Next Generation Digital Forensic Investigation Model (NGDFIM) - Enhanced, Time Reducing and Comprehensive Framework

Next Generation Digital Forensic Investigation Model (NGDFIM) – Enhanced, Time Reducing and Comprehensive Framework

Akash A Thakar[1], Kapil Kumar[2], Baldev Patel[3]

[1]Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad – 380009, India
[2]Associate Professor, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad – 380009, India
[3]Department of Microbiology, Gujarat University, Ahmedabad – 380009, India

E-mail: kkforensic@gmail.com

Abstract. Rapid technological advancement can have a substantial impact on the process of digital forensic investigation and presents numerous challenges to the investigator. With these challenges, it is imperative to have a standard framework for the digital forensic investigation to be implemented within most incidents. This induces a great stride to formulate a non-specific framework that may be applied to most digital investigation procedures. The Next Generation Digital Forensic Investigation Model (NGDFIM) formalizes the framework to facilitates the practitioners in the investigation process. This framework could potentially generate more evidence during the incidence response through on-site triage as compared to conventional investigations process. Moreover, the framework diminishes the analysis time and provides the suspect with privacy protection by incorporating custom content imaging.

1. Introduction

Information and communication technologies (ICT) has significantly progressed in recent years. It brings substantial advantages to the lives of individual and entities. Within the time of digitization, individuals are utilizing information and communication technologies for their assistance in day to day work. However, the high use of the internet and digital devices heightens the risk of cybercrime. Nowadays cybercrimes are most favorable for criminals because perpetrators do not require to present at the scene of crime, which makes it difficult to detect and bring charges before the courts. Attackers are using sophisticated tools and techniques for exploiting vulnerabilities present in the system or network. To mitigate such crimes, the investigator must reveal the footprints of the criminal from potential evidence. In the court of law, the evidence collection and analysis process is given high importance for the admissibility of evidence. Digital forensics is vital to a successful digital crime prosecution. However, Digital forensic investigators are facing many challenges like big data, encryption, anti-forensic techniques, anonymity, etc. To answer such challenges, many tools and frameworks have been designed but from the best knowledge of the author, it can be said that most of the frameworks and models were focusing on data imaging and recovery process. Numerous evidences may be found from other artifacts, though that are unclear to date**.** Therefore, a formal digital forensic investigation framework is needed to identify and analyze vital digital evidence. In this paper, we

proposed the enhanced, time reducing, and more precise framework for the digital forensic investigation that provides data integrity of the evidence, as well as privacy protection to the suspect during the investigation.

The rest of the paper is structured as follows: The related work is elaborated in Section 2. In section 3, the proposed framework is explained and the final section concludes the work.

2. Related work

Digital forensic is an emerging field for the last few years. Innovations in technologies like social networking sites, cloud computing technologies, mobile technologies, the dimensions of information, encryption, anti-forensic tools, utilization of private and portable browsers, varieties of malware, etc. lead the forensic investigators to numerous morden challenges and make the investigation more complex and cumbersome. To answer these challenges, a comprehensive, advanced and scientific digital forensic process model is required.

A number of researches have been carried out in this field. From the best knowledge of the authors, the first article on the digital forensic investigation model was presented by Michael Pollitt [1]. He mapped the proposed model with the admissibility of documentary evidence to the court of law. The article classifies four phases for the admissibility of any evidence to the court as follows: *Acquisition → Identification → Evaluation → Admission as Evidence.* They conclude that digital evidence must be scientifically accurate and legally acceptable and that the process should prove law and science.

In the Digital Forensic Research Conference, Gary Palmer described the standard digital forensic investigation process that could be implemented to most of the investigating and prosecuting of digital devices [2]. The model represents an essential baseline for subsequent work. The framework consists of seven steps as follows: *Identification → Preservation → Collection → Examination → Analysis → Presentation → Decision*.

In 2002, Reith et al. developed an abstract digital forensic framework to enhance the model developed by DFRWS [3]. The presented model comprises nine steps as follows: Identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence. According to the authors, the framework standardizes the digital forensic investigation process.

In 2003, an integrated digital investigation process (IDIP) was described by Carrier and Spafford for corporate and legal investigations [4]. The framework was developed from physical investigation theories and techniques. The physical investigation model was mapped with a digital investigation model. The model comprises 17 phases arranged in five groups as follows: Readiness phase, deployment phase, physical crime scene investigation phase, digital crime scene investigation phase, and review phase.

Peter Stephenson proposed a comprehensive End-to-End Digital Investigation (EEDI) framework [5]. The method lets the investigator utilize a structured investigation method by digital technology along with the traditional method. An author defines the process of DFRWS as class and the actions that are defined as elements. Six classes are defined and the author encompasses processes into nine steps. Finally, nine steps were represented by Digital Investigation Process Language (DIPL) and colored petri net modeling.

In 2004, Baryamureeba and Tushabe introduced an Enhanced Integrated Digital Investigation Process (EIDIP) [6]. It was based on the conceptual IDIP model developed by Carrier and Spafford [4]. An author identifies the machine as the primary scene of crime and the physical scene of crime as a second. In the EIDIP model, two additional phases introduced by the author are, traceback and dynamite. It distinguishes among the primary crime scene and the secondary crime scene. Readiness, deployment, traceback, dynamite, and analysis are the phases mentioned in the EIDIP.

In the study, Carrier and Spafford presented a framework for interactive event-based analysis [7]. Authors have simplified the structure available and have provided three phases, system preservation, a search of evidence, and reconstruction of events. Documentation is necessary for all processes. The emphasis of the model was on the reconstruction of events.

Ciardhuáin suggested a thirteen-stage digital investigation procedure [8]. Author presented a brief background of preceding frameworks and correlate it with the framework proposed. The author describes the phases as activities within the proposed framework.

In 2005, Beebe and Clark introduced a multi-tier framework since most frameworks available are of a single tier [9]. They suggested subtasks for the process of data analysis using the Survey, Extract and Analyze (SEE) method, and the objective-based task for analysis task is given.

A new concept in digital forensic investigation was offered by Ruibin et al. [10]. According to the authors, first, seek the case information, it is perceived as a clue to an investigation. Besides that, the authors explain a need for reuse of knowledge within the case and in different situations. Another notion stated in the study is the thought of case-relevance. The paper also explains the automated proof extraction module.

A digital forensic investigation process was proposed by Kent et al. which contains four phases, collection, examination, analysis, and reporting [11]. The media is turned into evidence within that context. For that purpose, when data is collected from media, and inserted into the format processed by forensic software, the data is then converted into information by analyses and the information becomes evidence.

The framework proposed by Kohn et al. was the convergence of current models and incorporating the phases and processes of previous frameworks [12]. The author offers three stages, preparation, investigation, and presentation to achieve the digital forensic investigation needs.

In 2006, a field triage model for the rapid response was proposed by Rogers et al. [13]. The Cyber Forensic Field Triage Process Model (CFFTPM) offers an on-site digital investigation approach. The principal advantage of the model is its pragmatism.

Another framework was proposed in 2007 by Freiling and Schwittay [14] for incident response and computer forensic. The framework incorporates two principles, incident response and computer forensic, to enhance the overall investigation. The system defined three stages, pre-analysis, analysis, and post-analysis.

A detailed review and methodology for digital forensic investigation were given by Selamat et al. [15]. By grouping and combining the related activities and processes into the appropriate phases, the author mapped the different frameworks. The phases identified by the authors are preparation, collection and preservation, examination and analysis, presentation and reporting, and disseminating the case.

Trček et al. developed the formal Digital Forensic Readiness (DFR) framework [16]. The DFR model is improved with the aid of service-oriented architectures (SOAs), sensor networks, and requirements for interoperability. Two new phases were incorporated into DFR, viz security services, and security mechanisms. Besides, the paper explains multilevel keyed message authentication codes (MACs) for the protection of evidence integrity. The framework provides digital forensic readiness measures to an organization.

A comprehensive analysis of the literature on the advancement of the digital forensic framework is provided by Agarwal et al. [17]. An author mapped the available models and suggested a structural model comprising 11 phases.

A thorough analysis of the digital forensic framework was presented by Ademu et al. [18] and suggests a model for the advancement in investigation procedure containing four phases, and four phases are further divided into several rules.

The Integrated Digital Forensic Process Model (IDFPM) was described by Michael Kohn [19]. The author compared the terms used in present frameworks and based on that, tried to standardize the model. Furthermore, the author gave a short review of the tools used for digital forensic investigation, that supports the framework. Finally, the author provides The Integrated Digital Forensic Process Model Prototype (IDFPMP).

A Comparative Digital Forensic Model (CDFM) was proposed by Dr Dhananjay and Nilakshi which comprises of 5 phases: foundation, accumulation and conversation, inspection and analysis, presentation and documentation, and justification and disseminating the case [20].

A taxonomy of digital forensic research is provided by Raghavan [21]. An author thoroughly studied and classified the present digital forensic investigation frameworks in four categories: acquisition and representation, discovery and examination, analysis, and process modeling.

The privacy-preserving enhanced digital forensic investigation framework (PPEDFI) was proposed by Anuradha Gupta [22]. The model was composed of three elements, expert system, evidence extraction, and ranking. In the model, files are rated through SVMRank according to case relevance.

In 2014, Quick et al. discussed the forensic analysis of large volume data through the digital forensic framework, focused on data reduction and data mining. Framework consists of ten steps [23]. suggested imaging the files specific to the case, instead of imaging whole storage media. Moreover, the author addressed open-source data and closed source data meaning data available on the internet and data from internal storage devices respectively.

Twenty-five digital forensic investigation frameworks have been examined and the strengths of all the aforementioned frameworks have been incorporated to introduce a new framework [24]. Jain and Kalbande have introduced a new system by integrating conventional framework with two additional modules, Case Registration, and History Keeper and Evidence Loader.

In a paper, Montasari suggested the on-site triage process model, the Structured Two-Stage Triage Process Model (FTSTPM) [25]. The first stage was known as the method of preparation and the second stage was the on-site triage evaluation process.

In the article, Ahmadi et al. have presented a methodology for rapid investigation by imaging some of the common windows forensic artifacts only instead of imaging the whole hard disk [26]. It will reduce the time and storage space.

Verma et al. attempted to respond to the data privacy challenge during the investigation process and using a machine learning technique, proposed the automated system for a digital forensic investigation called DF 2.0 [27]. The forensic exhibit (device or image) is taken as an input in the framework, subsequently it is used for forensic pre-processing where the current case information is added and the duplicate files and files mentioned in NSRL are removed. In addition, the data collected during the second step is used as input for automated digital forensic processing, where the investigation process is performed and the files are bifurcated using the machine learning technique to provide privacy.

In the study, Dimpe and Cogeda identified the basic criteria for successful digital forensic investigation [28]. The authors suggest a new method comprises of eleven steps. The author mentioned that after each stage, documentation is needed. Also, the author illuminates the skills needed for digital forensics. In addition, they identified the legal context, in which the admissibility of evidence and laws on cybercrime were discussed. Finally, they offer a detailed guide for the handling of evidence, in which they address the chain of custody, management of evidence, and the rules of evidence.

ISO 27037: 2012 provides generic guidelines for handling digital evidence. Sudyana et al. [29] mapped the existing framework to ISO 27037: 2012 and concluded that the Integrated Digital Forensic Process model (IDFPM) framework proposed by Kohn [19] nearly accomplished with ISO 27037: 2012. The author modifies IDFPM and presents a comprehensive framework that is divided into the following five groups: preparation, incident, incident response, digital forensic investigation, and presentation.

In the research Shayau et al. [30] have described a framework that identifies the modified system files and detects files inserted into system directories. It also verifies its integrity by hashing. The whole idea behind the framework is to capture the fresh OS files and kept it in a database as a standard and compare it with the suspect system to narrow down for investigation and focus on the files that are modified. Constrain with that framework is that the same OS version and build is required to use as a standard and is not possible for each time.

Big data is the key problem of a present digital forensic investigator. Song and Li [31] defined big data as 3Vs, Volume, Variety, and Velocity. In the paper, a framework for the investigation of big data was presented wherein the author identifies three phases, Digital Forensic Technology,

Intermediate Technology and Big Data Technology. Hadoop framework was considered for big data technology.

3. Proposed Framework

The preceding section outlined the several significant digital forensic investigation frameworks presented to date. It is observed from that, there is a few lacuna in all the frameworks available to date or are constrained to some circumstances. The core purpose of the framework is to provide a generic reasonably complete framework that can be implemented in all circumstances and all sorts of devices. The author named it as next generation digital forensic investigation model. (NGDFIM). The proposed framework is separated into 3 phases that are, on-site triage phase, analysis phase, and the presentation phase. Figure 3. Next Generation Digital Forensic Investigation Model Flow Chart elaborates the proposed framework.

3.1. On-site triage phase

The initial and most critical phase of the investigation is the on-site triage phase. It comprises several processes to be followed by the first responder to meet the requirements of digital forensic standards. The very first process is to secure the crime scene to avoid any individual interference. After that, the evidence to be gathered is identified. There are two possibilities for collecting evidence, either the electronic device is running or not. If the device is on, begin with distinguishing whether or not the live acquisition is possible. An investigator will then need to identify the operating system and version running in the device. The reason is that, if an unsupported driver is loaded into the kernel, it may result in BSOD, which wipes out the data from physical memory. An investigator should then capture the physical memory by means of an appropriate memory acquisition tool on a sterile external drive. The hash value is captured to prove the integrity of the image file. If the device is portable, then collect the device and if the device is not portable, remove the hard-disk and collect it in a forensically sound manner along with other storage devices and follow the chain of custody process.

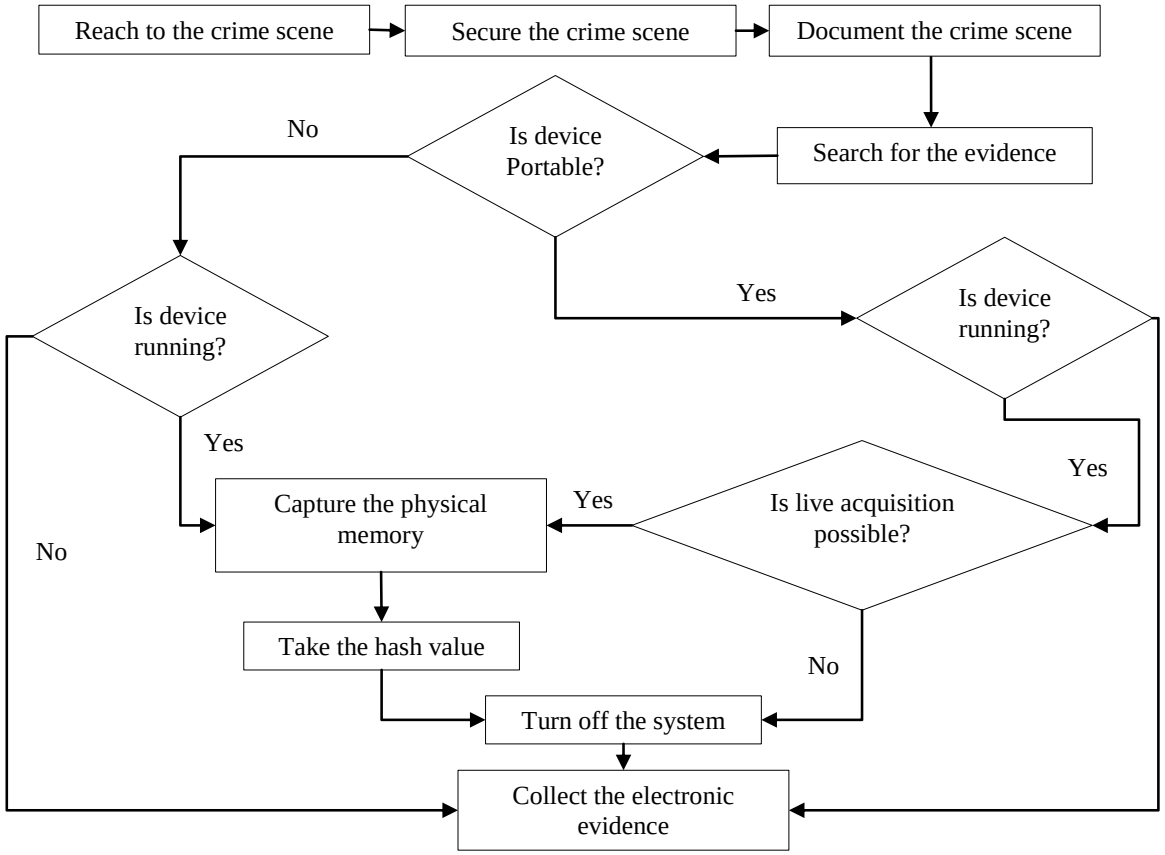

Figure 1. Flowchart for On-site Triage Phase

3.2. Analysis phase

In the analysis phase, the foremost step is to image the evidence item to preserve original evidence, and the image file can further analyze. A memory image file is attached to the memory analysis tools if the live system was found at the scene of crime. The image file is loaded into the memory analysis tool. For the rapid investigation, a new technique is implemented for memory analysis. Wherein, an image of a respective fresh operating system is acquired and used as a baseline to compare and identify the non-native processes of the suspect machine. It would be much beneficial for cases like malware attacks to identify the rouge process.

Recently, big data analysis is the major concern for digital forensic investigation. It will take a gigantic sum of size and an awfully long time to image and store the entire device. That's the reason, we proposed to image the case significant files as it were rather than conventional imaging process, to overcome the capacity issue and it will moreover give the protection of the suspect's privacy. To maintain the integrity of the evidence, the hash values of the files were taken before and after the imaging process. However, the whole device can be imaged a while later, in case required. Then, the image file is analyzed in the forensic analysis tools.

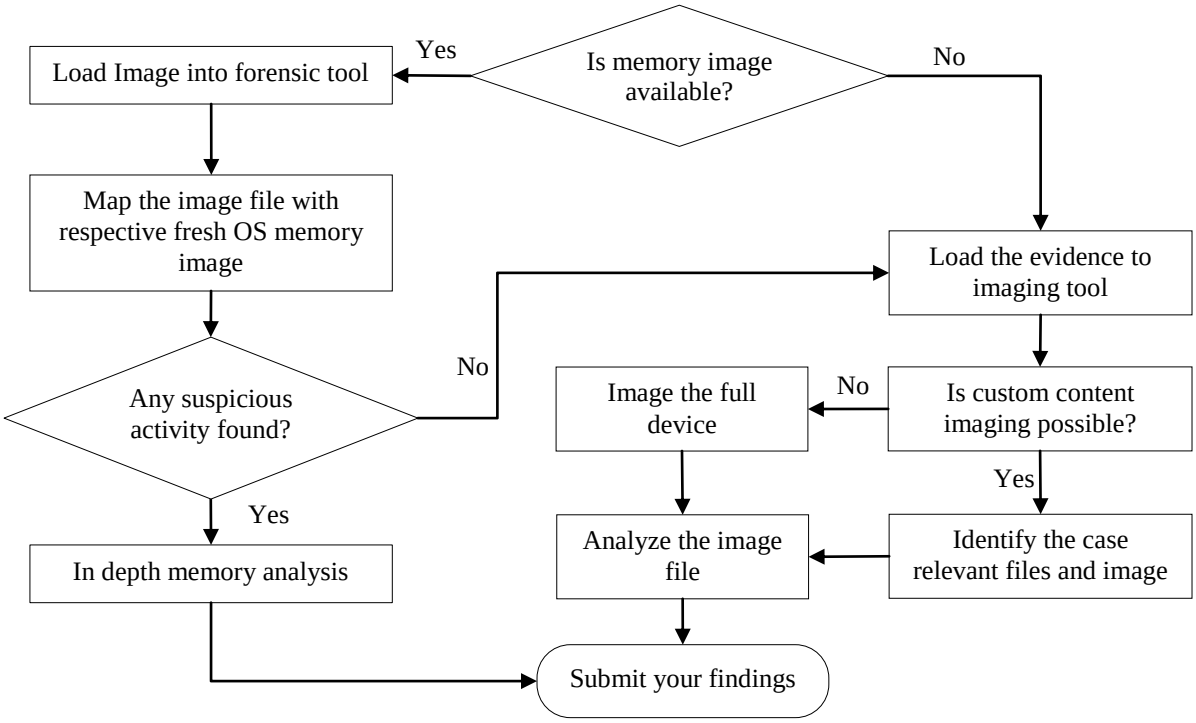

Figure 2. Flow Chart for Analysis Phase

3.3. Presentation phase

The investigation should prove the hypothesis that was reached during the investigation in the final phase of the framework. The major part of the forensic investigation is to report the findings. After the analysis phase, a wide-ranging report of the findings is submitted to the respective officials. For the report part, we proposed that instead of reporting every file, case-relevant files are only included in the report of the automated tool report generator. Moreover, elucidation of the report ought to be composed in a layman dialect so that non-technical individuals can too understand.

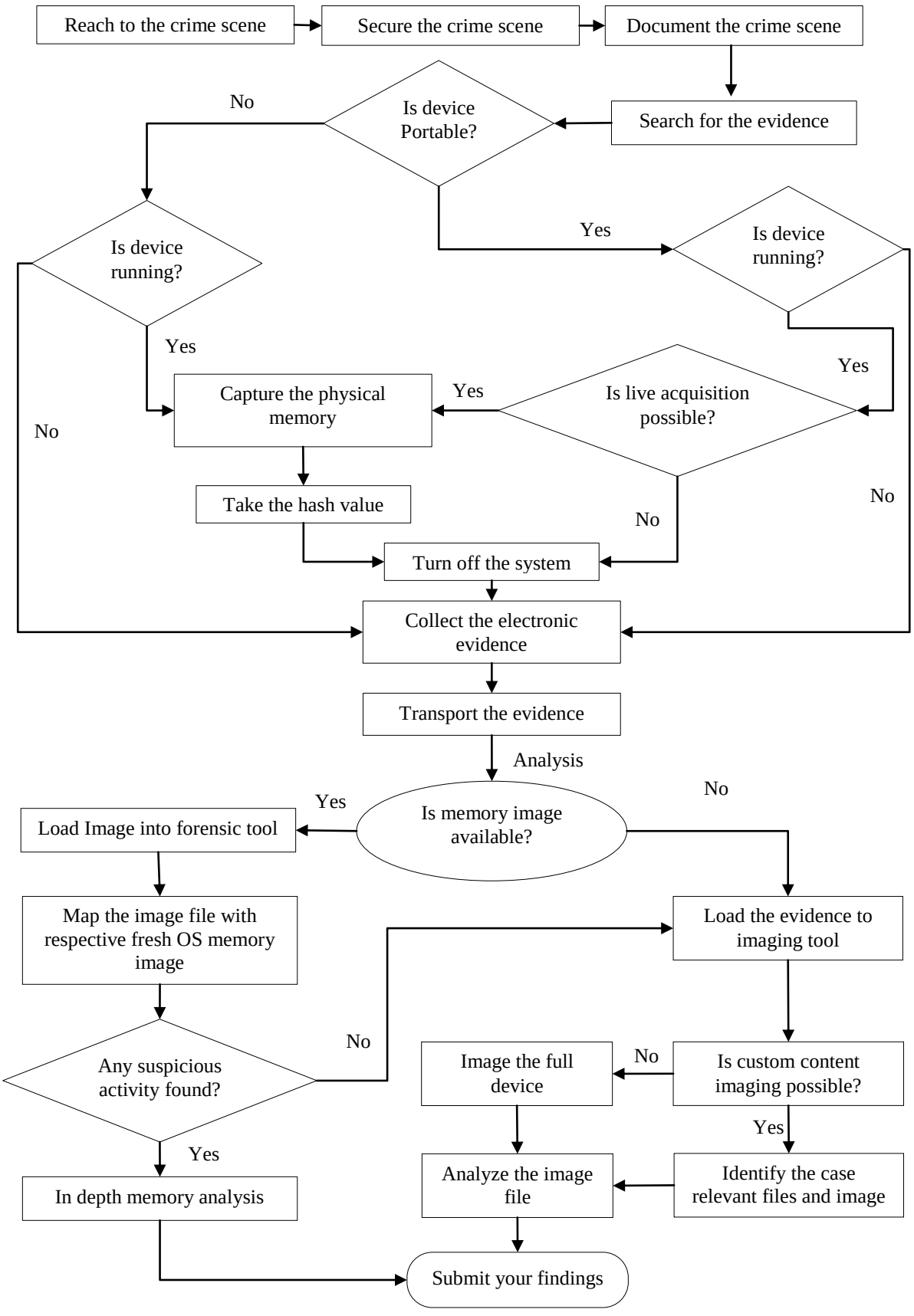

Figure 3. Next Generation Digital Forensic Investigation Model Flow Chart

4. Conclusion

This paper presents a high-level overview of the digital forensic investigation framework available so far. Based on these, and taking into account technological advances, big data analysis challenges, and privacy protection, an enhanced technological architectural framework, NGDFIM is presented to overcome these challenges. This paper provides a comprehensive framework for the application in most incidents without compromising the integrity of evidence. The modification aims to reduce the time of analysis by custom content imaging, enhance the efficiency of the overall investigation process through on-site triage process and memory image mapping, and protect the suspect's privacy during the digital investigation procedure. One of the biggest advantages of the framework is its pragmatic application. In real-life cases, a prototype may be created in the future to implement the framework.

References

[1] Pollitt M 1995 Computer Forensics: an Approach to Evidence in Cyberspace *Proceeding Natl. Inf. Syst. Secur. Conf.* 487–491
[2] Palmer G 2001 A Road Map for Digital Forensic Research *Digital Forensic Research Conference DFRWS USA*
[3] Reith M, Carr C and Gunsch G 2002 An Examination of Digital Forensic Models *Int. J. Digit. Evid.* **1** 3
[4] Carrier B and Spafford E H 2003 Getting Physical with the Digital Investigation Process *Int. J. Digit. Evid. Fall* **2** 2
[5] Stephenson P 2003 A comprehensive approach to digital incident investigation *Inf. Secur. Tech. Rep.* **8** 2 42–54
[6] Baryamureeba V and Tushabe F 2004 The enhanced digital investigation process model *Proceedings of the Digital Forensic Research Conference, DFRWS USA* 1–9.
[7] Carrier B D and Spafford E H 2004 An event-based digital forensic investigation framework *Digital forensic research workshop* 1–12
[8] Ciardhuáin S O 2004 An Extended Model of Cybercrime Investigations *Int. J. Digit. Evid.* **3** 1 1–22
[9] Beebe N L and Clark J G 2005 A hierarchical, objectives-based framework for the digital investigations process *Digit. Investig.* **2** 2 147–167
[10] Ruibin G, Yun C K and Gaertner M 2005 Case-Relevance Information Investigation : Binding Computer Intelligence to the Current Computer Forensic Framework *Int. J. Digit. Evid.* **4** 1 1–13
[11] Kent K, Chevalier S, Grance T and Dang H 2006 Guide to Integrating Forensic Techniques into Incident Response *Natl. Inst. Stand. Technol.* 800-86
[12] Kohn M, Eloff J H P and Olivier M S 2006 Framework for a Digital Forensic Investigation *Conf. Proc. ISSA from Insight to Foresight Conf.*
[13] Rogers M, Goldman J, Mislan R, Wedge T and Debrota S 2006 Computer Forensics Field Triage Process Model *J. Digit. Forensics, Secur. Law* **1** 2 19–38
[14] Freiling F and Schwittay B 2007 A Common Process Model for Incident Response and Computer Forensics *IT-Incidents Management & IT-Forensics – IMF* **114** 19–40.
[15] Selamat S R, Yusof R and Sahib S 2008 Mapping process of digital forensic investigation framework *Int. J. Comput. Sci. Netw. Secur.* **8** 10 163–169
[16] Trček D, Abie H, Skomedal Å and Starc I 2010 Advanced framework for digital forensic technologies and procedures *J. Forensic Sci.* **55** 6 1471–80
[17] Agarwal A, Gupta M, Gupta S and Gupta S C 2011 Systematic Digital Forensic Investigation Model *Int. J. Comput. Sci. Secur.* **5** 1 118–131
[18] Ademu I O, Imafidon D C O and Preston D D S 2011 A New Approach of Digital Forensic Model for Digital Forensic Investigation *Int. J. Adv. Comput. Sci. Appl.* **2** 12 175–178
[19] Kohn M D 2012 Integrated Digital Forensic Process Model *University of Pretoria*
[20] Kalbande D D and Jain N 2013 Comparative Digital Forensic Model *Int. J. Innov. Res. Sci. Eng. Technol.* **2** 8 3414–19
[21] Raghavan S 2013 Digital forensic research: current state of the art *CSI Trans. ICT* **1** 1 91–114

[22] Gupta A 2013 Privacy preserving efficient digital forensic investigation framework *6th Int. Conf. Contemp. Comput. IC3* 387–392
[23] Quick D and Choo K K R 2014 Data reduction and data mining framework for digital forensic evidence: Storage, intelligence, review and archive *Australia's national research and knowledge centre on crime and justice* **480**
[24] Jain N and Kalbande D R 2015 Digital forensic framework using feedback and case history keeper Proceedings *Int. Conf. on Communication, Information and Computing Technology, ICCICT*
[25] Montasari R 2016 A Formal Two Stage Triage Process Model (FTSTPM) for Digital Forensic Practice *Int. J. Comput. Sci. Secur.* **10** 2 69–87
[26] Ahmadi H R, Mourad A, Tawil R and Awada M B 2018 A New Approach in Digital Forensics Investigation Process *Int. Conf. Comput. Appl. ICCA* 270–275
[27] Verma R, Govindaraj J and Gupta G 2018 DF 2.0: Designing an automated, privacy preserving, and effifficient digital forensic framework *Annual ADFSL Conference on Digital Forensics, Security and Law* 127–150
[28] Dimpe P M and Kogeda O P 2018 Generic Digital Forensic Requirements *Open Innovations Conference, OI* 240–245
[29] Sudyana D, Prayudi Y and Sugiantoro B 2012 Analysis and Evaluation Digital Forensic Investigation Framework Using Iso 27037:2012 *Int. J. Cyber-Security Digit. Forensics* **8** 1 1-14
[30] Shayau Y H, Asmawi A, Rum S N M and Ariffin N A M 2019 Digital Forensics Investigation Reduction Model (DIFReM) Framework for Windows 10 OS *IEEE 9th Int. Conf. Syst. Eng. Technol.* 459–464
[31] Song J and Li J 2020 A Framework for Digital Forensic Investigation of Big Data *3rd International Conference on Artificial Intelligence and Big Data, ICAIBD* 96–100