*2019 4th International Conference on Information Systems and Computer Networks (ISCON)*
*GLA University, Mathura, UP, India. Nov 21-22, 2019*

# Cyber Forensics and Comparative Analysis of Digital Forensic Investigation Frameworks

Kumar Shanu Singh
*Department of Computer Sci & Eng.*
Centre for Advanced Studies,
Lucknow, India
17mcs06@cas.res.in

Annie Irfan
*Department of Computer Sci & Eng.*
Institute of Engineering & Technology,
Lucknow, India
annieirfan.cs@gmail.com

Neelam Dayal
*Department of Computer Sci & Eng.*
Centre for Advanced Studies,
Lucknow, India
neelamdayal@cas.res.in

***Abstract*— With industrial revolution 4.0, automation foster communications between digital devices around the globe which involves several digital devices including cyber physical system devices, IoT devices, mobile devices, storage devices and network devices or even PCs as digital evidence; increasing the number of cybercrime rate. This brings us to question a necessity for advanced Digital Forensics Investigation Framework (DFIF) for the effective prosecution of digital crime in court of law; such that the framework should preserve integrity of evidence throughout steps while in process. Our paper is descriptive in nature that surveys recent trends of cybercrime attacks and explored associated Cyber Forensics. In addition, we have mapped process and output produced by different phase in the DFIF that have been examined from previously proposed frameworks and represented a comparative mapping of all frameworks. The mapping process results in optimized investigation process.**

***Keywords*— *Cyber crime attack; Digital forensic investigation framework (DFIF); Incident Response; Analysis; Investigation.***

## I. INTRODUCTION

With advent of industrial revolution 4.0 (I4.0), the era had marked upon the birth of various startups as well as giant companies in various sectors for automation. With prevailing traditional systems, I4.0 leads to computerization and inclusion of new technologies as cyber physical system, IoT, cloud computing and cognitive computing. Thus, the range of cyber-attacks and crime is exponentially increasing in number thereby producing a variety of digital marks and evidences. These evidence thus, need to be preserve for integrity to be prosecuted in court of law. Ever since the beginning of understanding, need for building DFIF was introduced which expanded the domain of digital forensic to a number of various fields like IoT forensics, Cloud Forensics, Network Forensics and Storage device forensics nevertheless the general concept of preserving evidence in Chain of Custody (CoC) has not changed significantly. The origin of forensics is due to cybercriminal incidents reported, i.e. an illegitimate and inapt behavior of any individual or group with an intention. The role of forensics can be cataloged into different areas which facilitate analysis of criminal activities exploiting forensic methodologies and investigation framework, elaborated in further sections.

In essence, a DFIF phases include collecting, preserving, analyzing and providing scientific supported evidence for the criminal or civilian courts of law prosecution in appropriately documentation. In digital forensic investigation practices, there are bundle of digital forensic investigation frameworks developed by organizations / researchers with its own processes and focuses on some technical aspects/ phases. To date, technology investigated and available tools have guided the digital phases. As a result, when the underlying technology of the target device varies, new processes have to be developed. This brings us to the need comprehensive analysis of DFIF, as mapped in our paper.

Further, in Section 2, we discuss the predominant cyber-attacks in I4.0, complying standard OWSAP vulnerability and related forensic techniques. Section 3 gives a review of related works in the development of various DFIF. Paper proposes a mapping activity that can simplify the overall process of previous research within the Digital Forensic Testing Framework in Section 4. Section 5 gives a comparative result analysis of our study to show the balance of the investigation process for preparation of appropriate solid evidence that is to be presented in the court of law. Conclusion and future work is in Section 6.

## II. CYBER FORENSICS AND DIGITAL EVIDENCE: RECENT DEVELOPMENT

Digital evidences are the central component that needs to be examined for any criminal activities. It comprises both the traditional or physical evidence and cyber digital evidence. However, here we are scrutinizing the case of digital evidences. The current cybercrimes in I4.0 has possibly made large scope for various category of forensics. According to a survey report of EY Global Information Security Survey 2018-19 [1] which presented the top 10 biggest cyber threats to an organization worldwide contains are Phishing and Malware as top threats. Attacks like DDoS Attacks for disrupting services of an organization are ranked third, followed by Financial Frauds. Although there are more threats mentioned in the report, Internal Threats are also one of the rising concern. The attack percentage occurring is depicted in Figure 1.

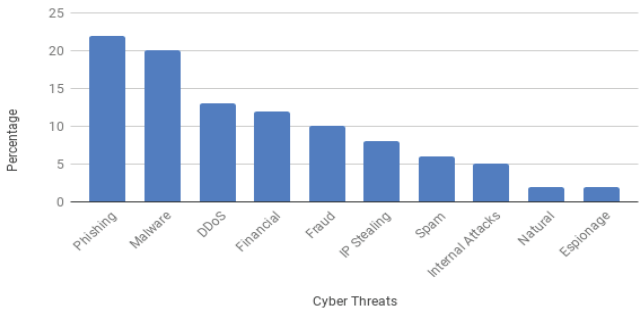


Fig. 1. Cyber Crime Reported data by EY Global in 2018-19

To understand the **5W** i.e. 'who, what, when, where and why' of a cyber-incident, the evidence collected from the crime origination is wisely observed. This whole process of validating the findings with the details/ information obtained from evidence is known as cyber forensics. Table 1 given elaborates major forms of cyber forensics. The new emerging fields of forensics is the consequences of the new technological development for measuring web app security risk. This can be additional understood in reference to the list in OWASP 2017[2].

However, the different forms of digital evidence are still needed to be prosecuted within the same laws of court to prove the guilty, with change in the technique for analysis of evidence. Further, in Section 3, we have reviewed various DFIF from 2003 to present, for understanding and to bring a structured and comprehended Forensic framework as area for further research.

## III. Review of Digital Forensic Investigation Frameworks

This section studies the significantly popular related work on DFIFs. These DFIFs had been divided into several phases as described in Table 2. Our work starts a comprehensive analysis from the earliest and prominent work of *Carrier et al.* [3] in 2003, which recommended a model for dealing with examining potential evidence. The emphasis was to combine both law and forensic science and to document the process involve in the investigation into standard acceptable form. Five different phases were introduced in this method, which can be acknowledged for admission of any evidence in the court.

In 2004, the *Digital Forensic Research Working Group* [4] recommended a standard investigation process, which stands applicable to all or most of the investigations involving digital systems as well as for networks. In this framework, processes are defined in a way to handle both physical and digital evidence. This framework marks the foundation for more of work published.

However, *Career et al* in 2004, based on the earlier work, proposed framework named "Event-Based Digital Forensic Testing Framework" that includes five steps. It provides a model that can be applied to classify events and also provides many benefits as a mechanism listed by the authors in the form of a mechanism to implement the same framework for future digital technologies. However, this framework in real life the model was challenged by forensic experts like *Kohn* [5] and *Hevner* [6]. In this model, the author did not separate primary crime scene (from which the digital crime commenced) and secondary crime scene (victim's location), hence it affects rebuilding of events or incomplete findings.

*Ciardhuáin et al.* [7] proposed a clear investigating framework till the matter is not reported, steps will be taken from the beginning of the investigation process with the preparation of the investigation and throughout the process. This framework offers development of techniques and tools to support investigators and such structure can be considered as a comprehensive package.

*Kohn et al.* [5] proposed compiled framework based the works in [4][8][9][7][10][11]. Their research work has emphasized on two important points. Firstly, acquaintance of relevant lawful foundation is most important step before making the framework from right at the beginning of the investigation is established to investigation termination. Secondly, any framework must include at least three phases so as to meet the minimum requirements of forensic investigation. Therefore, Kohn has organized the stages in three stages and proposed their structure. The benefits of this proposed structure can undoubtedly augmented to include number of additional steps, if required.

Computer Forensic Field Triage Process Model (CFFTPM) [12] recommends an onsite or field approach to provide system/media for deep examination, without the need to get a full forensic image or to return to the laboratory for identification, analysis, and interpretation of digital evidence. This structure, developed by the IDIP Framework [13] and Digital Crime Scene Environmental Analysis (DCSA) framework [14]. This framework gives a formal approach of real-world investigative approaches and their applicability and that adds an advantage of CFFTPM in contrast to other DFIFs.

*Freiling et al.* [15] proposed a forensics that outlines computer security incidents as a combination with data of accident response and computer forensics so as to improve the overall process of investigation into 4 phases concentrating on majorly on analysis. The Analysis phase include pre, actual and post analysis phase refers to all the steps and activities that are formerly executed to the real analysis starts, examination of evidence to finally documenting of the entire activities during the investigation consecutively. This framework provides a method for conducting the proper phenomenon and also integrates a forensic analysis into an incident response framework.

In 2007, *Bem et al.* [16] proposed a new structure that involves analyzing a case in two environments, the first is the virtual environment and the second is the traditional environment comprises of four phases. The proposed work focuses primarily on the analysis phase of a digital case in a virtual environment. They have listed different boundaries of virtual environments. Although virtual environments can be a replacement for the traditional environment, the virtual environment helps in the better use of less qualified personnel.

In 2009, Perumal et al.[17] proposed another digital forensic investigation model which is based on Malaysian investigative procedures. There are 7 steps in the proposed model. The framework include an additional feature for the evidence in running (in operation) which is similar to the performance of live forensics. The author argued that the presence of live data acquisition, which is centered on delicate proofs. Data will be analyzed and tested using the appropriate tools and techniques. In the previous models, similar to the presentation phase, here this is named as Proof and Defense phase. Finally, the archive storage phase is performed, related evidence is properly stored for future references, and may also be used for training purposes.

Pili et al.'s in [18] propose of a new framework based on the network forensics The structure is organized in nine phases where the frame network provides a foundation for the development of techniques and tools. Therefore, this structure is probably considered to be the most suitable for network forensics.

Roger et al. [19], proponents a multi-perspective cybercrime investigation process modeling framework that is

based on the generalization of the settings that were previously proposed. The proposed structure is made up of three phases which have been further classified in twenty steps. The framework is mainly focused on examining and approach for various tasks, which are to be done under each process to achieve the respective test targets. Saleem et al.[20] proposed a model which is an expansion of Reath's abstraction model. The model has seven steps and talks about maintaining the integrity of digital evidence and preserving human rights from overlapping umbrella principles.

A new structure was proposed by *Bashir et al.*[21] 2015 which is known as the Triage Framework for Digital Forensics. This framework is based on the live analysis of the system. This paper represents a forensic examination method, in which machines have suffered many steps from identifying the machines' to making reports. The paper forensics determines the comprehensive steps involved in its triage. They describe step-by-step procedures for forensic analysis on compounding machines and for storing all these activities in the database for later use. In the proposed framework, triage is performed done after the date acquisition and before the detailed analysis phase.

Al-Khateeb et al.[22] proposed a new forensic model, in which the chain of custody is based on distributed distribution. They provided a scenario related to eHealth to show the value of this approach to introduce forensic readiness in computer systems and enable better police intervention.

A Blockchain-based framework was proposed by Lone et al. [23] in 2019, the modern digital forensics is known as Blockchain: Chain-of-Custody as a distributed ledger. In the proposed framework, the author implemented Blockchain in a chain of custody to tackle challenges faced while maintaining the integrity and authenticity of digital evidence for its acceptance in the court of law. The authors brought integrity and tamper resistance to the custody of the Digital Forensic Chain. The author also gave proof of concept in Hyper ledger Composer and evaluated its performance.

TABLE I. CATEGORY OF FORENSICS AND TYPE OF EVIDENCE COLLECTED

| Forensics | Description | Type of potential evidences | Cyber attack Vulnerability exploited |
|---|---|---|---|
| Computer Forensics | Originally known as digital forensics, includes laptops, computers | Evidence from computers systems and any primary memory and secondary memory (like USB pen drives), Documents, Email (Non-web-based), Files stored locally or on a media card, Internet Search History, Social Media accounts, Everything from All Categories | Malware, Email Phishing, DDoS, Internet bomb threat, cyber bullying and harassment, Enterprise hacking, Financial frauds. Spoofing, password attack, Potentially unwanted programs PUPs. |
| Mobile device forensics | Additionally contains an inbuilt communication system such as GSM, GPS. | Are not limited to short message services or emails; it also includes data regarding the location of the user, call log, user dictionary content, data from installed applications, media (audio, video, images, other files), system files, usage logs, and any other deleted data. Social Media accounts, Game consoles. | Spoofing, , password attack, Cyber Staking, Identity theft |
| Network forensics | Investigating network traffic and network packets over different networks. | Covers intrusion detection and firewalls. Being volatile and not easy to log network data as the attacker may be passive or active. | Spoofing, , password attack, Broken Access Control |
| Database Forensics | Study of databases and its metadata | Analyses of database content, log files, and in-RAM data | SQL Injection attack , Broken Access Control , Cross Site Scripting , Insecure Deserialization |
| IoT forensics | Study of IoT devices as embedded systems and devices that communicate | Analyse the IoT devices as embedded system, wearables, independent products that interact like toys and home-kitchen appliances, etc.; CCTV camera, drones, CPS. | Spoofing, password attack, Botnets, Enterprise hacking, |
| Software/ Web application forensics | Study of code of softwares | Analysis to check whether code had been copied or tampered or malware injection | Broken Authentication, Security Misconfigurations |
| Fraudent Data Analysis | Study of devices that are especially designed to gain financial gains. | Analysis of phishing websites or fake URL that makes illegitimate transactions, ATM cloning, UPI frauds, may include linkage to SNS accounts. | Financial frauds, Sensitive Data Exposure. |

After a comprehensive analysis of the DFIFs, three major finding that we established are process redundancy, area focus, and framework features. For instance, [11] and [24] their structure consists of duplication process or activities. [8] and [12] were focusing on creating a method for quick forensic analyses, while [19], [16] and [21] are focusing on the analysis process so that the evidence can be obtained and increase the whole process for investigation. [14] and [20] frameworks have characteristics of specificity, and pragmatism. [22] and [23] have implemented Blockchain to ensure integrity in chain of custody. All these settings have their own strength; however, as of today, no single framework can be used as a general guideline for examining the cases of all incidents. Therefore, to overcome this issue, a general framework is required and research is needed.

TABLE II. A COMPARATIVE ANALYSIS ON PHASES OF DFIFS

| No | DFIF | Author | Year | No of Phases | Phases in DFIF |
|---|---|---|---|---|---|
| 1 | Integrated Digital Investigation Process (IDIP) | Carrier et al. | 2003 | 5 | Readiness, Deployment, Physical Crime Scene Investigation and Digital Crime Scene Investigation; and Review |
| 2 | The Enhanced Digital Investigation Process Model | Baryamureeba et al. | 2004 | 5 | Readiness, Deployment, Traceback, Dynamite and Review |
| 3 | An Event-Based Digital Forensic Investigation Framework | Carrier et al., | 2004 | 4 | Readiness, Deployment, Physical and Digital crime scene investigation and Presentation |
| 4 | Extended Model of Cybercrime Investigation | Ciardhuáin et al. | 2004 | 13 | Awareness, Authorization, Planning, Notification, Search, Identification, Collection, Transport, Storage, Examination, Hypothesis, Presentation and Dissemination. |
| 5 | Framework for a Digital Forensic Investigation | Kohn et al. | 2006 | 3 | Preparation, Investigation and Presentation. |
| 6 | Computer Forensics Field Triage Model (CFFTPM) | Rogers et al. | 2006 | 6 | Planning, Triage, User profile, Chronology/timeline, Internet activity, and Case. |
| 7 | Common Process Model for Incident and Computer Forensics | Freiling et al. | 2007 | 4 | Pre-incident preparations, Pre-analysis, Analysis and Post analysis. |
| 8 | Computer Forensic Analysis in a Virtual Environment | Bem et al. | 2007 | 4 | Access, Acquire, Analyze and Report |
| 9 | Digital Forensic Model based on Malaysian Investigation Process (DFMMIP) | Perumal et al. | 2009 | 7 | Plan, Identification. Reconnaissance, Investigation, Transportation and storage, Analysis and tested, Proof of Defense and archive storage. |
| 10 | Network forensic frameworks: Survey and research challenges | Pilli et al. | 2010 | 9 | Preparation, Incident reaction, Detection, Collection, Protection, Examination, Analysis, Investigation, and Presentation. |
| 11 | Multi-Perspective Cybercrime Investigation Process Modeling | Roger et al., | 2012 | 3 phases comprising 20 steps | Multi-perspective Cybercrime Investigation Process Modeling, Active investigation and Reactive investigation |
| 12 | Extended abstract digital forensics model with preservation and protection as umbrella principles | Saleem et al. | 2014 | 7 | Preparation and Planning, Collection, Examination, Analysis, Reporting, Presentation, Archiving and Returning |
| 13 | A triage framework for digital forensics | Bashir et al., 2015 | 2015 | 5 | Identification, Data preservation, Extraction, Triage and Evidentiary Report |
| 14 | Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger | Al-Khateeb et al., 2019 | 2019 | 6 | Identification, Preservation, Collection, Examination, Analysis and Presentation |
| 15 | Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer | Lone et al.2019 | 2019 | 6 | Identification, Search & Seizure, Preservation, Examination, Analysis and Reporting |

## IV. MAPPING SCHEME FOR DFIF

With the popular structure outlined in Section 3, it can be contemplated that each frameworks is evolved on the preceding experiences and many of them focus on different areas of investigation. However, the computational output of all frameworks is the same, regardless of sequence of processes and activity used are slightly different.

In this section, we introduce a mapping scheme for the Digital Forensic Investigation Framework (DFIF) to the group and merges all activities/processes that generate the same output. The mapping scheme is intended in order to balance the process of obtaining prevailing direction that can make strong evidence for presentation. The steps implemented to design the DFIF charting scheme are as follows:

*Step 1*. Identify existing structures

*Step 2*. Formation of phase name

*Step 3*. Mapping the Process

In this phase, we have analyzed the previous structure

*a) Identify existing structures*

In this phase, we have analyzed the previous structure by identifying the activities/processes and output. The result of this identification is summarized into five categories on the basis of activities/processes related to awareness and increasing potential of the forensic organization, evidence collection, analysis of evidence, presenting of result and termination of the case as shown in Table 3.

*b) Formation of phase*

After the first step based on the activities/processes and output, phases have been categories as Readiness, Reconnaissance/Footprinting, Investigation, Presentation, and Presentation as shown in Table 3. Output of the phases are also depicted in same table.

1. *Readiness:* In this phase, we determined all the activities/processes which deal with maximizing the potential of an organization by reducing the cost of the investigation.
2. *Reconnaissance/Footprinting:* All the phases which deal with collection & preservation of evidence or deals with the collection of evidential data using several techniques and mechanisms are included in this single phase.
3. *Investigation:* This phase includes activities/processes that deal with analysis and examination of digital evidence using various forensic techniques to relate to crime.
4. *Presentation:* This phase involves all those activities/ processes, which include dissemination of findings of the investigation, so on the basis which decision can make.
5. *Incidence Closure*: It includes phases which involve the termination of cases and sharing of outputs of an investigation to other forensic organizations for future reference.

TABLE III. PHASES OF OPTIMIZED DFIF WITH ACTIVITIES AND OUTPUT

| Phase | Phase Name | Process/Activities | Output |
|---|---|---|---|
| 1 | Readiness | • To obtain authorization to initiate an investigation.<br>• Keeping infrastructure and resources updated to deal with any investigation.<br>• Identifying and verifying a crime scene.<br>• Spreading awareness "Why investigation is important?"<br>• Discovering stratagems to get information from both inside and outside the organization.<br>• Identifying previous investigations for support.<br>• Notifying subject and other concern parties that an investigation is taking place. | Update, Planning, Authorization, Identification, Warrant, Notification, Search and Seizure, Confirmation |
| 2 | Reconnaissance/ Footprinting | • Determining potential digital evidence and potential sources.<br>• Determining the physical location of evidence.<br>• Transforming evidence into data.<br>• Securing the authenticity and integrity of digital evidence.<br>• Preserving and storing of digital evidence in a secure environment.<br>• Isolating the digital evidence from getting temper.<br>• Create copies of digital evidence using standard procedures. | Crime class, Potential Evidence, Potential Sources, Transportation, Integrity, Authenticity, Storage, Devices, Event |
| 3 | Investigation | • Determining the cause and by whom & when.<br>• Determine and validating procedures and techniques for analysis.<br>• Discover hidden data, recover deleted data, and extract encrypted data.<br>• Recognize the hidden pattern and determine the skill level of a suspect.<br>• Validating or refuting accusations of a suspect<br>• Identify potential evidence in the unconventional location.<br>• Document findings & results and draw conclusions on the basis of it.<br>• Examine and validate the earlier proposed hypothesis.<br>• Propose and validate a new hypothesis based on findings.<br>• Construct timeline analysis report. | Deleted/hidden/encrypted File, Events log, Timeline Report, Information, Log Files, Location, Cause, Hypothesis |
| 4 | Presentation | • Present findings and results to subject and concern bodies.<br>• Determine the relevance and reliability of evidence and testimony for same.<br>• Judicious interpretation from the analysis phase<br>• Provide an explanation and justification of the conclusion.<br>• Present both physical and digital evidence before the judiciary.<br>• Try to confirm the pattern of the incident in each piece and chain of evidence.<br>• Validate the new hypothesis and defend it against critiques.<br>• Dissemination of relevant findings and results to other concern audiences. | Presentation, Evidence, Decision, Report, Conclusion, Prosecution, Testimony |
| 5 | Incident Closure | • Ensuring physical and digital property to the appropriate owner.<br>• Determine what and how criminal evidence needs to be terminated.<br>• Identifying the area of improvement by examining the investigation.<br>• Circulate the knowledge gained from the investigation.<br>• Termination of investigation and preserving knowledge. | Dissemination of Knowledge Gained, Upgraded Policies and Investigation Procedures, Evidence Return/Disposal, Investigation Termination |

*c) Mapping the Process*

This step comprises analysis of previous activities/processes and output are identified and mapped in the name of the new defined phase. Using a table we have summarized all the activities/processes and output of selected DFIF into defined five phases. The overview of the result generation is shown in Table 4.

TABLE IV. MAPPING PROCESS IN DFIF

| **Phase / Output** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|
| ***Baryamureeba et al., 2004*** | | | | | |
| Readiness | ✓ | | | | |
| Deployment | ✓ | | | | |
| Traceback | | ✓ | | | |
| Dynamite | | | ✓ | ✓ | |
| Review | | | | | ✓ |
| ***Perumal et al., 2009*** | | | | | |
| Planning | ✓ | | | | |
| Identification | | | | | |
| Reconnaissance | | ✓ | | | |
| Transport & Storage | | | | | |
| Analysis | | | ✓ | | |
| Proof & Defence | | | | ✓ | |
| Archive Storage | | | | | |

## V. RESULT ANALYSIS

As per the mapping scheme defined in Section 3, simplification of the activities/processes and the output of all the selected frameworks is done into five phases and is shown in Table 5.

From the analysis shown in Table IV, it is concluded frameworks mostly consists of some crucial phases which include Phase 2 – Reconnaissance/Footprinting, Phase 3 - Examination, and Phase 4 - Presentation excluding Phase 1 and Phase 5. Although Phase 1 and Phase 5 are not included in some frameworks, the learning in [5], [15], [24], [25], [19], and [22] shows that both phases are important in order to complete investigation. Phase 1 is to secure that the investigation process has begun and it should be executed following standard procedures and the chain of custody is protected. While excluding Phase 5, there will be a circumstance of inadequate investigation and no advancement in investigation procedures or policies. Therefore, a standard framework should include all proposed phases which are the readiness phase, reconnaissance/ footprinting, investigation phase, presentation, and incident closure.

TABLE V. MAPPING PROPOSED AND OPTIMIZED DFIF

| **Digital Forensic Investigation Framework/ Model** | **Phase** | **Phase 1** | **Phase 2** | **Phase 3** | **Phase 4** | **Phase 5** |
|---|---|---|---|---|---|---|
| | Carrier et al., 2003 | | ■ | ■ | ■ | |
| | Baryamureeba et al., 2004 | ■ | ■ | ■ | ■ | ■ |
| | Carrier et al., 2004 | ■ | ■ | ■ | ■ | |
| | Ciardhuáin et al. 2004 | | ■ | ■ | ■ | ■ |
| | Kohn et al., 2006 | ■ | ■ | ■ | ■ | ■ |
| | Rogers et al., 2006 | ■ | ■ | ■ | ■ | |
| | Freiling et al., 2007 | ■ | ■ | ■ | ■ | ■ |
| | Bem et al., 2007 | | ■ | ■ | ■ | |
| | Perumal et al., 2009 | ■ | ■ | ■ | ■ | |
| | Pilli et al., 2010 | | ■ | ■ | ■ | |
| | Roger et al., 2012 | ■ | ■ | ■ | ■ | ■ |
| | Saleem et al., 2014 | | ■ | ■ | ■ | ■ |
| | Bashir et al., 2015 | | ■ | ■ | ■ | ■ |
| | Al-Khateeb et al., 2019 | ■ | ■ | ■ | ■ | ■ |
| | Lone et al., 2019 | | ■ | ■ | ■ | ■ |

## VI. CONCLUSION AND FUTURE WORK

The mapping scheme gives a standardized DFIF for establishing clear guidelines for the forensic process/activities and receiving a precise idea of output for each particular activity which is associated throughout investigation. In our study of the previously proposed framework, the overlays of steps/processes have been detected in each stage with a different vocabulary, focus area and outline characteristics. The proposed mapping schema attempts to reduce the existing convoluted framework to a universal DFIF for investigating cases of all digital incidents and protecting the chain of custody without tampering evidence. In order to augment the investigation process, the proposed mapping scheme can be extended to map for various cases and digital evidence. To verify the effectiveness of the framework, a prototype will be developed. With new technologies, challenges faced by the law still needs to be addressed and encountered by the researcher, which opens a large scope of work[26][27].

## REFERENCES


[1] P. Van Kessel, “Is cybersecurity about more than protection?,” Ey Glob. Inf. Secur. Surv. 2018-2019, 2019.

[2] T. Ten, M. Critical, W. Application, and S. Risks, OWSAP Top 10 - 2017. 2017.

[3] B. Carrier and E. H. Spafford, “Getting Physical with the Digital Investigation Process,” Int. J. Digit. Evid. Fall, 2003.

[4] V. Baryamureeba and F. Tushabe, “The Enhanced Digital Investigation Process Model Venansuis Baryamureeba and Florence Tushabe,” 2004.

[5] M. Kohn, M. S. Olivier, and J. H. P. Eloff, “Framework for a Digital Forensic Investigation.,” Communications, 2006.

[6] Hevner, March, Park, and Ram, “Design Science in Information Systems Research,” MIS Q., 2004.

[7] Ciardhuáin, Séamus Ó, "An Extended Model of Cybercrime Investigations," vol. 3, no. 1, pp. 1–22, 2004.

[8] B. Carrier and E. H. E. H. Spafford, "An event-based digital forensic investigation framework," Proc. 4th Digit. Forensic Res. Work., pp. 11–13, 2004.

[9] R. Jones, "Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet," Int. J. Law Inf. Technol., 2004.

[10] J. I. Trombka et al., "Crime scene investigations using portable, non-destructive space exploration technology," Forensic Sci. Int., 2002.

[11] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," Int. J. Digit. Evid., 2002.

[12] M. Rogers, J. Goldman, R. Mislan, T. Wedge, and S. Debrota, "Computer Forensics Field Triage Process Model," J. Digit. Forensics, Secur. Law, vol. 1, no. 2, 2006.

[13] B. Carrier, "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers," Int. J., 2003.

[14] A. Brinson, A. Robinson, and M. Rogers, "A cyber forensics ontology: Creating a new approach to studying cyber forensics," Digit. Investig., vol. 3, no. SUPPL., pp. 37–43, 2006.

[15] F. C. Freiling and B. Schwittay, "A Common Process Model for Incident Response and Computer Forensics," in IT Incident Management and IT Forensics, 2007.

[16] D. Bem and E. Huebner, "Computer forensic analysis in a virtual environment," Int. J. Digit. Evid., vol. 6, no. 2, pp. 1–13, 2007.

[17] S. Perumal, "Digital Forensic Model Based On Malaysian Investigation Process," IJCSNS Int. J. Comput. Sci. Netw. Secur., 2009.

[18] E. S. Pilli, R. C. Joshi, and R. Niyogi, "A Framework for Network Analysis," Int. J. Comput. Appl., vol. 1, no. 11, pp. 1–6, 2010.

[19] A. EtoundiRoger and M. Moyo Achille, "Multi-perspective Cybercrime Investigation Process Modeling," Int. J. Appl. Inf. Syst., vol. 2, no. 8, pp. 14–20, 2012.

[20] S. Saleem, O. Popov, and I. Bagilli, "Extended abstract digital forensics model with preservation and protection as umbrella principles," Procedia Comput. Sci., vol. 35, no. C, pp. 812–821, 2014.

[21] M. S. Bashir and M. N. A. Khan, "A triage framework for digital forensics," Comput. Fraud Secur., vol. 2015, no. 3, pp. 8–18, 2015.

[22] H. Al-khateeb, G. Epiphaniou, and H. Daly, "Blockchain and Clinical Trial," pp. 149–168, 2019.

[23] A. H. Lone and R. N. Mir, "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer," Digit. Investig., vol. 28, pp. 44–55, 2019.

[24] V. Baryamureeba and F. Tushabe, "The Enhanced Digital Investigation Process," Digit. Forensic Res. Work., 2004.

[25] M. Guido et al., "Generating a Corpus of Mobile Forensic Images for Masquerading user Experimentation," J. Forensic Sci., vol. 61, no. 6, pp. 1467–1472, 2016.

[26] J. H. Ryu, P. K. Sharma, J. H. Jo, and J. H. Park, "A blockchain-based decentralized efficient investigation framework for IoT digital forensics," J. Supercomput., no. 0123456789, 2019.

[27] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," Inf. Sci. (Ny)., 2019.