analysis, and presentation of evidence located on computers, cell phones, or networks. It brings the evidentiary fruits of electronic data for many types of decisions, such as divorce, child custody, contract resolution, or criminal judgments [9]. The digital forensic process is very time-consuming because it requires the examination of available data volumes from the scene.

Cybercrime is a growing problem year after year. The ability of Law Enforcement Agencies (LEAs) to investigate and prosecute criminals for these crimes still leaves much to be desired on the process, tools, or training. There is a lack of awareness of available training courses or educational materials on cybercrime investigation and digital forensics, especially for LEAs [5]. This study provided a digital evidence assessment in investigating crimes. Conducting 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 [11]. This quick intelligence can be used at the scene to guide the search and seizure, and in the lab to determine if a media is worth to be examined. With the development of information technology, LEAs need to improve the speed and quality of cybercrime investigations. Performing forensic triage can be required to quickly and efficiently review several target systems. This study tries to propose a practical strategy to mitigate the enormous backlog of cases for law enforcement.

The structure of this study is organized as follows. Section 2 provides a review of digital evidence and forensic investigations in LEAs. The proposed triage triangle strategy of digital forensic components described in Section 3. Section 4 demonstrates the discussions and analyses. Finally, the last section concludes the study.

## II. REVIEWS

### A. Digital Evidence

Most of our daily activities and interactions are recorded in electronic devices. Digital devices are everywhere and help people communicate locally and globally. Computers, cell

Manuscript received Dec. 27, 2017. This work was a follow-up of the invited journal to the accepted & presented paper of the 21st Conference on Advanced Communication Technology (ICACT2019), and this research was partially sponsored by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-109) and the Ministry of Science and Technology of the Republic of China under the Grants MOST 107-2221-E-015-002..

Da-Yu Kao is with the Department of Information Management, Central Police University, Taoyuan 333, Taiwan (phone: +886-3-328-2321; fax: +886-3-328-5189; e-mail: dayukao@gmail.com).

Ni-Chen Wu is with the Department of Information Management, Central Police University, Taoyuan 333, Taiwan (phone: +886-3-328-2321; fax: +886-3-328-5189; e-mail: dorislovesnoopy@gmail.com).

Fuching Tsai is with the Department of Criminal Investigation, Central Police University, Taoyuan 333, Taiwan (Corresponding Author phone: +886-3-328-2321; fax: +886-3-328-5189; e-mail: fctsai@mail.cpu.edu.tw).

phones, and the Internet are valuable sources for digital evidence. Digital data is always stored in various locations across a system or physical location. Any piece of information technology can be used criminally. Digital evidence is defined as information and data of value to an investigation that is stored on, received, or transmitted by an electronic device [3]. Digital evidence can help answer any questions in an investigation ranging from the whereabouts of a victim at a given time to the state of mind of the criminal. Answering these questions requires some degree of crime reconstruction, including a combination of temporal, functional, and relational analysis of available evidence [3]. This evidence can be acquired when electronic devices are seized and secured for examination. When investigators attempt to retrieve digital data, critical evidence in cybercrime investigations must be extracted from that digital domain. Digital evidence is [2]:

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

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

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

4) *Volatile:* It is volatile and sensitive.

### *B. Forensic Investigations in LEAs*

Cybercrimes often raise new challenges for the LEAs. Criminals were keeping up with the new technology while law enforcement lagged. The knowledge, skills, and abilities of investigators in the field of digital evidence are a necessary step in successfully pursuing cybercriminals. Investigators must have the capability to analyze any evidence retrieved in investigating cybercrimes [5]. Crime scene investigation in LEAs includes case analysis, report writing, and legal presentation [12].

*1) Case Analysis*

Different experts should independently report the case analysis.

*2) Report Writing*

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

*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. THE PROPOSED TRIAGE TRIANGLE STRATEGY OF DIGITAL FORENSIC COMPONENTS

Cyberspace introduces a wide range of new vulnerabilities criminals can use to take advantage of their victims. As new crimes emerge from the misuse of cyberspace, LEAs must change and develop their strategies to address previously unknown issues [8]. The proposed triage triangle strategy of digital forensic components is divided into three categories (Fig. 1): principles, forensics, and governance. This strategy helps LEAs deal with reducing digital forensic backlogs.

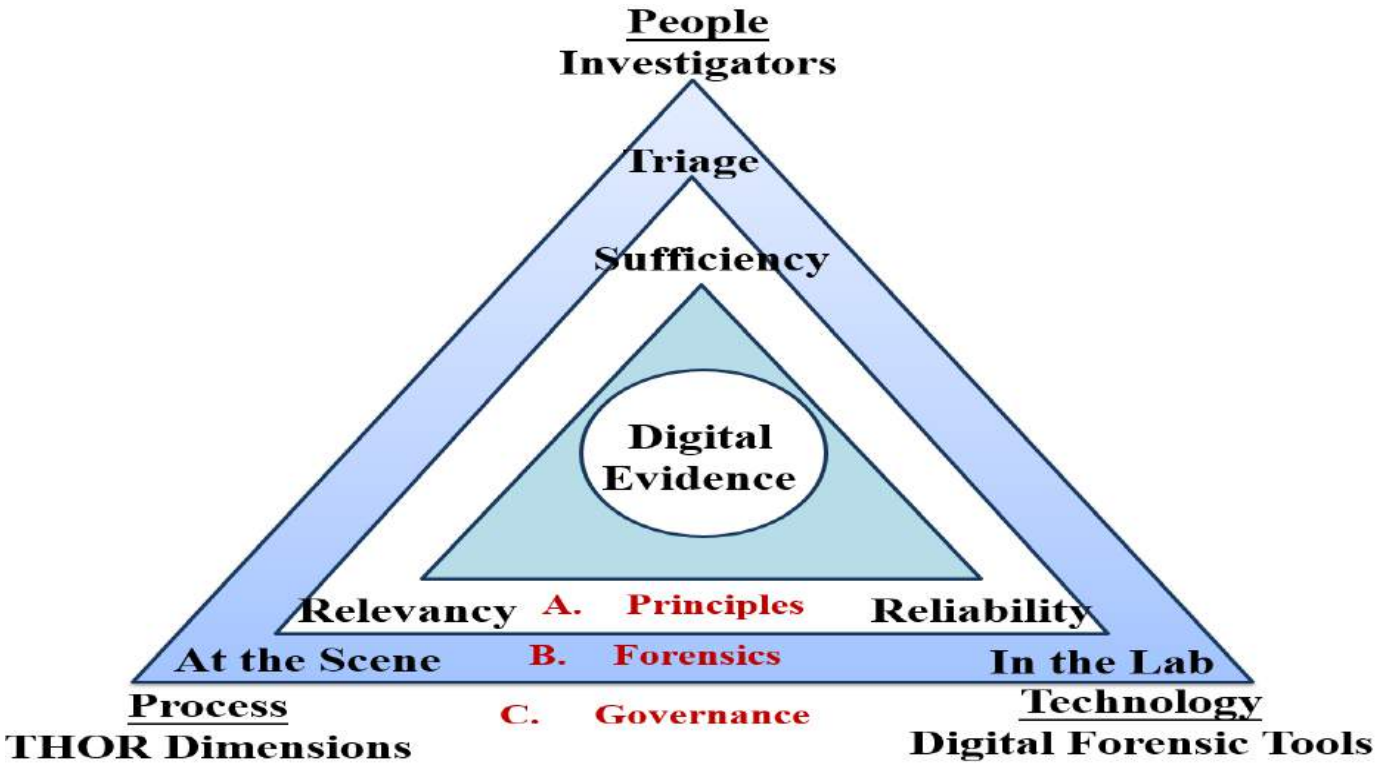


**Fig. 1.** Triangle strategy of digital forensics process

### A. Principles

Digital forensics is a branch of forensic science to encompass the investigation in electronic devices. It focuses on the recovery and analysis of raw data in digital devices. Investigators face numerous challenges, technical difficulties, or legal issues surrounding cybercrime investigations. It is essential not to overlook or minimize the vast amount of information stored in a computer, the nature of volatile memory, and a lack of sufficient strategies. The required principles for digital evidence handling should be satisfied as follows [6]:

*1) Sufficiency*

Investigators should be able to decide how much and which material to collect or acquire at the scene. They need to exhaust different methods, tools, and practices to identify, extract, and convert data to unequivocal evidence. There must be sufficient evidence to make the investigation convincing. They should have taken into consideration that enough material has been gathered to prove somethings.

*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 relevance of pertinent data affects the weight and usefulness of the evidence. Time, efforts, and cost spent in an 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 merely copying of data. All processes used in handling potential digital evidence should be auditable. Chain of custody should be preserved during collecting, examining, analyzing, 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.

### B. Forensics

Digital forensics deals with how data is gathered, investigated, recovered, found, analyzed, and stored in electronic devices in a court of law. Trace evidence in the computer environment falls within the realm of digital forensics. When people interact with people, places, and objects in the digital realm, these virtual traces will be kept as deleted file fragments, activity logs, document metadata, or email headers. They may be deemed to be of evidence value in identifying the origins of the parties involved in a criminal case. In Fig. 1, there are three forensic elements in our proposed triage triangle strategy. The detailed description is demonstrated in the following:

*1) Triage*

Most digital evidence investigation is completed at the scene promptly. Increasing cases and computers need to be analyzed effectively and efficiently. Specific investigations with a high level of technical difficulty are likely to be conducted in the lab [5]. 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 investigate in a limited time. Some digital forensic tools meet this need by extracting the recently changed files from a computer.

*2) At the Scene*

Investigators to any criminal complaint must ask the pressing questions at the very beginning and handle any relevant digital evidence appropriately at the scene. That will directly impact the effectiveness of an investigation and the admissibility of that evidence in court [5]. When first responders arrive at the 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 the Lab*

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

### C. Governance

There is always a continuous need for investigators to utilize tools in the effective handling of digital evidence and ensure a timely, valid, and accurate presentation to a court. These abilities of investigators may affect the tools used and the understanding of any evidence retrieved to ensure that the evidence is admissible in court [5]. This study proposes a minimum requirement for compliance with digital forensic processes.

*1) People: Investigators*

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 unplug a computer and expand the backlog as a mountain in the lab.

*2) Process: THOR Dimensions*

Investigators need proper processes to identify, collect, acquire, and preserve digital data. 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 [4]:

a) *Technical*-related to technology, technological approaches, and solutions.

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

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

d) *Regulatory*-related to law provisioning, standardization, and forensics.

*3) Technology: Digital Forensics Tools*

The ability to use appropriate digital forensic techniques and tools varies by agency and geographic location. These techniques and tools are not sufficient to keep pace with changes in digital devices. Proprietary sources for the software or hardware generally limit the particular discipline of purchased training courses in the digital forensics process. The need for freeware or open-source tools within digital forensics across all LEAs is critical for the nature of the discipline in legal proceedings [8]. The range of digital forensics includes computer devices, network servers, and mobile handsets. The following of digital forensic tools is designed for different types of examined targets.

a) *Memory Forensics:* Volatility, WindowsSCOPE, RAM Capturer, Magnet RAM Capture, and Memoryze.

b) *Mobile Device Forensics:* CelleBrite UFED, XRY, and Oxygen Forensic Suite.

c) *Network Forensics:* Wireshark, Network Miner, Xplico, and E-Detective.

d) *Computer Forensics:* EnCASE, FTK, Sleuth Kit Autopsy, TCT, and DEFT.

## IV. Discussions and Analyses

Computers now hold more information and more processing power than before. That brings a great challenge for LEAs to deal with increasingly large amounts of digital evidence. Investigators must have the capability to process large amounts of information accurately, completely, and promptly [8]. This practical method of reducing digital forensic backlogs becomes critical for LEAs.

### *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 proliferate [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 the injury situation of the patients to determine the priority treatment process [10]. First responders 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 the lab. The purpose of digital triage is to prioritize digital media and obtain quick intelligence. It is a solution to the problem of case backlogs [11]. Digital triage is the investigative beginning of the forensic examination. Fig. 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 the scene by non-digital evidence specialists to increase the efficiency of an investigation promptly and to decrease the examination backlog in the lab.

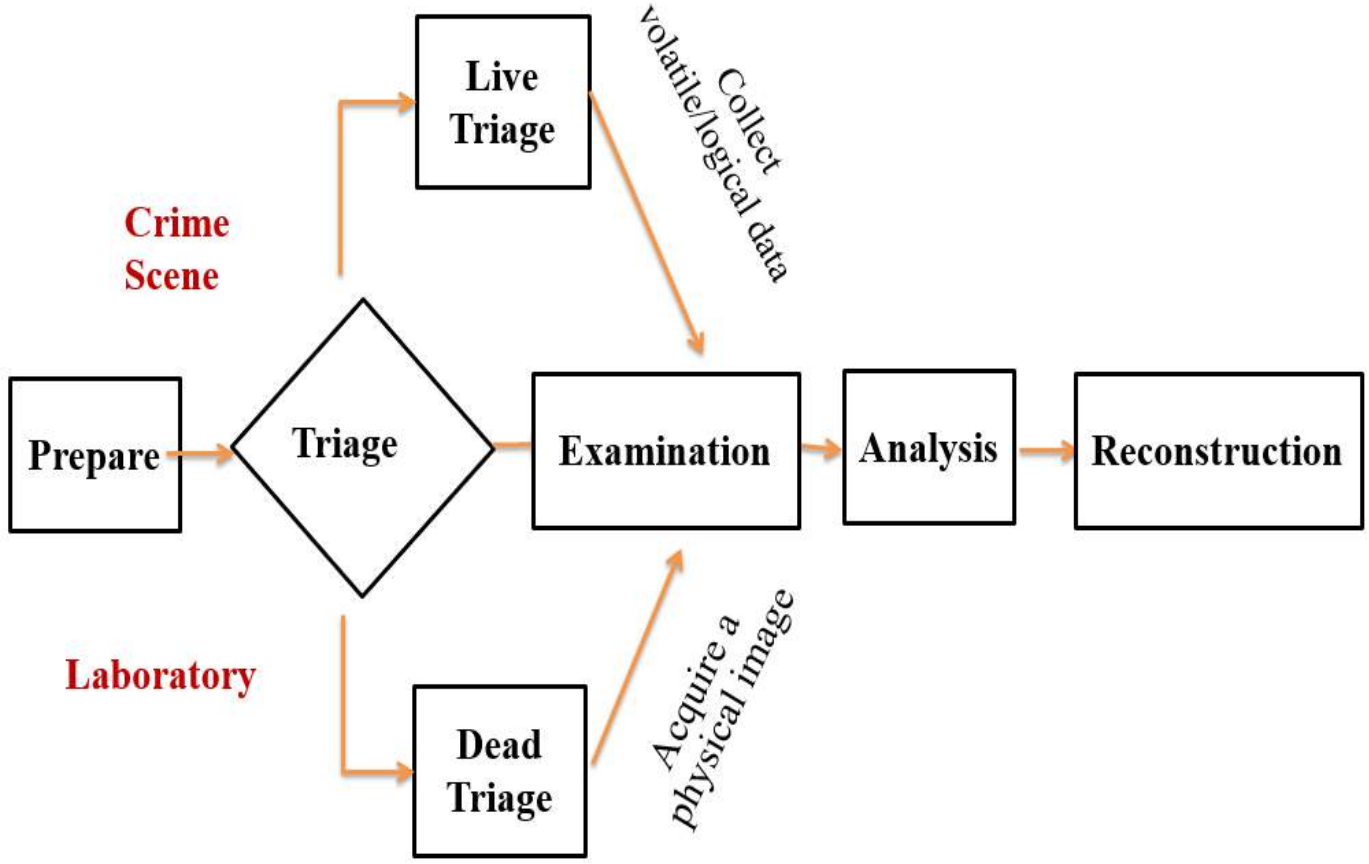


**Fig. 2.** The triage evidence process of TEAR phases in reducing digital forensic backlogs

*1) Live Triage: Volatile/Logical Data*

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

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

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

*2) Dead Triage: Physical Image Files*

Dead triage is conducted in the lab for the possible existence of the relevant evidence. Some types of tools are [10]:

*a) Acquiring a copy of the image file.*

*b) Indexing, searching, cracking, and analyzing digital content in digital media.*

*c)Presenting a forensic report*

*3) Scene Investigation*

Scene investigation focuses on the compelling evidence of the power-on status to detect and explore any possible answers to scenarios. At the scene, an active investigation of the primary memory content can be conducted to collect the volatile evidence under the power-on state quickly. The scene must be photographed or recorded appropriately. Turning off computer power is not the first thing to do at the 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 valuable evidence.

*4) Lab Forensics*

Lab forensics focuses on identifying results in the static evidence of shutdown status. In the 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 number of new cases for LEAs.

*B. TEAR Phases of THOR Dimensions in Digital Forensics*

An additional concern was the inability to communicate with other investigators, cross into other jurisdictions, and coordinate cybercrime investigations during investigations [5]. This proposed triage triangle strategy helps LEAs produce a quality report [6]. Fig. 3 also illustrates TEAR phases from the viewpoint of THOR dimensions to describe the proper practices for identifying, collecting, acquiring, and preserving the digital data [12]. The two axes represent the perspectives and processes of digital forensic investigation.

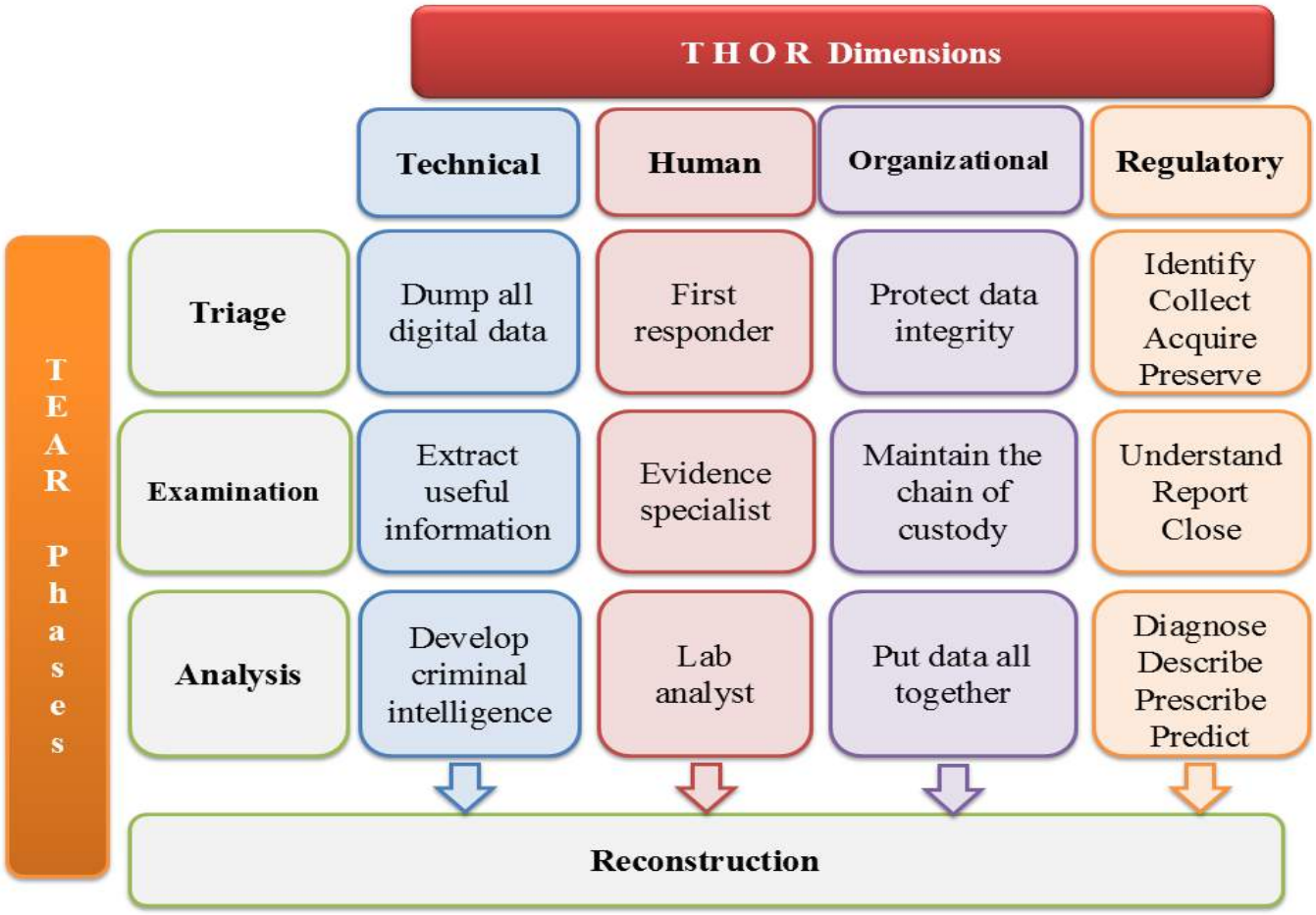


**Fig. 3.** The TEAR phases of THOR dimensions in the proposed triage triangle strategy

*1) Triage*

First responders can use a triage tool to preview data at the scene.

*a) Technical:* Some tools are available to dump relevant data.

*b) Human:* As technology changes, first responders must continually update their devices and training. They assist at the 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:* The ISO/IEC 27037:2012 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) Examination*

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

*a) Technical:* They use tools to extract useful information from collected evidence.

*b) Human:* They are responsible for documenting and preparing evidence once it arrives at the scene.

*c) Organizational:* They 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 and assists the court to close the case.

*3) Analysis*

Lab analysts should determine the processes necessary to complete the analysis.

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

b) *Human:* Forensics analysts who work in the lab combine relevant events into exploring the fact.

c) *Organizational*: They should put data altogether to help the court make the right decisions.

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

*4) Reconstruction*

Reconstruction refers to the systematic process of piecing together evidence and information gathered during a crime to gain a better understanding of what transpired between the victim and the criminal [3]. It involves ordering the evidential associations from temporal, relational, and functional analysis. Crime reconstruction is the determination of the actions and events for establishing the continuity 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 correct 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 Tools in Digital Forensic Investigations

Many LEAs use tools to examine a target machine or network [5]. Available tools can increase the speed of the digital forensic process and reduce the number of devices in the lab. That will reduce case backlog and improve the quality of first responders, evidence specialists, lab analysts, or investigators. Several tools for conducting cybercrime investigations in TEAR phases are introduced below (Table I) [11]. Well-planned use of digital forensic tools can improve efficient and effective investigations.

TABLE I
AVAILABLE TOOLS IN TEAR PHASES

| Phases | Functions | Tools |
|---|---|---|
| Triage | Identify artifacts in memory | Volatility, WindowsSCOPE, RAM Capturer, Magnet RAM Capture, and Memoryze |
| Examination | Examine images | FTK Imager |
| | Examine information from browsers | Dumpzilla |
| | Carve data files | SIFT |
| Analysis | Analyze information from a phone | CelleBrite UFED, XRY, and Oxygen Forensic Suite |
| | Parse the data of USB devices | USB Historian |
| | Acquire web pages | FAW |
| Reconstruction | Investigate the network-related activity | Wireshark, Network Miner, Xplico, and E-Detective |
| | Recover data from computer devices | EnCASE, FTK, Sleuth Kit Autopsy, TCT, and DEFT |

*1) Triage*

*a) Volatility:* It can identify the running processes, network activities, and open connections for volatile memory analysis of Windows, Linux, Mac & Android systems.

b) *WindowsSCOPE:* It enables memory forensics for Windows computers and provides the memory forensics analysis for security breaches. It can identify the processes, threads, and drivers running on the system.

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

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

e) *Memoryze:* It can create, acquire, and analyze an image and identify all running process, drivers, or malicious activities in live memory.

*2) Examination*

*a) FTK Imager:* It can create MD5 or SHA1 file hashes and examine files, memory dumps, or images.

*b) Dumpzilla*: It can examine the information from browsers.

c) *SIFT:* SANS Investigative Forensic Toolkit (SIFT) can carve data files, generate a timeline from system logs, and carry out forensic analysis.

*3) Analysis*

a) *CelleBrite UFED*: Cellebrite Universal Forensic Extraction Device (UFED) can extract information and recover deleted data from mobile devices.

b) *XRY:* It can analyze and recover information in a forensically sound manner from mobile phones, smartphones, and tablet computers.

*c) Oxygen Forensic Suite:* It can identify app accounts, communicated contacts, geolocation metadata, and other

information from a mobile phone. It can further analyze photos, documents, videos, and device database.

d) *USB Historian:* It can parse the USB history data from the computer.

e) *FAW:* Forensics Acquisition of Websites (FAW) can acquire web pages and files online.

*4) Reconstruction*

Evidence on computers and networks should be included to gain an understanding of a crime reconstruction [2].

*a) Wireshark*: It can capture the network-related activity, analyze network protocols, and support Windows, Linux, and Mac OS.

b) *Network Miner:* It can examine hostnames, sessions, open ports, and operating systems from network traffic.

*c) Xplico*: It can analyze email, HTTP contents, and VoIP call data from network traffic.

d) *E-Detective:* It can capture, decode, reassemble, and reconstruct various types of network traffic such as Email, Webmail, Instant Messaging, File Transfer, and VOIP.

e) *EnCase:* It can collect Internet artifacts, acquire data, and produce a report.

f) *FTK:* Forensic Toolkit (FTK) can crack a password, analyze emails, or look for specific characters in files.

g) *Sleuth Kit Autopsy:* It consists of command-line tools. It can analyze smartphones and hard disks.

h) *TCT:* The Coroner's Toolkit (TCT) can recover data from computer disasters under several Unix-related systems.

i) *DEFT:* Digital Evidence and Forensics Toolkit (DEFT) can gather, acquire, and preserve digital evidence on running systems.

## V. Conclusion

Cybercrimes have put LEAs at a significant disadvantage. There is still much work to ensure that LEAs have the necessary resources or tools in investigating cybercrimes. Digital forensics is a continuous procedure. Each phase has a high impact on the relevance, reliability, and sufficiency of the evidence. The increase of substantial digital evidence backlogs is encountered in a criminal investigation by LEAs throughout the world. The crime scene is often the driving force behind a successful criminal investigation. Properly collecting digital evidence is essential in cybercrime investigation. The examination of digital sources should be completed empirically, logically, and systematically consistent with organizational policy. With the development of information technology, investigators need to get the evidence quickly and sufficiently. This study explores this backlog challenge in digital forensics from a technical standpoint, proposes a triage triangle strategy, and contribute to an efficient digital forensic process. It is also critical to quickly assist the court in finding the root reasons for a case. This proposed strategy may improve the speed and quality of investigations.

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

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

[4] Choraś, M., Project Final Report: Comprehensive Approach to cyber roadMap coordINation and develOpment, ITTI Sp. Z o.o., Poland, pp. 15-39, 2016.

[5] Cummins Flory, T. A., "Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies," *Journal of Digital Forensics, Security and Law*, Vol. 11. No. 1, pp. 7-38, 2016.

[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] Keeling, D. G. and Losavio, M., "Public Security & Digital Forensics in the United States: The Continued Need for Expanded Digital Systems for Security," *Journal of Digital Forensics, Security and Law*, Vol. 12. No. 3, pp. 47-60, 2017.

[9] Losavio, M.M., Chow, K.P., Koltay, A., and James, J., "The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security, *Security and Privacy,* Vol. 1, No. 3, pp. 1-11, 2018.

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

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

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



Da-Yu Kao received the B.S. and M.S. degree in Information Management from Central Police University, Taiwan, in 1993 and 2001, the Ph.D. degrees in Crime Prevention and Correction from Central Police University, Taiwan, in 2009, respectively. From 1993 to 1996, he was with Taipei City Police Department, Taiwan, where he was an information technology police officer involved in the development of policing information systems. From 1996 to 2007, he was with Criminal Investigation Bureau, National Police Administration, Taiwan, where he was a detective and forensic police officer in cybercrime investigation and digital forensics. From 2007 to 2013, he was with Maritime Patrol Directorate General, Coast Guard Administration, Taiwan, where he was an information technology section chief in the department of information and communication. Since 2013, he has been with Central Police University, Taiwan, where he is currently an associate professor in the Department of Information Management. His research interests include cybercrime investigation, digital forensics, digital evidence, information management, criminal profiling, and cyber criminology.



Ni-Chen Wu received the B.S. degree in Information Management from Central Police University, Taiwan, in 2019. Since 2019, she is a police officer in Taiwan. Her current research interests include information security, incident response, cybercrime investigation, digital forensics, information systems management, criminal profiling, and cyber criminology.



Fu-Ching TSAI received the B.S. degree in Information Management from Central Police University, Taiwan, in 2001, the M.S. and Ph. D degrees in Institute of Information Management from National Cheng Kung University, Taiwan, in 2005 and 2013. Since 2018, he has been with Central Police University, Taiwan, where he is currently an assistant professor in the Department of Criminal Investigation. His research interests include big data analysis, data mining, text mining, and artificial intelligence.