

24th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems

An AutoTriage B-CoC model in digital forensic investigation

Po-Yu Jung^a, Fu-Ching Tsai^{a*}^a Department of Criminal Investigation, Central Police University, Taoyuan, Taiwan, R.O.C.

Abstract

With the high technologies are wildly adopted in illicit activities, the high volume and complexity of digital evidence make the collection task at the crime scene a great challenge. Triage is a well-known solution to give a quick review and prioritize the data regarding the admissibility of digital evidence. However, conducting triage at the crime scene may lead to evidence contamination due to limited time, space and human resources. And these common vital mistakes are fatal to the prosecution. In order to facilitate the effectiveness of the on-scene criminal investigation, we propose an AutoTriage B-CoC model to support automatic triage collecting and blockchain uploading. The superior accuracy and completeness of the digital evidence can be achieved without human interfering. The experimental results show that the on-scene examiner can manage the preservation and collection of digital evidence by typing two key values, CaseID and EvidenceID. We expect the detailed design of operations regarding to four phases, i.e. Triage, Documentation, Blockchain and Report, can provide important guidance for further practical applications.

© 2020 The Authors. Published by Elsevier B.V.

This is an open access article under the CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0>)
Peer-review under responsibility of the scientific committee of the KES International.

Keywords: Triage; Blockchain; Chain of custody

1. Introduction

The crime scene examination is critical and treated as the first step of the investigation process [1-3]. The information retrieved from the crime scene is vital for the admissibility of evidence for court purposes. However, conducting subsequent searching in the crime scene is a great challenge. When law enforcement officers successfully apply for a search warrant after a long time of investigation on a suspect and finally have the chance to seize the crime scene. The very first question that comes in mind is, "what items should be seized first?" [4]. Unlike the first responders in civil cases, law enforcement officers at the crime scene, are unlikely to acquire any disclosure from criminals to start an outward search. It is worth noting that this situation is more difficult in the digital forensic field.

Since the evidence in digital form is hard to be recognized compared to physical evidence, law enforcement practitioners need to figure out what devices may contain pertinent evidence [2, 3, 5-9]. Moreover, with the trend of high technology involving in criminal activities, crime scene examiner needs to search for various devices like computers, mobile phones, tablets, or even data stored in the cloud. When the volume and complexity of evidence are increasing, it is almost impossible to pack and transport every electronic device at the crime scene [10]. Therefore, providing an adequate process to prioritize the digital evidence in limited time is necessary for modern crime scene investigations [11].

*Corresponding author. Tel.: + 886-3-328-2321; fax: +886-3-328-4118.

E-mail address: fctsai@mail.cpu.edu.tw.

Forensic triage is a methodology that supports crime scene examiners collecting, analyzing and classification of relevant items and facilitate the efficiency to interpret digital evidence on-scene [1]. The triage procedure can provide instant information about the digital content in target devices without transmitting the evidence back to the forensic lab. Therefore, the quick responses from on-scene triage are essential for the first responders. There are several well-known triage tools that are applied to practical applications to support collecting pre-fetch files, registry files and logfiles [12]. But it is worth noting that the triage results may also be tampered due to inexperienced officers violating the integrity and authenticity of digital evidence. Digital evidence is easy to be altered or destroyed due to its fragile nature [9]. Unfortunately, the common vital mistakes are fatal to the prosecution. As far as our knowledge, how to maintain the integrity of triage results at the crime scene and avoid the human error when seizing under emergent conditions is rarely discussed in current researches.

In order to fill the gap between the efficient triage procedure and the immutable triage results, we propose a prototype that utilizes the automation of triage collection and blockchain technology to facilitate the efficiency of on-scene investigation and ensure tamper protection for digital evidence. The remainder of this paper is organized as follows: in section 2, we analyze the state-of-the-art digital forensic models followed by addressing the research gap in the on-scene criminal investigation. In section 3, we propose the prototype by using blockchain technology to enhance the audibility of digital evidence in criminal case management. In section 4, we demonstrate the experiment result. Finally, the last section concludes the paper and makes some suggestions for future work.

2. Literature review

2.1. Triage in digital forensic models

With the emerging trend of new technologies been wildly adopted in modern illicit activities, almost every crime has electronic devices that might be crucial for further investigation. Therefore, digital forensic plays an important role in providing authentic facts in legal proceedings. However, unlike traditional forensic sciences, such as chemistry and physics, the new inventing digital forensic is still at the initial exploring stage [8]. For example, the question of "what is the best digital forensic strategy?" is under discussion in current researches [6, 9]. Therefore, the courts usually rely on previous principles, which used to test "classical evidence", to verify the reliability of "digital evidence", such as the Daubert test is taken in the United States [2]. When the evidence is presented to the court, there are two aspects of digital evidence that must be considered, namely legitimacy and scientificity. The legitimacy focuses on ensuring the authenticity and integrity of evidence, such as the well-known "Fruits of the Poisonous Tree" doctrine and the "Chain of Custody" rule. On the other hand, scientificity focuses on ensuring the verification of the evidence is correct.

In order to ensure the scientifically reliable and legally accurate of digital evidence, various digital forensic models have been proposed. The objectives of these researches are to explore applicable skills and procedures for collecting and analyzing digital content. In this research, we focus on the evidence collecting phase at the crime scene. When conducting an on-scene search, identifying devices that contain potential digital evidence is the very first step. This initial step determines the consequent strategies to facilitate the recovery of evidence.

To quickly examine possible devices, the CFFTPM (Computer Forensics Field Triage Process Model) triage process is proposed, which is a compromising method between ideal lab examining and practical use. The triage process supports an effective preview of digital evidence so as to rank the evidence items in terms of importance or priority. Consequently, the evidence which is the most important or the most volatile need to be dealt with first [1]. Utilizing the triage process helps reduce the potential backlog and associated delays in digital evidence gathering [10, 13]. More importantly, the triage process does not preclude the lab phase for a more detailed examination and analysis [1].

Triage applications are typically used for preserving volatile data, such as network status, process data, user's activity, registry logs, system event logs. However, the triage application would inevitably change the potential evidence's file system and registry more or less [12]. Therefore, the detailed documentation is required to record the trail of every possible alternation on digital evidence.

2.2. Documentation in digital forensic models

Although the triage process can help the on-scene examiners searching admissible evidence, the triage applications, in most situations, are designed by commerce, and the producers always refuse to show their source code [14]. Therefore, the court may doubt whether or not theses triage applications would alter the evidence so as to impair its integrity. Thus, the SWGDE (Scientific Working Group on Digital Evidence) suggests that examiners should document the triage process in sufficient detail to allow its repetition and account for artifacts created by the triage process [11]. In order to preserve the audit trail, the complete documentation is required.

ACPO (Association of Chief Police Officers) states that "an audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result" [15]. Most of the existing model emphasized the importance of documentation or contemporaneous notes, but when

and how it differs from each other. For example, should the on-scene examiner document everything during the investigation process [16], or document the entire scene and the specific location of the evidence [17]? Robin Verma proposed the Digital Forensic 2.0 model [18], using machine learning to triage and add the logging system to record all system operations and investigator actions. Verma indicated that there are two reasons. Firstly, to resolve conflicting situations like allegations of data privacy violations. Secondly, for studying investigation styles of examiners for learning and training purposes.

Documentation or logging the triage process need to be both complete and tamper-proof. There are two possible solutions to achieve this goal [18]. The first solution is to capture the activity logs with the help of the dedicated application running on the forensic environment, which needed the examiners to be honest and not to interfere with the logging system. The second solution is to capture the examiner's activities in the operating system and save the logfile to a safe location. Either of them have pros and cons. In this research, we propose a model that can automatically log the process of triage and upload the logging results into the blockchain. By automatically uploading the chain of custody to the blockchain, the results can avoid the alternation by human error and ensures the data not be tampered.

Highly automated digital forensics sometimes referred to as push-button forensics (PBF), has received much criticism from the digital investigation community [19]. Some researchers consider that digital forensic investigation is a complex procedure, so it is improper to use the fully automatic application through the entire investigation. Nevertheless, utilizing an automatic process can successfully reduce human intervention and decrease the error rate [20]. Therefore, we try to use an automatic mechanism to preserve the documentation outcome of the evidence triage process so as to guarantees the audit trail before the acquisition.

2.3. Blockchain

The blockchain technology can be seen as a decentralized public ledger of all transactions across a peer-to-peer network, which means it has two characteristics. The first characteristic is decentralized, which means users can confirm transactions without the need for a central certifying authority. The second one is tamper-proof. Once the transaction is verified, it is permanently written in the block. The United States Department of Commerce National Institute of Standards and Technology (NIST) and The United States Department of Homeland Security (DHS) has created a flowchart to decide whether a blockchain is needed [21]. It has mentioned 6-factors that need to be considered: (1) Need a shared consistent data store. (2) More than one entity needs to contribute data. (3) Updated data does not need to be modified. (4) Sensitive information does not need to be uploaded. (5) Having a hard time deciding who should be in control of the data store. (6) Need a tamper-proof log of all writes to the data store.

Whenever the digital evidence has delivered to the court, there is always one thing that needs to be proved "Does the data have tampered?" Nowadays, the court and the practitioners use the paper-based chain of custody. Every time the parties dispute about the evidence has tampered or not, the court needs to summon the examiners or the evidence collectors to the court, testifying how they acquired the evidence and how the evidence was handled since acquisition. Thus, providing a shared consistent data store and a tamper-proof log of evidence is critical for the judicial process.

The immutability and authenticity of blockchain are appropriate for audit evidence transactions. Therefore, we can use the advantages of blockchain to demonstrate the detailed history of digital evidence records. Previous researches have proven that the blockchain technology can be used as a mechanism ensuring the traceability of chain of custody [22, 23]. Blockchain-based chain of custody (B-CoC) had dematerialized the chain of custody to the blockchain, which is able to guarantee auditability of the evidence. However, previous models rarely discuss how to decrease human error and maintain efficiency. Law enforcement officers usually suffer from limited time and resource at the crime scene. The more manually operating procedures there is, the higher error rate may cause. Therefore, we propose an automatic triage B-CoC model.

3. AutoTriage B-CoC model

3.1. Model construction using DSRP

In this study, we apply the Design Science Research Process (DSRP) to fill the gap between triage and blockchain in digital forensic. The DSRP is suitable for the task of creating and evaluating a new process model[2, 9]. We demonstrate the AutoTriage B-CoC model by following the six steps of DSRP, which are (1) problem identification and motivation, (2) objectives for a solution, (3) design and development, (4) demonstration, (5) evaluation, (6) communication.

3.1.1. Problem Identification and Motivation

For more effectively collect the high complexity and large volume of data at the crime scene, the triage process is essential to retrieve relevant information. But triage log also undoubtedly may suffer from contamination by untrained detectives. This study aims to utilize an automatic triage procedure to avoid human errors. In addition, the current paper-based chain of custody is insufficient to provide transparency when digital evidence is improperly modified or reproduced. To fill the above gap, we integrate automation triage and blockchain in this study.

3.1.2. Objectives for a Solution

The objective of this research is to propose a model named AutoTriage B-CoC, to avoid unintentional errors in the triage process and ensure the immutability of digital evidence by blockchain technology.

3.1.3. Design and development

Through the literature review, we identify the research gap related to on-scene digital forensic investigation. We design a model that supports document every step taken in the identification process and ensure the log file remains unchanged by automatically uploading the logfile of the triage process to a trusted third party database. The mechanism can prevent human intervention or intentional modification. Furthermore, we use blockchain to maintain the integrity of the chain of custody.

3.1.4. Demonstration

In this study, we use typical cases to determine the applicability of the Autotriage B-CoC framework. This is a recognized method used by previous researches [2, 3, 5, 6, 9, 24, 25].

3.1.5. Evaluation

The proposed AutoTriage B-CoC framework needed to be evaluated to determine how well it supports the solution to the identified problem. In this phase, the AutoTriage B-CoC will be submitted to law enforcement, prosecutors, judges, and researchers in academia. The aim is to acquire insightful and reliable feedback from authoritative external reviewers, which can help rolling wave planning.

3.1.6. Communication

For receiving feedback from the proposed model, we will collect the suggestions from users' experience and communicate with them directly. The feedback would help to improve the performance of the AutoTriage B-CoC model.

3.2. AutoTriage B-CoC model

In this study, we take Ethereum as the platform due to its smart contract support. The smart contract is like a script that will execute certain movements when the condition is met. Smart contracts are the databases without the connection to the real-world data. In order to build the connection as a data-feed service in practical application, we add oracle services to the AutoTriage B-CoC. Secondly, we add the event to the AutoTriage B-CoC, which can emit the information to the transactions, thus by looking at the detail of transactions, we can check the evidence information. Furthermore, we can flexibly design the arguments and add them to the topic, easy to use filter searching, such as Case[CaseID] and EvidenceHash. As such, we propose an AutoTriage B-CoC framework, which composed of four dimensions, Triage, Documentation, Blockchain and Report, as shown in Fig. 1.

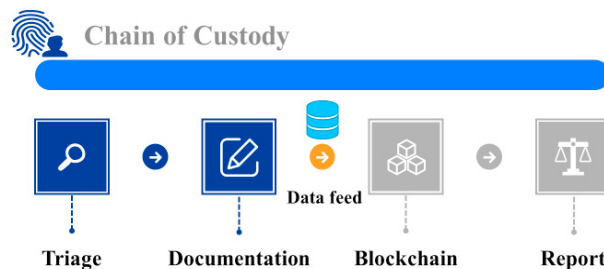


Fig. 1. AutoTriage B-CoC framework workflow

3.2.1. The triage phase

- Search – searching for the physical devices that may contain relevant evidence.
- Identification – find out which devices contain relevant evidence. This step may need to interact with the devices in a forensic sound manner. And the person needs to have competent knowledge to do so.
- Triage – Whenever its possible, practitioners using an automatic application to find out whether this device does contain relevant evidence, thus prevent backlog and save time. In some situations, it is not suitable to use the automatic application, take the different operating systems; for instance, practitioners can not use a Windows triage application in Linux. As such situation, practitioners need to use the forensic sound manner and manually triage the device.
- Seizure – comply with local laws and seize the devices contain relevant evidence and the item listed on the search warrant. If not, do not seize it.

3.2.2. The Documentation phase

- Logging system – this system simultaneously starts when identification starts, namely, every action taken in the triage process to the potential devices needs to be documented.
- Automatic upload logfile to the trusted database – this step is using the help of scripts to automatically upload the triage logging system once the logging system creates logfile. The logging system will have the following information that certain information was input by the practitioners: (1) CaseID, (2) EvidenceID.
- Trusted database – The evidence information will be stored in the trusted database, and through the help of oracle, the evidence information will synchronize with the smart contract. Even the database was attacked and the evidence information was modified, the blockchain will have the audit trail to examine which information is incorrect.
- Update the Evidence information – this step is not only for law enforcement but also for the attorney, prosecutors, and judges to update the receivers and transferring time when handling the evidence.

3.2.3. The Blockchain phase

- Create Case/Evidence – this step is for the authorized staff who only need to type in the CaseID and EvidenceID. Then the data feed feature, such as Oracle, will automatically query the information from the trusted database. The uploaded information is as follows: Evidence Hash, Triage Log, Evidence Description, Collecting Time, Collector, Transferring Time, Current Owner, and Active status. Only the Evidence Hash, Logfile Hash, and Active status are set public viewable. Take the privacy and the principle of non-disclosure investigation into consideration, except for the features mentioned above, the rest of the evidence information can only be seen by the authorized staff.
- Oracle- By using the data-feed feature, we synchronize the evidence information with the smart contract. Whenever the status of evidence changed in the database, the oracle will retrieve the data from the database and send it to the smart contract. In the meantime, the smart contract will generate a transaction and add it to the block.
- Transaction- The two useful information in the transaction log are data and topics. Data is the evidence information written in the transaction. And topics can be seen as a filter that can be used to index the argument in the smart contract, such as CaseID and EvidenceID. We can use the decentralized application(DAPP) to interact with the transaction and look for the information we want.

3.2.4. The Report phase

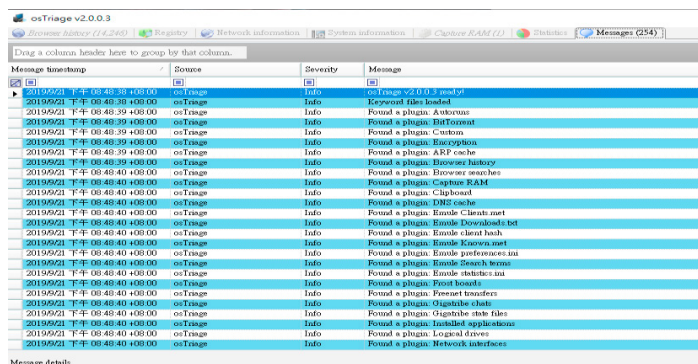
- Presentation – Whenever there is a need to examine the digital chain of custody, such as judges or the evidence successor, they can check the storage information in the smart contract. For further inspection, they can use decentralized applications via web3 filter to flit out every transaction and see every changed information in the block.

4. Experimented result and discussion

4.1. Tool selection

There are numerous triage products in the market. The considerations for selecting tools depending on the environment, devices, and operating system. In this study, we tested typical triage application Ostraiage version 2, which is designed by the FBI and released in 2015, suitable for investigating child pornography.

We tested osTriage in the Windows 10 operating system and analyzed the report. We discovered that typical triage application does contain what most interested the practitioners, such as files name, hash, created time, last modified time, and preview et cetera. However, it still lacks the source code that can be seen and justified by third parties or the logfile that recorded what the application did to the devices. The screenshot of osTriage is shown in Fig. 2.



Message timestamp	Source	Severity	Message
2019/02/17 00:40:30:000	osTriage	Info	osTriage v2.0.0.3 loaded
2019/02/17 00:40:30:000	osTriage	Info	Keyboard files loaded
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Antivirus
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: BitTorrent
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Custom
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Encryption
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: ARP-cache
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Browser history
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Browser cookies
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Capture RAM
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Clipboard
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: DNS-cache
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Enable Clients.net
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Enable Downloads.net
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Enable cloud hash
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Enable Known.net
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Enable performance.ini
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Enable Search terms
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Enable statistics.ini
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Print results
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Firewall transfers
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Ghostfile chat
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Ghostfile new files
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Installed applications
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Logical drives
2019/02/17 00:40:30:000	osTriage	Info	Found a plugin: Network interfaces

Fig. 2. The screenshot of Ostraiage.

We tested another application called Problem Steps Recorder, designed by Microsoft, which was first used to record the process causing problems. Problem Steps Recorder is like a combination of screen capture and annotation tool. It does not record the typed text. Still, it documented where we clicked and what did we do to the computer in script and snapshots. Screenshot of Problem Steps Recorder shown in Fig. 3.

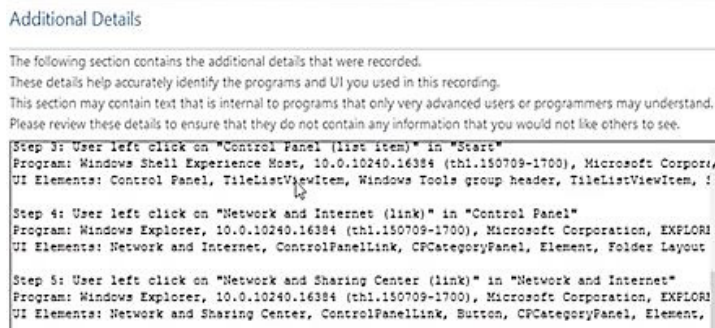


Fig. 3. The screenshot of Problem Steps Recorder.

Oracle is the connection between smart contracts and the real world. It is vital that choosing reliable and provable oracle services. Since Chainlink is an oracle service, which is famous for its decentralized system, providing information that observed and retrieved by more than one node, hence prevent the situation that the oracle node occasionally retrieves the wrong data. It is more reliable than one node oracle services. In addition, we choose the Google Cloud platform as our database. The concept of using Chainlink to connect Ethereum and Google Cloud is as below: When smart contract applications request data from Chainlink, Chainlink will retrieve data from the Google Cloud in return.

4.2. Run through presume scenario

Case Scenario: The local police department received a report that someone might be pedophilia. After a period of investigation, the detective successively applied for a search warrant. Then the detective came to the suspect's house and showed the warrant to the suspect. After controlling the suspect at the crime scene, the detective needs to collect the potential evidence and also preserve the integrity of the chain of custody. Since the search warrant declared only the property that contains evidence should be seized. Law enforcement followed the AutoTriage B-CoC framework to acquire admissible digital content and preserve the chain of custody as follows.

4.2.1. The triage phase

- The detective searched for any device that may contain child porn or relevant evidence. He found a power-on windows desktop and a power-off laptop.
- In order to find out the devices which stored child porn, the detective decided to examine the power-on desktop quickly.
- The detective used Steps Recorder to document every step taken to the computer. Meanwhile, he plugged in the USB that contains osTriage application, and input the relevant fields, such as caseID, EvidenceID, collector's name, collecting time, and started triage.

4.2.2. The documentation phase

- After the triage process, the detective stored the logfile, which contains every step is taken and the screenshot, into a clean-acquisition laptop. The scripts automatically transfer logfiles into JSON and stored in the trusted database(google drive). Meanwhile, google cloud platform use BigQuery, the google drive API, to access the logfiles for later chainlink data query.
- The power-off laptop is taken back to the laboratory for further examination and acquisition. The evidence information stored in the power-off laptop should also be transferred to JSON format to BigQuery.

4.2.3. The blockchain phase

- The authorized staff interact with the smart contract and use the function "Create", inputs the CaseID and EvidenceID. Once the request was confirmed, the transaction will be documented to the blocks and stored the evidence information permanently into the blockchain. Chainlink will automatically synchronize the evidence information with the smart contract.
- When evidence is transfer to others, such as examiner, attorney, prosecutor, and judge, they need to update information in google cloud. Thus, Chainlink will automatically update the evidence's current owner and transfer time.

4.2.4. The report phase

- Whenever law enforcement officers, attorneys, prosecutors, and judges want to see the information of the chain of custody, they only need to use decentralized applications to interact with transactions. By querying the indexed arguments, such as CaseID or EvidenceID, the users can easily look up the whole process of the case and evidence. As for irrelevant people, they can only see the public information, such as evidence hash, logfile hash, but not allowed to see the private content of the case.

5. Conclusion

With more electronic devices been wildly applied in criminal activities, the successful prosecution of a suspect is highly related to the skill of on-scene investigation and the immutability of digital evidence. In order to diminish human error in the on-scene investigation and facilitate the integrity of digital evidence, we proposed an AutoTriage B-CoC framework, which can automatically proceed triage, transform logfile into JSON format and upload it to the online Google Drive. The experimental results show that we successfully reduce the chaos of digital evidence collection at the crime scene. The only task that on-scene examiners need to do is typing CaseID and EvidenceID. By automatic uploading triage results through the Oracle interface, the blockchain also ensures the integrity and traceability of digital evidence. We expect the detailed design of operations regarding four phases, which are Triage, Documentation, Blockchain, and Report can provide important guidance for further practical applications.

Acknowledgment

This research was supported by the Ministry of Science and Technology of the Republic of China under the Grants (MOST 108-2410-H-015-001 –) and partially supported by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-109).

References

1. Rogers, M., et al., *Computer Forensics Field Triage Process Model*. The Journal of Digital Forensics, Security and Law, 2006.
2. Adams, R., *The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice*. 2012, Murdoch University.
3. Carrier, B. and E.H. Spafford, *Getting physical with the digital investigation process*. International Journal of digital evidence, 2003. **2**(2): p. 1-20.
4. McKemmish, R., *What is forensic computing?* 1999: Australian Institute of Criminology Canberra.
5. Casey, E., *Digital evidence and computer crime: Forensic science, computers, and the internet*. 2011: Academic press.
6. Valjarevic, A. and H.S. Venter. *Harmonised digital forensic investigation process model*. in *Information Security for South Africa*. 2012. IEEE.
7. Baryamureeba, V. and F. Tushabe. *The enhanced digital investigation process model*. in *Proceedings of the Fourth Digital Forensic Research Workshop*. 2004.
8. Cohen, F.B., *Digital forensic evidence examination*. 2012: Fred Cohen & Associates Livermore.
9. Montasari, R., *The Comprehensive Digital Forensic Investigation Process Model (CDFIPM) for Digital Forensic Practice*. 2016.
10. Pearson, S. and R. Watson, *Digital triage forensics: processing the digital crime scene*. 2010: Syngress.
11. SWGDE, *Best Practices for Computer Forensic Acquisitions*. 2018.
12. Shiaeles, S., A. Chryssanthou, and V. Katos, *On-scene triage open source forensic tool chests: Are they effective?* Digital Investigation, 2013. **10**(2): p. 99-115.
13. Gentry, E.E., *SEAKER: A Mobile Digital Forensic Triage Device*. 2019, California State University Channel Islands.
14. Marshall, A.M. and R. Paige, *Requirements in digital forensics method definition: Observations from a UK study*. Digital Investigation, 2018. **27**: p. 23-29.
15. ACPO, *Good Practice Guide for Digital Evidence*, T.A.o.C.P. Officers, Editor. 2012.
16. Köhn, M., M.S. Olivier, and J.H. Eloff. *Framework for a Digital Forensic Investigation*. in *ISSA*. 2006.
17. DOJ, *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*. 2008.
18. Verma, R., G. Gupta, and D. Chang, *Digital Forensics 2.0: an automated, efficient, and privacy preserving digital forensic investigation framework*. 2018, IIIT-Delhi.
19. James, J.I. and P. Gladyshev, *Challenges with automation in digital forensic investigations*. arXiv preprint arXiv:1303.4498, 2013.
20. Butterfield, E., et al., *Automated Digital Forensics*. 2018.
21. Yaga, D., et al., *Blockchain technology overview*. arXiv preprint arXiv:1906.11078, 2019.
22. Lone, A.H. and R.N. Mir, *Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer*. Digital Investigation, 2019. **28**: p. 44-55.
23. Bonomi, S., M. Casini, and C. Ciccotelli, *B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics*. arXiv preprint arXiv:1807.10359, 2018.
24. Beebe, N.L. and J.G. Clark, *A hierarchical, objectives-based framework for the digital investigations process*. Digital Investigation, 2005. **2**(2): p. 147-167.
25. Ciardhuáin, S.Ó., *An extended model of cybercrime investigations*. International Journal of Digital Evidence, 2004. **3**(1): p. 1-22.