Digital Forensics Techniques and Trends: A Review

Himanshu Dubey
Department of Computer Science and Engineering,
Netaji Subhas University of Technology, India
himanshu_e21@nsut.ac.in

Shobha Bhatt
Department of Computer Science and Engineering,
Netaji Subhas University of Technology, India
shobha.bhatt@nsut.ac.in

Lokesh Negi
Department of Computer Science and Engineering,
Netaji Subhas University of Technology, India
lokesh.negi.is20@nsut.ac.in

Abstract: *The research work presented in this paper aims to review Digital Forensics (DF) techniques and trends. As computer technology advances day by day, the chances of data being misused and tampered with are also growing daily. The advancement in technology results in various cyber-attacks on computers and mobile devices. DF plays a vital role in the investigation and prevention of cyber-attacks. DF can be used to find the shreds of evidence and prevent attacks from happening in the future. Earlier presented reviews highlighted specific issues in DF only. This paper explores deeply DF issues by highlighting domain-specific issues and possible helpful areas for DF. This article highlights the investigation process framework and related approaches for the digital investigation process. The cognitive and human factors that affect the DF process are also presented to strengthen the investigation process. Nowadays, many DF tools are available in the industry that helps in DF investigation. A comparative analysis of the four DF tools is also presented. Finally DF performance is discussed. The submitted work may help the researchers go deeper into DF and apply the best tools and models according to their requirements.*

Keywords: *Digital forensics, digital evidence, digital investigation model, digital forensic tool.*

Received June 4, 2022; accepted November 27, 2022
https://doi.org/10.34028/iajit/20/4/11

1. Introduction

Digital Forensics (DF) is the branch of forensic science that deals with uncovering and interpreting digital data. DF generally deals with the findings, validation, and interpretation of digital evidence related to a digital crime. Due to internet devices nowadays, the security risks of digital media have also increased [49]. Various attacks, malware, and malicious activities are over the internet. The crimes may occur due to a lack of security and existing known and unknown vulnerabilities; therefore, DF is needed to reach out to the openness and avoid the crime. DF is also used in intellectual property theft, fraud investigation, data theft, bankruptcy investigation, forgery investigation, and industries-related espionage [8, 33]. The primary purpose of using DF is to check the integrity of the information. It is used for protection against data theft, blackmail, and money laundering. DF can be applied in measurement science to investigate the tampering of measurement instruments [26].

The main objective of DF is to retrieve the digital evidence and then maintain the digital proof to its native form so that it can help make a legitimate case [17, 22]. There is a notable variation of digital evidence sources like PCs, laptops, Network servers, hard discs, USB drives, networks, and smartphones. While gathering information during DF, some basic principles must be considered. Forensic experts using the tools must also prepare the activity chart side by side. They have to keep a record of the activities in order.

The research work in DF is challenging, from acquiring data to preserving and protecting the data. As direct testing on the device is not appropriate, an image file is created, and the testing is done on that image file. The image file should always be the same for acquiring the data while obtaining the image from any electronic device, such as hard drives, CDs, DVDs, digital cameras, and pen drives. If the image file is not the same, some tampering is done with the data. Therefore, image file verification is performed by using Message-Digest (MD5) checksum and Secure Hash Algorithm (SHA) checksum algorithms. The DF tool creates the image file, which contains all the modified file information and the deleted files. That image recovers the deleted data, making the image file different from the standard copy function [24]. The next challenge in DF is to develop tools that work on all platforms and support all formats [9]. There are few tools available in the market that operate on the same platform and different file formats. As the distributed system's usage increases, the challenge is further increased. Some data is stored on system A, and some part of the data is saved on system B at the other location, so sometimes it is difficult for a tool to extract the data from different machines simultaneously [41]. Legal issues are another DF challenge after analyzing and documenting data. Certain things need to be addressed to avoid manipulation, like all the investigation is to be done live and recorded, and multiple teams must verify the investigation [23]. Another challenge is to investigate the massive amount of storage at once, so the investigation can be done by splitting the storage. Another challenge is that some cybercriminals use anti-DF techniques, including cryptography and hashing, which may slow down the investigation process, so the digital investigator must be an expert in handling specific security issues. Another challenge is using IP spoofing and mac spoofing techniques by cybercriminals. So, it becomes difficult to locate the address of the cybercriminal, which may create difficulties in the investigation process done by the DF expert [43]. Researchers also face challenges in searching for digital evidence in IoT devices due to the mobility of devices [54]. There is also a lack of well-defined methods for collecting digital evidence.

The studies found that DF is an important research area for researchers, and most researchers have worked on specific issues related to DF. So there is a need to cover more issues related to existing and emerging technologies for DF. The research work presented in this paper covers different issues affecting the DF process. This work presents a survey highlighting the investigation process framework and related approaches for the digital investigation process. The research also aims to cover the general problems and specific domain issues related to IoT-based systems, cloud-based systems, deep learning-based DF, and current trends. The cognitive and human factors that affect DF process are also presented to strengthen the investigation process. Nowadays, many DF tools are available in the industry that helps in DF investigation. The comparative analysis of the four DFtools is also presented in this paper. The DF readiness parameters are also discussed. The performance factors for DF were also highlighted. This work will help to improve the digital investigation process by applying appropriate techniques at every step.

Section 2 elaborates on the literature review, while section 3 describes DF with its branches. Section 4 describes the DF process phases: acquisition analysis and presentation phase. Section 5 focuses on the DF investigation models. Section 6 describes the cognitive and human factors that affect the DF process. Section 7 describes the tools used in the DF investigation process with comparative analysis. Section 8 describes the parameters for Digital Forensic Readiness (DFR). Section 9 presents an analysis and discussion, and the conclusion is presented at the end.

2. Literature Review

This section describes the earlier works carried out to review DF. Different DF investigation models were discussed [3]. The investigation process has changed in the past 25 years, and the approach toward the investigation has also changed. So, the paper also discussed the different models with their shortcomings and advantages. The investigation models from 1995 and up to 2015 were presented. These models are the early phase, Digital Forensic Research Workshop Models (DFRWS) investigation, and computer forensic investigation process models.

The context-based methodology was applied for IoT-based forensic investigations to handle sensitive data [14]. Due to the lack of standardized methods in IoT-based systems, the context was used for investigation using three operating systems: Windows, Ubuntu, and Android. The test was conducted to check the proposed approach in real-life scenarios. The researchers conducted real-life scenarios such as denial of service attacks on the Windows operating system, malware infection in Ubuntu, and internal attacks in Android. It was stated that the proposed method is helpful in real-life investigations.

The survey was conducted for forensic challenges on the Internet of Things (IoT) [51]. It was stated that DF in the field of IoT faces challenges due to the diversity of devices, systems, and non-standardization in the said field. The paper also highlighted legal, privacy, and cloud security challenges in IoT-based systems. It has also discussed the frameworks for extracting data in a privacy-preserving way and securing the integrity of evidence using decentralized blockchain-based systems.

The work discussed helpful investigation systems such as laboratory information management systems, digital media exploitation kits, and advanced forensic formats [25]. This allowed the investigator to think about the different scenarios and follow the right investigation path. The authors also defined new methods to capture other footprints on complex surfaces, which will help the investigation process. The tools for the investigation process, their steps, and their working were also explained.

A review of DF was presented in [7]. The author explained how the pieces of information are collected. The basic principle of DF, the characteristics of DF, and the DF framework were also presented. Five DF tools used in the DF investigation process were EnCase, X-Ways forensics, HELIX3, and XRY with their working.

The research work aimed to review DF capabilities and how to manage them [38]. The authors identified the existing investigation models and the organization's attitudes toward cybersecurity. The authors also discussed the grounded theory methods in DF research. So that method includes how they ground their data in different categories and dimensions. The paradigm model and the DF organizations' core capability framework were presented for data analysis and some results to help understand cybersecurity in organizations. The proposed framework aimed to reduce the possible changes to DF evidence presented in the court of law. The grounded theory presented in this paper solely focused on the process rather than the result, emphasizing the development and analysis process.

Different forensic tools were investigated on specific parameters like reliability and validity [15]. These tools were Helix3 Pro, Forensic Toolkit (FTK) imager, and AIR. It was also stated that other variation performances in the above given three tools depend on measurable and immeasurable parameters. Therefore, the authors also investigated tools for DF. For integrity management, FTK was better than Automated Incident Response (AIR) and Helix3 Pro. FTK and AIR were better than the Helix3 Pro.

The research work described program execution and the data flow for gathering the software used [5]. The system's Random-Access Memory (RAM) has all the information, like active and dynamic processes. The operating system provides no information, but the memory dump or RAM dump can gather it. Several experiments were designed and tested to obtain the information even after stopping the process with the C program resource code.

Researchers described different forensic tools and their performances with comparative analysis [32] .It was clearly stated that the EnCase tool is far better for data recovery than the Autopsy, Recuva, and Operating System (OS) forensic tools. This tool provided the best result and was considered the most suitable tool for analyzing and retrieving the data.

The authors presented how the existing tools can be improved for the investigation process by including searching and recovering deleted files [53]. If the file was deleted, it goes to the recycle bin, and if the file was deleted from the recycle bin, it was never deleted permanently. The deleted file areas were marked as free space and allocated to the new file. So, the area was known as the slack area from where the deleted data was recovered.

The authors contributed a consistent and structured approach to the digital investigation process to collect the primary evidence that can be accepted in a court of law [1]. The existing digital investigation framework was analyzed, reviewed, and then compiled. This iterative structured model helped practitioners make a more convincing forensic case.

The problem of securing the privacy of information in DF and the investigation process was discussed [6]. The authors also reviewed various research fields and their latest trends to address the problems and revealed that every development and trend had influenced privacy issues.

The paper discussed the integration of DF and artificial intelligence for efficiency, accuracy, and cost reduction in the long term. The researchers studied cyber threats intelligence, artificial intelligence, and cybercrime investigation. The research findings show that the cost was reduced in DF by intelligent automation, and it also helps law enforcement agencies to find patterns in different crimes [27].

The research was conducted to find the impact of machine learning-based techniques on DF in voluminous data. DF faces challenges because of large amounts of data and the rapid development of computer science and information technology. The research findings indicated that machine learning-based approaches could be considered optimal methods to solve problems in DF. A large amount of data can be analyzed with a high level of accuracy in a short time. Different machine-learning techniques can be applied to extract and analyze digital evidence [42]. The researchers proposed a proactive approach for malicious software detection with forensic tools [4]. Various machine learning algorithms such as neural networks and decision tree boosted trees were applied to check whether the malicious activity was present. The research findings have shown that boosted tree performed very well. The advantage of using this method is that it does not require updates like antivirus.

As cloud-based services are increasing daily, threats to cloud-based systems are also increasing [40]. The research proposed implementing blockchain-based data login and integrity management for cloud forensics. Research findings indicated that blockchain-based data login could guarantee data integrity and, at the same time, can process more transactions than traditional non-permission-based blockchain systems. Log format unification for cloud environments was proposed to help DF investigators in cloud forensic environments [16]. The log format unification was implemented by using Distributed Management Task Force's (DMTF) and Cloud Auditing Data Federation (CADF) standards.

The ontologies were used in different domains to address the representation and reasoning issues about domain knowledge. The work focused on using ontologies in DF to categorize and explicitly describe the semantics. It was stated that internationally agreed ontological distinction is required for DF [29].

Table 1 shows a comparative analysis of different DF techniques.

Table 1. Comparative Analysis of different DF techniques.

Reference	Objective	Description	Key Findings
[14]	The context-based methodology was applied for IoT-based forensic investigations to handle sensitive data.	Due to the lack of standardized methods in IoT-based systems, the context was used for investigation using Windows, Ubuntu, and Android.	It was stated that the proposed method is helpful in real-life investigations
[32]	Researchers described different forensic tools and their performances.	The latest tools were analyzed and tested on the data recovery scenarios for recovering the information from the different sources.	The EnCase tool is far better for data recovery than the Autopsy, Recuva, and OS forensic tools.
[27]	The paper discussed the integration of digital forensics and artificial intelligence for efficiency, accuracy, and cost reduction in the long term.	The researchers have studied cyber threats intelligence, artificial intelligence, and cybercrime investigation.	The research findings show that the cost was reduced in digital forensics by intelligent automation, and it also helps law enforcement agencies find patterns in different crimes
[42]	Paper addressed the challenges in digital forensics because of large amounts of data and rapid computer science and information technology development.	The research was conducted to find the impact of machine learning-based techniques on digital forensics in voluminous data.	The machine learning-based approaches can be thought of as optimal methods to solve the problems in digital forensics, for a large amount of data can be analyzed with a high level of accuracy in a short time.
[40].	Research work focused on cloud forensics.	The authors implemented blockchain-based data login and integrity management for cloud forensics.	Research findings indicate that blockchain-based data login can guarantee data integrity and can process more transactions than traditional non-permission-based blockchain systems
[29]	The work focused on using ontologies in digital forensics to categorize and explicitly describe the semantics.	The ontologies were used to address representation and reasoning about domain knowledge.	It was stated that internationally agreed ontological distinction is required for digital forensics
[4]	The researchers proposed a proactive approach for malicious software detection with forensic tools.	Different versions of Windows operating systems with malicious registries were used in the conducted work.	The research findings show that boosted tree performed very well. The advantage of using this method is that it does not require updates like antivirus.
[16]	To help DF investigators in cloud forensic environments, log format unification for cloud environments was proposed.	The log format unification was proposed by using DMTF and CADF standard.	It was stated that investigators cannot only detect vulnerabilities but also make sure that in case of any cybercriminal activity, all necessary information is collected under a standard as CADF

3. Digital Forensic

DF can be defined as recognising, preserving, extracting, and documenting digital evidence. It is the process of discovering digital evidence from digital media such as hard disks, pen drives, computers, cell phones, servers, and networks [20, 45]. The digital evidence can be found in browser history/cache, emails, multimedia files, system logs, server logs, and network logs [30]. Figure 1 shows the categorization of DF fields. The upcoming subsequent subsections elaborate on all the categories.

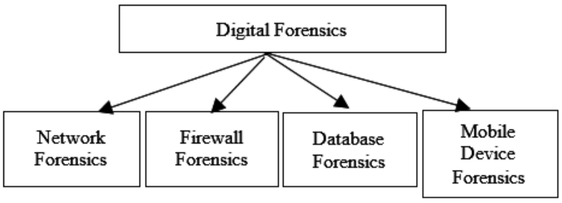

Figure 1. Branches of digital forensics.

3.1. Network Forensics

Network forensics detects various sources of attacking DF approaches [46]. It deals with network traffic analysis, information gathering, intrusion detection, and legitimate evidence. It handles dynamic and sensitive information. It is generally a proactive investigation. It monitors all the files which revolve around the particular network traffic area.

3.2. Firewall Forensics

The firewall keeps track of all incoming and outgoing packets in a log file. The digital investigator uses the same firewall log file to find the evidence and root cause of the crime in the network protected by the firewall [12].

3.3. Database Forensics

The databases and their metadata are used for database forensics. Forensic techniques are applied to the database and its metadata. Database forensics involves the time-stamping of a database and the live analysis for finding database tampering and related issues [39].

3.4. Mobile Device Forensics

It deals with recovering data and digital evidence from mobile devices using DF methods [39]. It also includes devices with internal memory and the communication process, like GPS, tablets, and PDA's.

4. Digital Forensic Phases

The DF process usually consists of three phases: acquisition, analysis, and presentation, as shown in Figure 2. In the acquisition phase, digital evidence is collected and examined in the analysis phase. Finally

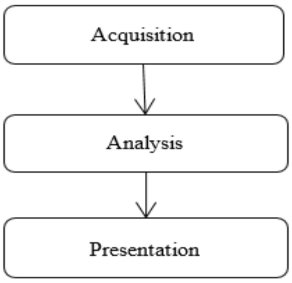

Figure 2. DF phases.

4.1. Acquisition

This phase collects digital evidence from electronic devices or digital devices to be examined later. The acquisition is of two types, namely, data acquisition and memory acquisition. In the acquisition process, data or information is acquired by creating the image of devices, and then the operation is done on that image. Different types of devices from where evidence can be gathered are physical hard drives, pen drives, digital cameras, optical media, and embedded devices and chipsets [36].

4.2. Analysis

It is the process of examining and testing the acquired data after identification and interpretation. The crime-related document, image, file, video, and logs are identified and refined. And then, in the next step, interpretations of digital evidence are made of the acquired artefacts, and then they go further for scientific analysis [34].

4.3. Presentation

It is the process by which the digital investigator will share the reports of their investigations. The case analysis is presented in the court of law for further proceedings. It consists of significant actions taken by the digital investigator and how the investigator does the whole process in steps. Further, the outcomes were carried out after the investigation, and the meaning of the collected artefacts is also presented [19].

The National Institute of Standards and Technology's (NIST) defined DF process includes four phases: collection, examination, analysis and reporting [32]. These three phases are usual in the DF process. However, some DF models include more than three phases. For example, the Systematic Digital Forensic Investigation Model (SDFIM) in [2] has eleven phases for investigating cybercrime and cyber fraud. The Integrated Digital Forensics Process Model (IDFPM) of [34] is divided into four phases preparation, incident, DF investigation, and presentation [30].

5. Digital Investigation Models

The Digital investigation process consists of six phases [37]. Figure 3 shows the DF investigation process framework with six phases: identification of evidence, acquisition and preservation of evidence, examination of evidence, analysis of evidence, documentation of evidence, and presentation of evidence.

1. Identification of evidence: in this phase, the security expert identifies the gadgets or places where the information or data is hidden and then packed and labelled according to the categories [31].
2. Acquisition and Preservation of evidence: in this phase, firstly, the evidence is acquired from the crime scene and then creates the image of obtained digital evidence, which is volatile and non-volatile evidence, and then labels the evidence. After that, packing and transporting the evidence is to be done, resulting in the preservation of evidence.
3. Examination of evidence: forensic experts in this phase examine the evidence through different operations. The forensic expert creates an image of data gathered from the crime scene and then looks at the image file to find the deleted modified files [44].

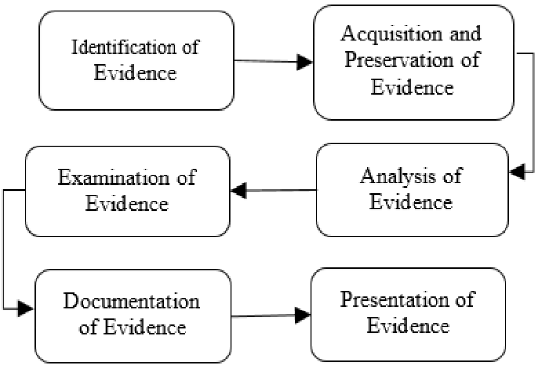
Identification of Evidence
Acquisition and Preservation of Evidence
Examination of Evidence
Analysis of Evidence
Documentation of Evidence
Presentation of Evidence

Figure 3. The DF investigation process.

4. Analysis of evidence: forensic experts analyze the collected information in this phase.
5. Documentation of evidence: this phase maintains the collected evidence in the document form.
6. Presentation of evidence: in this phase, the documented data or information is presented to the court of law [2].

Figure 4 shows different DF models. The abstract Digital Forensic Model (DFM) consists of incident identification, tools and technology preparation, strategic planning, securing the state of physical evidence, gathering physical scenes, duplicating the evidence, analysis, presentation and returning evidence.

The Digital Forensic Research Workshop Model (DFRW) contains processes: identification, preservation, collection, examination, analysis, presentation and decision. This model inspired researchers to enhance further progress in this field. An integrated Digital Investigation Model (DIM) consisting of five phases: readiness, deployment, trackback, dynamite, and review is presented [10]. The authors gave the enhanced digital Forensic Investigation Models (DFIM) in 2004. The traceback and reconstruction methods were added to this model. The extended model of cybercrime investigation gathers information flow of cybercrime in a detailed and systematic way. The DFM based in Malaysia intended to serve cybercrime laws in Malaysia and incorporated live and static data acquisition. The computer forensic field triage process model applies onsite forensic methodology in a short time without the need for a lab [54]. The scientific crime investigation model involves the individualization phase also in addition to other phases. The end-to-end digital investigation model intends to investigate the path of crime from the source to the destination to get the whole picture [50]. Dynamic addition of layers and sublayers with objectives are made in a hierarchical objective-based DIM [11]. The authors also stated that the complete process outcome might differ if the investigator misses a simple step or interchanges the step.

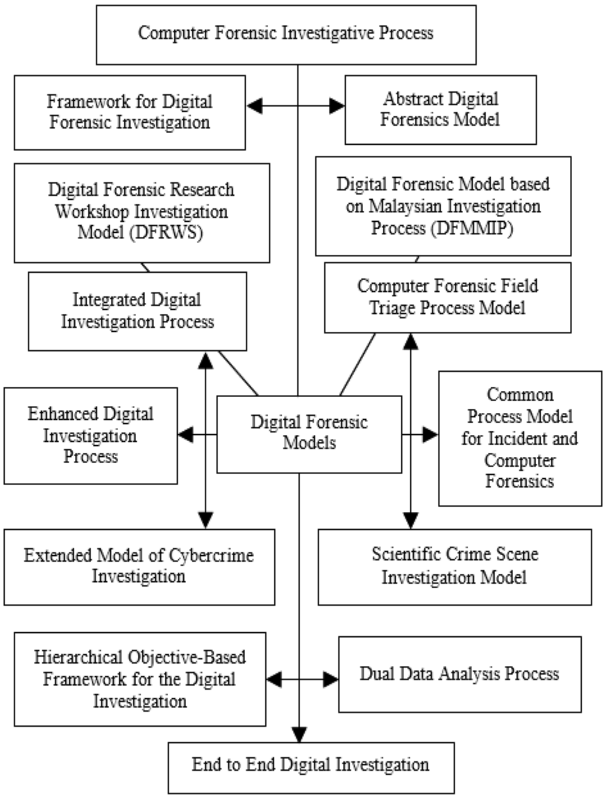
Computer Forensic Investigative Process
Framework for Digital Forensic Investigation
Abstract Digital Forensics Model
Digital Forensic Research Workshop Investigation Model (DFRWS)
Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)
Integrated Digital Investigation Process
Computer Forensic Field Triage Process Model
Enhanced Digital Investigation Process
Digital Forensic Models
Common Process Model for Incident and Computer Forensics
Extended Model of Cybercrime Investigation
Scientific Crime Scene Investigation Model
Hierarchical Objective-Based Framework for the Digital Investigation
Dual Data Analysis Process
End to End Digital Investigation

Figure 4. DF investigation models.

Researchers gave an event-based DF investigation framework in 2004 [13]. This paper presents a framework based on real physical crime scene processes. Each device must be treated as evidence at the physical crime scene in this model. This model works in three phases: preservation of digital evidence, searching and rebuilding the digital evidence. The main focus of the framework is to reconstruct events so that a hypothesis is created and tested or analyzed. Different DFM are used to find the commonly shared processes among the models [54]. The authors proposed a generic model consisting of preprocessing, acquisition, analysis, presentation, and post-process phases.

6. Cognitive and Human Factors in the Digital Forensic Process

Cognitive and human factors can affect the DF process, creating problems in DF investigation. Seven roots of the taxonomy for human and cognitive factors are presented [52]. Researchers also discussed the countermeasures of these factors. Figure 5 shows the cognitive and human factors that may affect the digital investigation process. There are seven factors; the first one is analytic design and brain, which states that the human brain has certain limitations to processing information, resulting in the binding of information in a single piece of information. The second factor is encouragement and training, which states that motivation plays a vital role in the decision-making in the digital investigation process; if the person is highly motivated and trained, it may result in a better investigation result. The third factor is the enterprise factor, which states that communication, social interactions, and identification are essential in the DF organization because they may reduce personal biasing. The fourth factor is the average assumption which states that experience may help solve new cases. The fifth factor is unrelated information which says that first, the relevant information is collected from the crime scene. Then passing that evidence from the collection unit to the analysis unit may cause the chances of mixing irrelevant information or tampering with evidence. The sixth factor is concerned data which states that for solving any criminal case, the data is to be captured and analyzed according to the concerned reference data properly; otherwise, it may increase the chances of biasing. The seventh and last factor is case material that states the collected information is to be correctly tagged or seized; otherwise, it may tamper with the other personal bias.

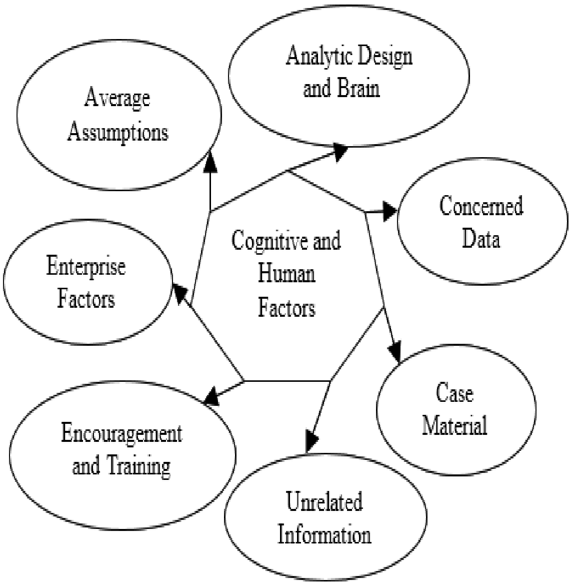

Figure 5. Cognitive and human factors that disturb the DF process.

7. Tools for Performing Digital Forensic Investigation

There are so many tools for performing DF investigations. Some are open-source, and some are licensed versions. According to the requirements, the investigator should use suitable and effective tools for that particular scenario. This section presents the four digital forensics tools with their characteristics.

7.1. EnCase

The Guidance Software developed EnCase in the year 1998. Now it has been acquired by the Open-Text. It is the most accepted forensic tool globally because of its features. 89% of the world's merchandise companies use EnCase software, 91% of the banks use EnCase, 98% of the federal agencies, and 80% of the Universities in the United States use EnCase software. The investigation cycle starts with the investigation, collecting and analyzing the data, and creating a report. It performs remote data collection and processing. It also makes password recovery. It also conducts memory acquisition and data acquisition. It maintains the integrity of the evidence and produces a large number of reports according to the findings. It performs Disk Imaging and data carving [35].

7.2. ProDiscover

It was developed by the Anthony Reyes Company (ARC) Group situated in New York. It is accessible in ProDiscover Basic, ProDiscover Forensic Edition, and ProDiscover Incident Response Edition (IRE). The ProDiscover basic is open source. It gathers the activity snapshots that are mandatory to safeguard user information. Time zone, web browsing activities, and device information can be collected with the help of ProDiscover software whenever required. The examination of files without changing the metadata is done by ProDiscover forensic edition. It is flexible and fast. It performs data acquisition and memory acquisition. It is also available with malware discovery hash sets. It generates computerized reports containing important information regarding the evidence [48].

7.3. Digital Forensic Framework (DFF)

It was developed by Frederic Baguelin, Solal Jacob, and Jeremy Mounier. It is a non-proprietary software digital forensics tool created on a personalized Application Programming Interface (API). It is accessible in 3 choices as Digital Forensic Framework (DFF), which is open source, DFF Pro, and DFF live. Skype analysis, report editor, hash scanner, and automation engine features are available in DFF Pro and DFF live. DFF open source would not get any registered features. It performs cryptographic hash computation. It also conducts a memory dump analysis. It imports all outlook mailboxes. It has batching and scripting capabilities. All the valuable information and web browsing reports are generated. It can extract the data automatically. It can execute the inspection during static and live audits [21].

7.4. Forensic Toolkit (FTK)

The Access Data Group developed FTK. Almost 129,869 government authorities and legal firms use the forensic toolkit globally. FTK can execute analysis on the mobiles and systems. Its main feature is refining, and the finding is slightly quicker than the other tools accessible. It can perform email audits. Users can execute the Forensic toolkit from a pen drive. It can obtain data from 3,600 cell phones. It can gather information during static analysis. It supports multi-languages. It also performs data acquisition and memory acquisition [28].

7.5. Comparative Analysis of the Tools

Table 2 compares four tools on seven parameters: license requirement, operating system support, data recovery, password recovery, Email analysis, real-time alert, and incident response. The license plays a significant role in using the software, while support for different operating systems makes the process easy. Data recovery and password recovery are also the biggest challenges for digital forensics. The email analysis helps the forensic expert to trace the sources of emails which have been deleted also. Real-time analysis of the running system allows digital forensic experts to work more easily. Incident response analysis supports the process by structured monitoring, detecting and reporting the threat [21].

Table 2. Comparison of four DF tools.

Features	Tool 1	Tool 2	Tool 3	Tool 4
License	P	P	OS	OS
Operating Systems	L,M,W,D	L,W	L,W	W
Data recovery	√	√	√	√
Password recovery	√	√	×	√
Email analysis	√	×	×	√
Real-time alert	√	√	√	√
Incident response	√	√	×	√

Nomenclatures used in the above table: Tool 1: Encase, Tool 2: ProDiscover, Tool 3: DFF, Tool 4: FTK, P: Proprietary, OS: Open Source, L: Linux, D: DoS, W: Windows, M: Mac OS.

The table shows that the EnCase software is the best among the four tools in most cases. The table also indicates that EnCase and ProDiscover are paid versions, and DFF and FTK are open sources. All four tools are supported in Windows OS. It is also presented that all four tools are better in real-time alert and data recovery. EnCase, ProDiscover and FTK operate for incident response and password recovery but not the DFF. The email analysis is only done by the EnCase and FTK tools.

8. Parameters for Digital Forensic Readiness

DFR refers to an organization's capacity to respond rapidly to a security issue and collect digital evidence with low expense and disruption to existing operations. There are three parameters for DFR: regular compliance, internal investigations, and legal evidence management [18]. Regular compliance refers to the capacity of an organization to show the regulations and laws by using digital evidence related to DFR. Internal investigations concern an organization's capability to introduce evidence to smooth internal investigations. Legal evidence management deals with the capability of an enterprise or organization to construct evidence that is used in legal cases. Figure 6 defines the value-based performance indicators for digital forensics. It mainly consists of evidence storage with the ability to secure and enforce investigation policies, crime scene processing with security and timely documentation, analyzing evidence with security and in time, information dissemination with utility and complete customer satisfaction.

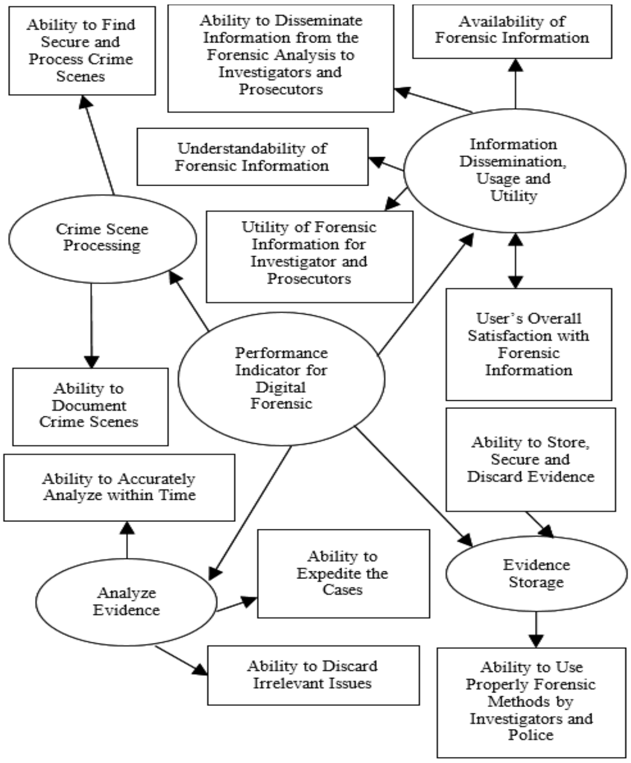
Ability to Find Secure and Process Crime Scenes
Ability to Disseminate Information from the Forensic Analysis to Investigators and Prosecutors
Availability of Forensic Information
Understandability of Forensic Information
Information Dissemination, Usage and Utility
Crime Scene Processing
Utility of Forensic Information for Investigator and Prosecutors
User's Overall Satisfaction with Forensic Information
Performance Indicator for Digital Forensic
Ability to Document Crime Scenes
Ability to Store, Secure and Discard Evidence
Ability to Accurately Analyze within Time
Ability to Expedite the Cases
Evidence Storage
Analyze Evidence
Ability to Discard Irrelevant Issues
Ability to Use Properly Forensic Methods by Investigators and Police

Figure 6. Digital forensic performance indicators [47].

9. Analysis and Discussion

Among all phases of digital forensics, the acquisition phase is more crucial because it is the phase in which the data is collected from the source location. Further, these sources cover evidence related to the crime, but it will be useless if the information is not managed correctly. So, the digital investigator has to collect the data accurately. So, the acquisition phase is the more crucial phase of all the three-phase of digital forensic stages.

The integrated digital investigation process model is the best because of the specific set of operations. The main focus of this model is to map the investigation process to the physical-digital investigation process. The model is quite large because it has five groups consisting of 17 phases. All the groups have their specified set of operations, making this model the best among the model used in this paper. Analytic design and brain, encouragement, and motivation are the most critical factors affecting the DF process. Biasing plays a vital role in the digital investigation process because if an investigator is biased, it may affect the whole process. The human brain has a limited capacity to do tasks. If an investigator reads a number and then writes it wrong in the report because the investigator memorizes it wrong, it may also affect the digital investigation process.

The comparative analysis of different tools shows that EnCase DF tool is more reliable than the aforementioned tools. Among all of them, EnCase is fast in recovery, password recovery, and email analysis. It also provides the feature of real-time alert and incident response. All the operating systems support the EnCase tool. Because of its feature sets, it makes EnCase the best tool.

The parameters used in DFR have their feature set to operate. But the main parameter is the internal investigation because it affects the procedures of the other two parameters. After all, it can propose the evidence in a new way. Further, it was also revealed that there is a need to standardize digital forensics-related issues.

The research findings also indicate a need to standardize DF methods like IoT-based forensics and cloud-based forensics. By using ontologies in digital forensics, better categorization and explicit description of semantics can be performed. It was also concluded that blockchain-based techniques could be applied to cloud forensics. Further, it was also observed that machine learning-based algorithms could be used for fast analysis and recognition-based systems.

10. Conclusions

This paper reviews DF techniques and trends, including different DFIM and tools. It also presents an investigation framework. A comparative analysis of the four DF tools is also presented. It is found that EnCase digital forensic tool is more reliable than other described tools. EnCase is fast in data recovery. Human factors affecting the digital investigation process are also stated in the paper. This paper also presents the parameters for DFR. The research findings can help to use suitable tools, models, and techniques for better results in the digital investigation process. The research can be extended by including artificial intelligence-based methods in DFs.

References

[1] Ademu I., Imafidon C., and Preston D., "A New Approach of Digital Forensic Model for Digital Forensic Investigation," *International Journal of Advanced Computer Science and Applications*, vol. 2, no. 12, pp. 175-178, 2011. DOI:10.14569/IJACSA.2011.021226

[2] Agarwal A., Gupta M., Gupta S., and Gupta S., "Systematic Digital Forensic Investigation Model," *International Journal of Computer Science and Security*, vol. 5, no. 1, pp. 118-131, 2011.

[3] Agarwal R. and Kothari S., "Review of Digital Forensic Investigation Frameworks," *Information Science and Applications*, vol. 339, pp. 561-571, 2015. https://doi.org/10.1007/978-3-662-46578-3_66

[4] Ali M., Shiaeles S., Clarke N., and Kontogeorgis D., "A Proactive Malicious Software Identification Approach for Digital Forensic Examiners," *Journal of Information Security and Applications*, vol. 47, pp. 139-155, 2019. https://doi.org/10.1016/j.jisa.2019.04.013

[5] Al-Sharif Z., "Utilizing Program's Execution Data for Digital Forensics," *in Proceedings of the 3rd International Conference on Digital Security and Forensics (DigitalSec)*, Kuala Lumpur, pp. 12-19, 2016.

[6] Aminnezhad A., Dehghantanha A., and Abdullah M., "A Survey on Privacy Issues in Digital Forensics," *International Journal of Cyber-Security and Digital Forensics*, vol. 1, no. 4, pp. 311-323, 2014. https://go.gale.com/ps/i.do?id=GALE%7CA354578179&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=23050012&p=AONE&sw=w&userGroupName=anon%7E445326da&aty=open+web+entry

[7] Anghel C., "Digital Forensics-A Literature Review," *The Annals of "Dunarea de Jos" University of Galati. Fascicle, Electrotechnics, Electronics, Automatic Control, Informatics*, vol. 42, no. 1, pp. 23-27, 2019. DOI: https://doi.org/10.35219/eeaci.2019.1.05

[8] Arshad H., Jantan A., and Abiodun O., "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence," *Journal of Information Processing Systems*, vol. 14, no. 2, pp. 346-376, 2018. DOI:10.3745/JIPS.03.0095

[9] Bariki H., Hashmi M., and Baggili I., "Defining a Standard for Reporting Digital Evidence Items in Computer Forensic Tools," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, vol. 53, pp. 78-95, 2010. https://doi.org/10.1007/978-3-642-19513-6_7

[10] Baryamureeba V. and Tushabe F., "The Enhanced Digital Investigation Process Model," *in proceedings of the Digital Forensic Research Conference*, Baltimore, pp. 1-10, 2004. https://dfrws.org/presentation/the-enhanced-digital-investigation-process-model/

[11] Beebe N. and Clark J., "A Hierarchical, Objectives-based Framework for the Digital Investigations Process," *Digit Investigation*, vol. 2, no. 2, pp. 147-167, 2005. https://doi.org/10.1016/j.diin.2005.04.002

[12] Bensefia H. and Ghoualmi N., "An Intelligent System for Decision Making in Firewall Forensics," *in Proceedings of the Digital Information and Communication Technology and its Applications*, Dijon, pp. 470-484, 2011. https://doi.org/10.1007/978-3-642-21984-9_40

[13] Carrier B. and Spafford E., "An Event-Based Digital Forensic Investigation Framework," *in Proceedings of the DFRW Digital Forensic Research Conference*, Baltimore, pp. 1-29, 2004.

[14] Castelo Gómez J., Carrillo Mondéjar J., Roldán Gómez J., and Martínez Martínez J., "A Context-Centered Methodology For IoT Forensic Investigations," *International Journal of Information Security*, vol. 20, pp. 647-673, 2021. https://doi.org/10.1007/s10207-020-00523-6

[15] Cusack B. and Liang J., "Comparing the Performance of three Digital Forensic Tools," *Journal of Applied Computing and Information Technology*, vol. 15, no. 1, pp. 1-9, 2011.

[16] Dalezios N., Shiaeles S., Kolokotronis N., and Ghita B., "Digital Forensics Cloud Log Unification: Implementing CADF in Apache CloudStack," *Journal of Information Security and Applications*, vol. 54, pp. 102555, 2020. https://doi.org/10.1016/j.jisa.2020.102555

[17] Damshenas M., Dehghantanha A., and Mahmoud R., "A Survey on Digital Forensics Trends," *International Journal of Cyber-Security and Digital Forensics*, vol. 3, no. 4, pp. 209-235, 2014.

[18] Elyas M., Maynard S., Ahmad A., and Lonie A., "Towards a Systemic Framework for Digital Forensic Readiness," *Journal of Computer Information and Systems*, vol. 54, no. 3, pp. 97-105, 2015. doi:10.1080/08874417.2014.11645708

[19] Galloway P., "Preservation of Digital Objects," *Annual Review of Information Science and Technology*, vol. 38, pp. 549-590, 2004. https://doi.org/10.1002/aris.1440380112

[20] Garfinkel S., "Digital Forensics Research: The Next 10 Years," *Digital Investigation*, vol. 7, pp. S64-S73, 2010. https://doi.org/10.1016/j.diin.2010.05.009

[21] Ghazinour K., Vakharia D., Kannaji K., and Satyakumar R., "A Study on Digital Forensic

Tools," *in Proceedings of the IEEE International Conference on Power, Control, Signals and Instrumentation Engineering*, Chennai, pp. 3136-3142, 2018. DOI: 10.1109/ICPCSI.2017.8392304

[22] Grispos G., Storer T., and Glisson W., "A Comparison of Forensic Evidence Recovery Techniques for a Windows Mobile Smart Phone," *Digital Investigation*, vol. 8, no. 1, pp. 23-36, 2011. https://doi.org/10.1016/j.diin.2011.05.016

[23] Guido M., Buttner J., and Grover J., "Rapid Differential Forensic Imaging of Mobile Devices," *Digital Investigation, Evaluation of Digital Forensics Tools on Data Recovery and Analysis*, vol. 18, pp. S46-S54, 2016. https://doi.org/10.1016/j.diin.2016.04.012

[24] Guo Y. and Slay J., "Data Recovery Function Testing for Digital Forensic Tools," *in Proceedings of the 6th International Conference on Advances in Digital Forensics*, Hong Kong, pp. 297-311, 2010. https://doi.org/10.1007/978-3-642-15506-2_21

[25] Gupta P., Singh J., Kaur A., and Shashi M., "Digital Forensics: A Technological Revolution in Forensic Sciences," *Journal of Indian Academy of Forensic Medicine*, vol. 33, no. 2, pp. 166-170, 2011. https://www.indianjournals.com/ijor.aspx?target=ijor:jiafm&volume=33&issue=2&article=018

[26] Irons A., "Digital Forensics and Measurement Science," *Measurement and Control*, vol. 43, no. 8, pp. 238-242, 2010. DOI:10.1177/002029401004300803

[27] James J. and Gladyshev P., "Automated Inference of Past Action Instances in Digital Investigations," *International Journal of Information Security*, vol. 14, no. 3, pp. 249-261, 2015. DOI:10.1007/s10207-014-0249-6.

[28] Kamal K., Alfadel M., and Munia M., "Memory Forensics Tools: Comparing Processing Time and Left Artifacts on Volatile Memory," *International Workshop on Computational Intelligence*, Dhaka, pp. 84-90, 2016. DOI: 10.1109/IWCI.2016.7860344

[29] Karie N. and Venter H., "Toward a General Ontology for Digital Forensic Disciplines," *Journal of Forensic Science*, vol. 59, no. 5, pp. 1231-1241, 2014. DOI:10.1111/1556-4029.12511

[30] Kent K., Chevalier S., Grance T., and Dang H., *Guide to Integrating Forensic Techniques into Incident Response*, National Institute of Standards and Technology, 2006. doi:10.6028/NIS.SP.800-86

[31] Kohn M., Eloff J., and Olivier M., "Framework for a Digital Forensic Investigation," *in Proceedings of the Information Security South Africa from Insight to Foresight Conference. So*, Sandton, pp. 1-8, 2006.

[32] Lazaridis I., Arampatzis T., and Pouros S., "Evaluation of Digital Forensics Tools on Data Recovery and Analysis," *in Proceedings of the 3rd International Conference on Computer Science, Computer Engineering, and Social Media*, Thessaloniki, pp. 67-71, 2016.

[33] Lillis D., Becker B., O'Sullivan T., and Scanlon M., "Current Challenges and Future Research Areas for Digital Forensic Investigation," *in Proceedings of the 11th ADFSL Conference on Digital Forensics, Security and Law*, Daytona Beach, pp. 1-11, 2016. https://doi.org/10.48550/arXiv.1604.03850

[34] Lim C., Zhang M., Ouw Z., and Ahmadi H., "Forensics Analysis of USB Flash Drives in Educational Environment," *in Proceedings of the International Conference on Information, Communication Technology and System*, Surabaya, pp. 237-242, 2014.

[35] Lovanshi M. and Bansal P., "Comparative Study of Digital Forensic Tools," *Data, Engineering and Applications*, Singapore, pp. 195-204, 2019. https://doi.org/10.1007/978-981-13-6351-1_15

[36] Mcdown R., Varol C., Carvajal L., and Chen L., "In-Depth Analysis of Computer Memory Acquisition Software for Forensic Purposes," *Journal of Forensic Sciences*, vol. 61, no. S1. pp. S110-S116, 2016. https://doi.org/10.1111/1556-4029.12979

[37] Muhammad G. and Alghathbar K., "Environment Recognition for Digital Audio Forensics Using MPEG-7 and Mel Cepstral Features," *The International Arab Journal of Information Technology*, vol. 10, no. 1, pp. 43-50, 2013.

[38] Mukherjee S. and Haque S., "Review Paper on Digital Forensics Practices: A Road Map for Building Digital Forensics Capability," *Iconic Research and Engineering Journal*, vol. 1, no. 9, pp. 96-99, 2018.

[39] Mumba E. and Venter H., "Mobile Forensics Using the Harmonized Digital Forensic Investigation Process," *in Proceedings of the Information Security for South Africa*, Johannesburg, pp. 1-10, 2014. DOI: 10.1109/ISSA.2014.6950491

[40] Park J., Park J., and Huh N., "Block Chain Based Data Logging and Integrity Management System for Cloud Forensics," *Computer Science and Information Technology*, vol. 1, pp. 149-159, 2017. DOI : 10.5121/csit.2017.71112

[41] Popescu A. and Farid H., "Statistical Tools for Digital Forensics," in *Proceedings of the 6th International Conference on Information Hiding*, Toronto, pp. 128-147, 2004. https://doi.org/10.1007/978-3-540-30114-1_10

[42] Qadir A. and Varol A., "The Role of Machine Learning in Digital Forensics," *in Proceedings of the 8th International Symposium on Digital Forensics and Security*, Beirut, pp. 1-5, 2020.

DOI: 10.1109/ISDFS49300.2020.9116298

[43] Rachit., Bhatt S., and Ragiri P., "Security Trends in Internet of Things: A Survey," *SN Applied Sciences*, vol. 3, no. 1, pp. 1-14, 2021. DOI:10.1007/s42452-021-04156-9

[44] Reith M., Carr C., and Gunsch G., "An Examination of Digital Forensic Models," *International Journal of Digital Evidence Fall*, vol. 1, no. 3, pp. 1-12, 2002. https://www.researchgate.net/publication/2589967

[45] Richard G. and Roussev V., "Next-Generation Digital Forensics," *Communications of the ACM*, vol. 49, no. 2, pp. 76-80, 2006. DOI:10.1145/1113034.1113074

[46] Rizal R., Riadi I., and Prayudi Y., "Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 4, pp. 382-390, 2018. https://go.gale.com/ps/i.do?id=GALE%7CA603050343&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=23050012&p=AONE&sw=w&userGroupName=anon%7E426fc0c5&aty=open+web+entry

[47] Rodrigues C. and Toledo J., "A Value Based Method for Measuring Performance on Forensic Science Service," *Gestão and Produção*, vol. 24, no. 3, pp. 538-556, 2017. DOI: 10.1590/0104-530x2137-16

[48] Sanap V. and Mane V., "Comparative Study and Simulation of Digital Forensic Tools," *International Journal of Computer Applications*, vol. 975, pp. 8887, 2015.

[49] Sharma K. and Bhatt S., "SQL Injection Attacks-A Systematic Review," *International Journal of Information and Computer Security*, vol. 11, no. 4/5, pp. 493-509, 2019. DOI: 10.1504/IJICS.2019.101937

[50] Stephenson P., "End-to-End Digital Forensics," *Computer Fraud and Security*, vol. 2002, no. 9, pp. 17-19, 2002. https://doi.org/10.1016/S1361-3723(02)00914-4

[51] Stoyanova M., Nikoloudakis Y., Panagiotakis S., Pallis E., and Markakis E., "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 1191-1221, 2020. DOI: 10.1109/COMST.2019.296258

[52] Sunde N. and Dror I., "Cognitive and Human Factors in Digital Forensics: Problems, Challenges, and the Way Forward," *Digital Investigation*, vol. 29, pp. 101-108, 2019. https://doi.org/10.1016/j.diin.2019.03.011

[53] Velakanti G. and Katuri A., "Enhancement of Existing Tools and Techniques for Computer Forensic Investigation," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 1, pp. 161-164, 2014.

[54] Yusoff Y., Ismail R., and Hassan Z., "Common Phases of Computer Forensics Investigation Models," *International Journal of Computer Science and Information Technology*, vol. 3, no. 3, pp. 17-31, 2011. DOI:10.5121/ijcsit.2011.3302

Himanshu Dubey holds M.Tech in Information Security. He did his M.Tech from AIACTR, GGSIPU, Delhi-India. Himanshu got his B.Tech in Computer Science and engineering. His research areas are digital forensic, cyber forensic, Blockchain, and cyber security.

Shobha Bhatt is an Assistant Professor in the Computer Science and Engineering department at the Netaji Subhash University of Technology, East Campus Geeta Colony Delhi, India. She has obtained Ph.D. from Guru Gobind Singh Indraprastha University Delhi. Dr. Shobha Bhatt has more than 22 years of teaching experience and more than 9 years of research experience. She has guided eight MTech theses and over twenty BTech theses. Her publications in reputable journals and conferences number more than 25, and she has attended several workshops and faculty development programs.

Lokesh Negi holds BTech in Computer Science and Engineering and completed MTech in Information Security from Netaji Subash University of Technology, Delhi, India. He has published conference papers in the area of cryptography and steganography.