


P2DF: A Privacy-Preserving Digital Forensics Framework

Muhammad Abulaish, South Asian University, India

 <https://orcid.org/0000-0003-3387-4743>

Nur Al Hasan Haldar, The University of Western Australia, Australia

Jahiruddin Jahiruddin, Department of Computer Science, Jamia Millia Islamia, India

ABSTRACT

The extensive use of digital devices by individuals generates a significant amount of private data which creates challenges for investigation agencies to protect suspects' privacy. Existing digital forensics models illustrate the steps and actions to be followed during an investigation, but most of them are inadequate to investigate a crime with all the processes in an integrated manner and do not protect suspect privacy. In this paper, the authors propose the development of a privacy-preserving digital forensics (P2DF) framework, which facilitates investigation through maintaining confidentiality of the suspects through various privacy standards and policies. It includes an access control mechanism which allows only authorized investigators to access private data and identified digital evidence. It is also equipped with a digital evidence preservation mechanism which could be helpful for the court of law to ensure the authenticity, confidentiality, and reliability of the evidence and to verify whether privacy of the suspect was preserved during the investigation process.

KEYWORDS

Access Control, Digital Forensics Framework, Digital Investigation, Privacy Preservation

1. INTRODUCTION

The advancements in information and communication technologies have enormously impacted the information storage and sharing approaches in the current digital world. It provides a simple and cost-effective way of storing, transmitting, and sharing of digital data. Though digital technologies have enhanced the life of an ordinary person, they provide equal opportunities to the anti-social elements to use such technologies for many fraudulent activities. Nowadays, cybercriminals find digital technologies and tools to be most convenient and comfortable way for conducting cybercrimes. As a counter-measure, researchers have proposed various tools and techniques to recover digital data from deleted files, browsing history, cache entries, cookies, and registry in an automated manner to control cybercrimes and speed up the investigation process (Al-Rowaily et al., 2015; Yasin & Abulaish, 2013). A detailed discussion and comparative analysis of various digital forensics frameworks and tools can be found in (Abulaish & Haldar, 2018). Such tools and techniques play an important role and they can be used to analyze digital data and collect digital evidences to serve different spectrum of legal and industry purposes (Hibshi et al., 2011). However, usability and performance consistency are still critical issues, as misunderstanding of manuals and technical advancements may lead to false

DOI: 10.4018/IJDCF.288547

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

interpretations in the real-life cases. Moreover, a very few researchers in the area of digital forensics works toward the automation of the investigation process to minimize human effort and investigation time (Gupta, 2013).

Digital forensics is a promising research field, which aims to apply scientific techniques and tools to investigate digital devices of the crime suspects. It uses a number of valid and systematic processes to acquire and validate the digital evidences extracted from the crime-related digital devices. The objective of the digital forensics is to understand and reliably correlate the sequence of crime events supported by the data available in associated digital devices. In 2001, a digital forensic research workshop was initiated to provide a knowledge sharing platform where experts from academia and industries could share their knowledge and experiences related to the digital forensics science. In this venue, Palmer (2001) compiled the definition of digital forensics as “*the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations*”. This is one of the highly popular and accepted definitions in the digital forensics research community. However, Willassen & Mjølsnes (2005) broadened this definition to suit more in the scope of digital forensics by excluding the specific terms such as “criminal events”, “unauthorized actions”, etc. This definition includes various definitions of digital forensics and also includes the commercial investigation forensics analysis (Kohn et al., 2013).

The primary target of digital forensics is to identify crime-related evidences such that an event can be reconstructed. It pursues a proper investigation process to relate digital evidences to establish legal information for judicial process and inspection. Such investigation process follows a number of steps to carry out an appropriate investigation practice. Some of the necessary steps are *identification, preparation, collection, analysis, and presentation* of findings. Most of the forensic investigation approaches differ in the process of data collection methods. Some methods acquire the full image of a digital device, whereas other extract selective data files in accordance with some practical guidelines (Williams, 2012). Though the investigation phases are almost similar in most of the famous process models, the investigation approaches may differ in some cases. Such disparity may occur due to the varieties in digital devices (mobile forensics, computer forensics, etc.), policies (organizational rules, country-based policies, etc.), and associated data types (email data, image, text, etc.).

The generic digital forensics investigation models emphasize on data integrity and advocate to preserve a full bit-stream image of the original storage media. Such models acquire all data stored in suspect’s electronic devices without considering their relevance to the investigation requirements. While considering the civil cases or seizure orders, the private information can be accessed by the inquiry team without its being related to the investigation subject (Law et al., 2011). However, personal data that are irrelevant to the investigation should be masked during the initial phases of the forensics investigation process, and the agencies should handle investigations to protect users’ privacy up to the maximum possible extent. Therefore, privacy preservation should be essentially addressed in digital forensics investigation process. But, unfortunately, most of the existing digital forensics process models do not integrate the concepts and procedures to support data privacy protection. They mainly focus on the technical aspects of data handling, such as collecting, preserving, examining, and explaining the hypothesis of incidents. Hence, investigating an incident with the existing models that lack users’ data privacy concern can breach the human rights. Another fundamental challenge confronted by most of the existing process models is due to the immense volume of user-generated data. Such scenario has a significant impact on data acquisition procedure as well as the way in which data is examined (Mohay, 2005). Other notable challenges can be observed because of the legal and technical complexities of an investigation process. An investigator should strictly follow the guidelines of legal requirements while handling any digital investigation case. Therefore, the aforementioned

significant challenges should be contemplated while proposing a digital forensics process model. To this end, the main contributions of this study can be summarized as follows:

- Presenting a privacy-preserving digital forensics (P2DF) framework which mainly focuses on protection of private data throughout the forensics investigation process.
- Presenting an efficient approach to complete a crime investigation with confidence by providing a set of forensically sound and robust procedures.
- Introducing the use of data warehouse to facilitate data analysis at different levels of granularity.
- Addressing the issues of digital evidence identification, preservation and presentation, various legal and technical challenges, and integration among identified digital evidences.

2. RELATED WORK

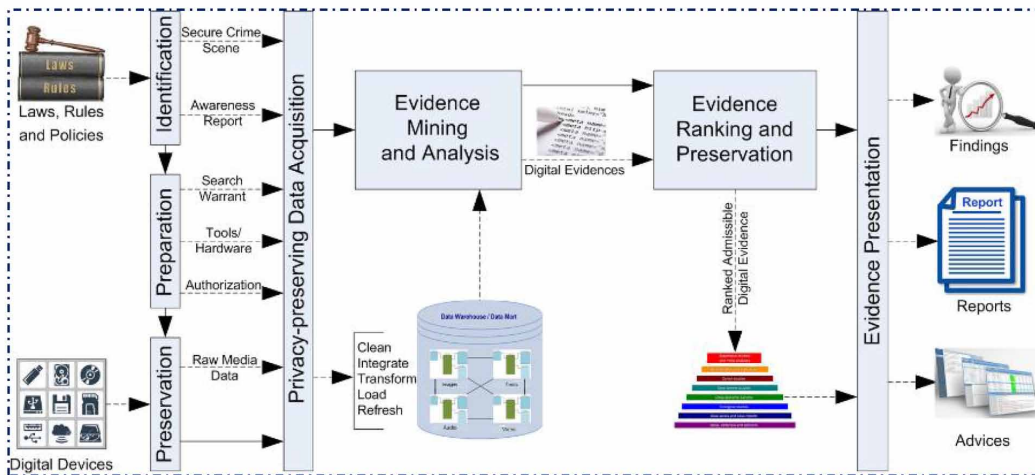
Most of the existing modern age digital forensics framework, e.g., Anwar & Abulaish (2014), are dedicated to forensics analysis, but still lack in the unified solutions as privacy-preserving, evidence mining, and preservation of evidences in an integrated manner. On the other hand, the majority of the earlier age forensics investigation models do not have a clear concept to handle each notion. Privacy-preservation is one of the major concerns which mainly arises when bit-by-bit image of the digital devices is taken by the investigators and imaged data are analyzed as a whole to present before the court of law. Such practices can breach the laws of human rights and privacy. Various digital forensics investigation process models described in (Baryamureeba & Tushabe, 2004; Beebe & Clark, 2005; Carrier & Spafford, 2003; Kohn et al., 2006; Lee et al., 2001; Reith et al., 2002) suffer from such privacy concern. Bui et al. (2003) identified some significant concerns about computer forensics where user privacy was one of the vital interests.

As a solution to the privacy issues in digital forensics framework, Burmester et al. (2002) suggested two different approaches to confronting the privacy challenges – (i) specifying the authorization and privacy policies during an investigation process, (ii) encrypting private data using cryptographic techniques at the time of data acquisition. Deghantaha et al. (2014) presented a privacy-respecting cross-disciplinary foundation which favors both the legal documents like search warrant and the privacy of the user data. Apart from the availability of country-wise data protection systems, Srinivasan (2006) proposed ten other privacy-protecting policies that target to restrict an investigator to analyze private data. However, he realized that only country-specific privacy laws are not sufficient to protect users' privacy alone. In order to balance user confidentiality and investigation process, the authors in (Croft & Olivier, 2010) proposed a digital investigation process, emphasizing to release private data in a sequential manner. In this process, data are packaged in a cryptographic means, and investigator can access the encrypted data until she produces an incriminating evidence. Another cryptography-based model was proposed by Law et al. (2011), which allows a data owner to encrypt digital media and perform index over it. The investigator performs keyword search using an encrypted keyword list without having any knowledge about the encryption key. Such practices are useful to protect user data privacy, but investigator must be reliable to the data owner. In some case, if the data owner encrypts the investigator's search keys with a false key, the investigator will be unable to find a conclusion. On the other hand, a different approach based on homomorphic and commutative encryption scheme was presented by Hou et al. (2011). This method allows investigation officer to obtain necessary evidence at the time of protecting the privacy of a user.

Most of the aforementioned researches have attempted to solve a conflict between forensics approaches and privacy preserving without providing any practical solution. The cryptography-based privacy preserving proposals encrypt all user data during evidence collection phase, and again decrypt those in evidence analysis phase. The problem with these processes is that encryption and decryption of complete user data is costly and an inefficient solution. The relevant-only but private data should be encrypted to speed up a privacy protected investigation process. In the line, other existing

subjects associated with the forensics frameworks suffer with the issue of handling enormous data. Evidence confirmation from a vast set of digital data and the preservation of identified evidences create various problems. They add much more complexities due to existing of storage media with much larger storage capacity (Garðnkel, 2010). The challenges due to voluminous digital data have been debated by various forensics experts in (Garðnkel, 2010; Raghavan, 2013), including some genuine concerns related to the data diversity and storage. However, as a solution to this problem of extracting evidences from the voluminous digital data, a variety of approaches have been proposed by the researchers. Some of the remarkable strategies are data reduction (Raghavan, 2013; Beebe, 2009), user-profiling (Garðnkel,2010), data mining (Beebe & Clark, 2005; Chen et al., 2004), triage (Parsonage, 2009; Rogers et al., 2006), and case-oriented mining (Zhang&Wang, 2009). Instead of having a number of researches related to the data handling issue only, a unified and integrated solution for both analytical efficiency and privacy preservation is still an unsolved subject.

Figure 1. System architecture of privacy-preserving digital forensics (P2DF) framework



3. PROPOSED FRAMEWORK

This section presents the functional details of our proposed privacy-preserving digital forensics (P2DF) framework, which can be used for data acquisition and analysis, evidence mining, presentation of identified evidences, and preservation of the digital data in an integrated manner without compromising the user’s privacy. Figure 1 presents an architecture of P2DF, depicting different modules and their interdependence. The phases of P2DF framework are *identification*, *preparation*, *preservation*, *privacy-preserving data acquisition*, *evidence mining and analysis*, *evidence ranking and preservation*, *evidence presentation*, and *review*. It follows an iterative flow and executes each phase in a sequence. Backtrack of a previous phase is allowed only if the current phase is not satisfied with the output of the last step. Hence, previous phases can be reviewed by tracing back from the current phase. Figure 2 presents a sequence diagram of the P2DF phases. Phase-wise description of the P2DF framework is presented in the following sub-sections.

3.1 Identification

Identification is the very first phase of the proposed P2DF framework. This step is initiated by reporting a crime or a suspected incident. The type and the characteristics of the offenses are also identified here. In this phase, laws, rules, and crime-related policies are imposed in measuring the intensity as well as the impact of the offenses in the system. One of the important activities of this phase is to secure and well document a crime scene such that intruders could perform no modifications or damages. Such items which may contain crucial evidence for a suspected incident have to be seized, and a list of evidences is to be identified and must be initiated for custody. In this phase, an awareness should also be created such that the need for an investigation can be evaluated. Though this phase is not explicitly within the existing model, it is a significant phase because of its impact on other aspects.

3.2 Preparation

The *preparation* phase comes into the course once the identification phase is completed and investigators are asked to carry out the research. The court of law should issue a search warrant and authorization letter before initiating the investigation process. In this phase, important activities related to tools selection, strategy, support, and management are performed. This phase also ensures suitability of the operations and existing infrastructure to support the investigation. Identification and management of required tools and equipments to match the level and type of digital crime is also an important constituent of this phase. The tool selection is one of the major activities of this phase. The associated personnel are trained with the selected tools such that the enormous digital data can be handled easily in time. The chosen equipment must be well-functioning and should be ready to perform as soon as instructed. In some cases, if the investigation team identifies some tasks which are beyond their expertise, it should be informed promptly to the authorities. The authorities and investigation team together should take alternative strategies to solve such impediments. After handling all the technical and operational barriers, other concern parties should be informed about the subject of investigation.

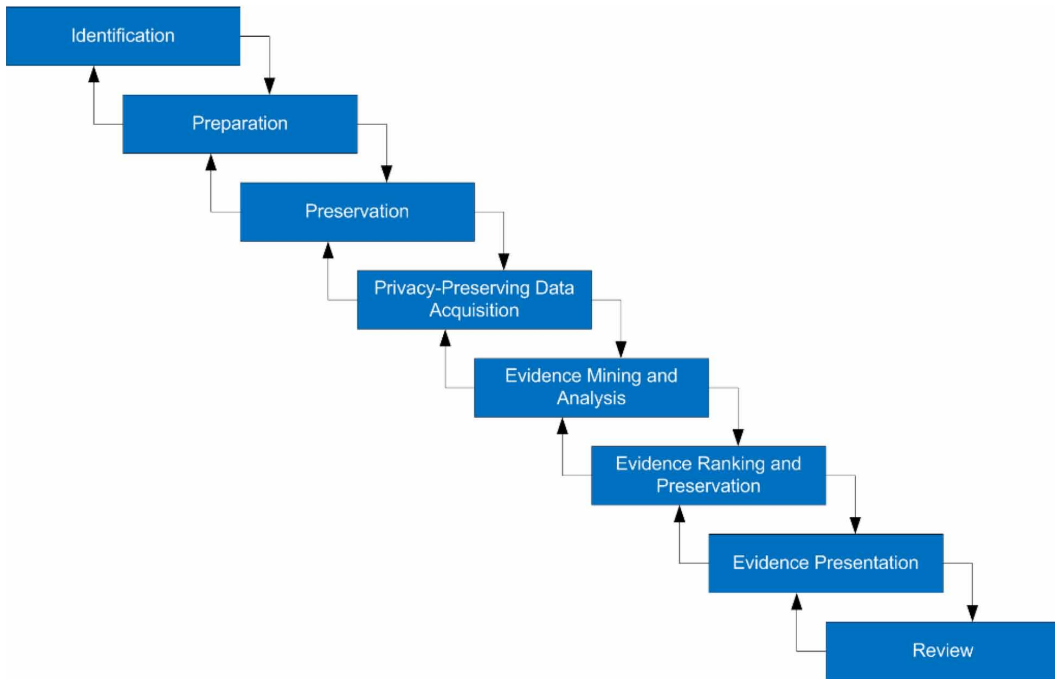
3.3 Preservation

The *preservation* phase of the P2DF framework targets to preserve the digital crime scene for further validation using synchronization and analysis of evidences. After seizing the digital media of suspects, bit-by-bit imaging of the contents of the original data is performed. The process of imaging should be in a way (i.e., write protected mode) such that it can prevent any accidental or unintentional changes while copying by an investigator. The imaging of “two” same copies is suggested in our process model where one copy will be preserved safely by legal authorities, and digital forensics investigator will use another copy of the disk image. The court of law can use the first copy of the image as a safeguard to confirm about any doubt related to any evidence. However, integrity should also be preserved in both of the duplicate copies. The original digital drives must be kept in a secure place to avoid any possibilities of data tampering. The preservation phase in P2DF framework is not about the preservation of evidence because confirmation about evidence is not yet recognized. This phase is to preserve all the digital data from the suspect’s devices to safeguard data integrity. The protected digital images are verified in each step using MD5 or SHA-1 hash technique so that any change in the image copy can be detected promptly.

3.4 Privacy-Preserving Data Acquisition

The *data acquisition* phase takes the retained digital images as a source of data. However, the activities of data acquisition phase in P2DF framework are not simple like other forensics process models. In most of the available models, the complete system data is used to identify evidence. However, only most relevant data that are related to the crime under investigation are considered in P2DF framework. Since an accused cannot be treated as a criminal unless she is convicted by the court of law, it is

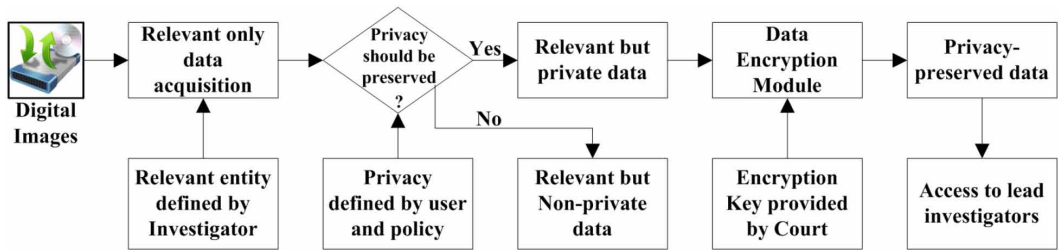
Figure 2. Phases of proposed privacy-preserving digital forensics (P2DF) framework



unethical to extract and analyze her private data in the name of investigation. In other words, we need to extract only crime-related data and that too should be kept confidential. The relevance of each data source (i.e., folders, files, or hard disk partitions) is marked by the investigator, whereas the privacy is defined by the user and organizational laws. The data acquisition module extracts data from the storage devices based on the given case profile. It takes three input for data acquisition – (i) extracted image of the digital devices, (ii) case information and sample evidence (of incident type), and (iii) privacy entities defined by the user. The case information contains a set of possible crime scenario, reporting time of the offense, type of crime, investigator’s findings of the case (if any), and other observations which are important according to the investigator. Based on such criteria, the data acquisition is performed and the acquired data are stored in a data warehouse to facilitate OLAP operations.

The collected data should not be disclosed or shared with any unauthorized party. Both the data integrity and the data confidentiality should be well maintained. Any information which is not relevant to investigation should not be acquired at all. However, a relevant data may be private to a suspect and disclosure may affect human rights and privacy policies. In P2DF framework, extra attention is given to those data which are private to the user as well as relevant from investigator point of view. However, the approach of handling such type of data is entirely dissimilar than the processing of a non-private but relevant data. In line to the privacy-preservation approaches presented in (Halboob et al., 2014), a set of different data access levels can be constructed to handle data according to its relevance as well as sensitivity score. The most relevant and private data can be accessed by higher ranked investigators only. A flow-diagram of the privacy-preserving data acquisition module of P2DF framework is shown in figure 3.

Figure 3. Privacy-preserving data acquisition module



3.5 Evidence Mining and Analysis

Evidence mining refers to the computational process of discovering non-trivial patterns in large data. It involves some techniques of artificial intelligence, machine learning, statistics, and database systems. It also assists forensics investigators by producing some proper conclusions from the hefty dataset. In this phase, the crime-related evidence is extracted from the relevant acquired data. The potential evidences are usually kept hidden within some unusual locations. The more the relevant and concrete data are extracted from the hidden places, the more the useful proofs can be gathered for data analysis. Evidence validates the facts of a crime scene, and it can be used as testimony in the courtroom proceedings. In this context, the focus of evidence mining is not only to find proof to testify an offense, but also to preserve the output to support future investigations. Among various existing data mining techniques, pattern matching and descriptive modeling such as density estimation and cluster analysis will be useful in this phase to identify non-trivial evidences. Meanwhile, the sequential pattern of proof is necessary to identify evidence from the acquired data. To this end, association rule-based algorithmic techniques are more useful to find sequential patterns of evidence.

The *analysis* phase is used to draw conclusions based on the analysis of the identified evidences. In the analysis phase, a proper hypothesis will be created to find out the root cause of the incident, and it should be tested using acquired evidences. It can also initially predict the severity of the crime occurrences. However, one of the primary objectives of forensic analysis is the reconstruction of the events, which plays a critical role in solving a crime case by explaining individual characteristics of each piece of evidence. In the very first step of event reconstruction, an object is selected which is most relevant to the current needs of the investigation and has the unique characteristic change (Carrier & Spafford, 2004). The P2DF model helps an investigator to discover the data patterns from the evidence list. In the same way, a weighted graph can be formed using the metadata associated to the data patterns. In such graphs, nodes represent entities (i.e., person, organization, place, etc.) and edges represent the interaction between entities. The weights of edges can be computed using various statistical measures. Thereafter, evidence patterns, such as user community, community leader, outlier entity, etc. can be identified using different data mining techniques, which have unlimited potential to analyze evidence in a more efficient and faster manner.

3.6 Evidence Ranking and Preservation

Ranking of evidences saves both time and effort of the investigator by avoiding to search all recorded files. A less relevant evidence may also create much disorientation and may mislead the investigation findings. Hence, ranking of identified evidences is useful in better assumption and presentation of crime linkages. The *evidence ranking* module of the P2DF framework generates the levels of the files obtained from the *evidence mining* module. The weight of each potential evidence is calculated using various features associated with the evidence file. Some of the notable features that can be used for evidence ranking are: *similarity/relevance score, term priority, term frequency and inverse document*

frequency (TF-IDF), file creation, modification and access times, access frequency, evidence file type, evidence file depth, and file name.

A commutative rank of the relevance of each evidence is calculated using the features mentioned above. The rank is calculated as a function of relevance to the case. Ranking of each evidence file is provided from the case profile, and relevance of any evidence is directly proportional to its rank. The higher the rank of an evidence, the more the significance of it in the investigation process. Various evidence ranking algorithms, such as SVM-Rank, Search Hit Ranking algorithm, etc. can be used to calculate the position of the evidence documents. Such ranking of each evidence determines the importance in the investigation. A threshold can be used to filter out low-ranked evidences and its value can be tuned by the investigators depending on the severity of the case. The concept of evidence ranking has much more benefits in digital forensics investigations. It can not only concise the conclusion of an inquiry, but it can also help the court of law to take an immediate decision by concentrating on the top-ranked evidences only.

The preservation of digital evidence is incorporated during investigation process and ensuring the integrity of the digital evidences in the acquired image of the evidences. The P2DF framework has a Digital Evidence Preservation (DEP) mechanism which ensure the authenticity and confidentiality of the collected and stored evidences. The DEP module of our proposed framework contains two components (i) *Forensic Access Control (FAC)*, and (ii) *Secure Forensics Audit Trail (SFAT)*. The *FAC* ensures the prevention of the access of evidence data from unauthorized person, whereas the *SFAT* ensures the security of the digital evidences by recording activities of an investigator. The evidence is prevented from accessing by unauthorized person by encrypting them using identity-based encryption (IBE) technique. It could be helpful for the court of law to ensure the authenticity and reliability of the evidences, and to check whether privacy of the person was preserved during the investigation process, by tracking the activities of the investigator.

3.7 Evidence Presentation

At the end of the investigation process, a decision based on the adequate evidence should be made. The aim of this phase is to justify the findings of the case to a variety of audiences, including managerial board, legal authorities, technical personnel, and law enforcement. The presentation should be easily understandable to the community such that it can make an effective decision quickly. The compilation of evidence presentation deals with the entire investigation process, the sequence of proof, a chain of custody, and investigation findings. Advice and opinions are also made by the investigators to conclude the investigation from their side. One copy of the phase-wise documentation which was compiled during the inquiry process should be submitted to the court of law and included in the final presentation of reports based on their relevance in reaching a decision. However, the presentation of evidence is sometimes perplexed by the immature investigator and presenter, which may be further aggravated by the inadequate case management. Hence, to minimize the probable confusions, the findings should be presented by some experienced presenter. The final report should clarify the findings statistically with the legally acceptable logics and proofs. The report must be compact with a proper explanation of conclusion. Nevertheless, the presenter should be ready to defend any criticism, challenges or queries of the defender.

3.8 Review

The final phase of our proposed framework is the *review*, and it aims to review the findings and evidences to reconsider the investigation to identify the areas of improvement. In case any unsolved queries and criticisms still exist, a proper consideration of the study should be made to enhance the investigation outcome accordingly. Investigators can decide whether it is sufficient to review some particular module or a sequence of modules to improve the quality of evidence. However, each phase of the P2DF model is reviewed at the same time while investigation. This process is optional when the court of law is not satisfied with the findings, and the process of inquiry is identified for better

Table 1. Phase-wise activities and outcomes of the P2DF process model

Phase	Activities	Expected output
Identification	<ul style="list-style-type: none"> - Informing crime incident to authority - Identifying type of crime - Identifying need of investigation - Seizing suspects potential belongings - Documenting crime scene 	<ul style="list-style-type: none"> - Secure crime scene - Awareness report - Initial investigation record
Preparation	<ul style="list-style-type: none"> - Proper planning to execute investigation - Ensuring operation and infrastructure to support investigation - Issuing search warrant and authorization letter - Identifying strategy, policy and previous investigations - Notifying concern parties about the subject of investigation - Selecting relevant tools and techniques - Training technical team - Authorizing tasks to team members 	<ul style="list-style-type: none"> - Roadmap of investigation - Search warrant - Authorization - Notification - Approach strategy
Preservation	<ul style="list-style-type: none"> - Determining possible source of evidence storage - Imaging of storage media - Ensuring write protection while imaging - Verifying integrity and authenticity of data after imaging 	<ul style="list-style-type: none"> - bit-by-bit image of the digital storage - Potential data sources
Privacy-preserving Data Acquisition	<ul style="list-style-type: none"> - Defining relevance of data entity accordingly to investigation type - Compiling privacy rules and policies of country or organization - Defining user privacy - Extracting relevant only potential evidence data - Labeling user private data - Encrypting relevant but private data and handling with concern - Storing into data warehouse 	<ul style="list-style-type: none"> - Relevant-only data storage - Possible digital evidence sources
Evidence Mining and Analysis	<ul style="list-style-type: none"> - Locating potential evidence (possibly within unconventional locations) - Determining and validating technique to find and interpret significant data - Identifying evidence pattern and hidden data from acquired data - Analyzing evidences to determine its significance over crime - Formulating hypothesis to find out root cause of crime - Drawing conclusion based on identified evidences 	<ul style="list-style-type: none"> - Evidence files - Log files - Analysis result
Evidence Ranking and Preservation	<ul style="list-style-type: none"> - Identifying metadata which is useful to calculate the importance of evidence - Calculating weight of each evidence - Ranking evidences based on their significance in the incident - Preserving evidence for future reference 	<ul style="list-style-type: none"> - Ranked admissible digital evidence - Top-ranked evidence storage
Evidence Presentation	<ul style="list-style-type: none"> - Preparing and presenting the findings after analyzing the evidence - Creating report to summarize findings - Clarifying evidence and documenting all findings - Defending any type of criticism and challenges - Suggesting advice to help while concluding the case 	<ul style="list-style-type: none"> - Report of findings - Advice and notes
Review	<ul style="list-style-type: none"> - Reconsidering the investigation to identify the areas of improvement - Identifying exact modules to revisit 	<ul style="list-style-type: none"> - New procedure of investigation - Enhanced approach strategy

enhancement. The outcome of this phase could be a new procedure, or it may be any enhanced approach of analysis. Table 1 presents a summary of the phase-wise activities and expected outcomes of the P2DF model.

4. VALIDATION OF P2DF WITH RESPECT TO EXISTING FRAMEWORKS

We present a validation of the P2DF model with respect to 10 existing digital forensics frameworks. For reference purpose, we have named the existing frameworks as DFF01, DFF02, and so on. Table 2 presents a list of phases and sub-phases of the existing digital forensic frameworks. The IDs of these phases and sub-phases are written in parenthesis. Table 3 presents a comparison of the P2DF framework with existing digital forensic frameworks in terms of the phases and sub-phases. It can be observed from this table that DFF10 has maximum number of phases/ sub-phases. Moreover, P2DF has many novel sub-phases, such as *Privacy-preserving Data Acquisition (4.4)*, *Evidence Mining and Analysis (5.7)*, *Evidence Ranking and Preservation (5.8)*, and *Evidence Presentation (6.4)*, where the *Privacy-preserving Data Acquisition (4.4)* sub-phase is used to consider the privacy of the suspect at the time of investigation. Since most of the phase of our proposed P2DF framework are present in existing digital forensic frameworks, we provide validation of only newly introduced phases of P2DF in the following sub-sections.

Table 2. A summarized list of phases and sub-phases present in existing digital forensic frameworks

Phase (ID)	Sub-Phase (ID)
Identification (1.0)	Detection (1.1)
Preparation (2.0)	Readiness (2.1), Planning (2.2), Approach Strategy (2.3), Incident response (2.4), Formulation of response strategy (2.5), Notification (2.6), Documentation (2.7)
Preservation (3.0)	Data duplication (3.1), Storage (3.2)
Acquisition (4.0)	Collection (4.1), Gathering (4.2), Harvesting (4.3), Privacy-preserving Data Acquisition (4.4)
Analysis (5.0)	Evaluation (5.1), Examination (5.2), Interpret (5.3), Investigation (5.4), Reconstruction (5.5), Hypothesis (5.6), Evidence Mining and Analysis (5.7), Evidence Ranking and Preservation (5.8)
Presentation (6.0)	Report (6.1), Admission (6.2), Proof & Defense (6.3), Evidence Presentation (6.4)
Review (7.0)	---

4.1 Validation of Privacy-Preserving Data Acquisition Phase

In line to Halboob et al. (2014), the relevance and sensitivity score can be assigned to each data file by the expert investigators, based on their prior knowledge of the investigation and various organizational rules. Similarly, in line to Armknecht & Dewald (2015) and Tran et al. (2020), the private data of the suspect that are pertinent to investigator can be encrypted using the keys provided by the legal authorities, and such data can be made accessible to only top investigation officers. Like Seyyar & Geradts (2020), the top officers may search the keys in such private data without decrypting it. In line to Zhang et al. (2018), we have provided the following lemma that the data acquisition operation of P2DF framework preserves the privacy of the suspect.

Table 3. A comparison of P2DF with existing digital forensics frameworks in terms of phases and sub-phases

Digital Forensic Framework	Author, Year [Reference]	Phase & Sub-phase IDs
Investigative Process for Digital Forensic Science	(Palmer, 2001)	[1.0], [3.0], [4.1], [5.0, 5.2], [6.0]
Scientific Crime Scene Investigation Model	(Lee et al., 2001)	[1.0], [3.0], [4.1], [5.1, 5.3, 5.5], [6.0, 6.1]
Abstract Digital Forensics Model	(Reith et al., 2002)	[1.0], [2.0, 2.3], [3.0], [4.1], [5.0, 5.1], [6.0]
Integrated Digital Investigation Process Model	(Carrier & Spafford, 2003)	[1.1], [2.1], [3.0], [4.1], [5.4, 5.5], [6.0], [7.0]
Enhanced Integrated Digital Investigation Process	(Baryamureeba & Tushabe, 2004)	[1.1], [2.1], [3.0, 3.1], [4.1], [5.4, 5.5], [6.0], [7.0]
Extended Model of Cyber Crime Investigation	(Ciardhuáin, 2004)	[1.0], [2.2], [3.2], [4.1], [5.2, 5.6], [6.0, 6.3]
Hierarchical, Objective-based Framework	(Beebe & Clark, 2005)	[2.0, 2.4], [4.1], [5.0, 5.2, 5.5], [6.0], [7.0]
Investigative Framework	(Köhn et al., 2006)	[2.0, 2.2, 2.3, 2.6], [3.2], [4.1], [5.0, 5.2, 5.4], [6.0]
FORensics ZACHMAN framework (FORZA)	(Jeong, 2006)	[1.0], [2.2], [4.0], [5.0, 5.5], [6.0]
Integrated Digital Forensics Process Model	(Kohn et al., 2013)	[1.1], [2.0, 2.1, 2.3, 2.4], [3.0, 3.2], [4.1], [5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6], [6.0, 6.1], [7.0]
Privacy-Preserving Digital Forensics Framework (P2DF)	(Abulaish, Proposed)	[1.0], [2.0], [3.0], [4.4], [5.7, 5.8], [6.4], [7.0]

Lemma 1: *The data acquisition operation of P2DF preserves the privacy of the suspect.*

Proof: In our framework, the data irrelevant to the crime is not accessed by investigators. The relevance score is assigned by expert investigator and privacy of the data is marked by user of the data. Since private relevant data is encrypted using the keys provided by the legal authority, and only top investigation officers are allowed to perform the search operation without decrypting it, privacy of the user can not be breached. In this way, privacy of the suspect is preserved at the time of data acquisition.

4.2 Validation of Evidence Mining and Analysis Phase

In this phase, the crime-related evidence is extracted from the relevant acquired data. It is used to identify a set of evidence to understand the development of a crime scenario. At the time of evidence mining, it does not decrypt the relevant private data. The investigation officer creates a set of key terms based on his/her experience and similar previous crimes, and search them in acquired data without decrypting them. A private relevant data is marked as an *important evidence* only if it consists of at least t (a threshold decided by the investigation officer) key terms. Thereafter, only legal authority can decrypt and access private data, if needed, without sharing with the investigation officer. The analysis phase is used to analyze the identified evidences to draw conclusion. Before data analysis, the integrity and authentication of the data is to be checked, as proved in the following lemma.

Lemma 2: *The evidence mining and analysis phase of P2DF preserves the privacy of the suspect.*

Proof: Since the key terms are searched in this phase in private relevant data without decrypting the related files and the file containing important evidences are decrypted by only legal authorities and they are not shared with investigation officer, the privacy of the suspect is preserved.

4.3 Validation of Evidence Ranking Phase

In this phase, acquired files are ranked based on the rank scores computed using the identified relevant search keys (terms) and other features of the files. In P2DF, files are ranked on 10 parameters. Out of these, 3 parameters are computed using relevant terms such as *similarity/ relevance score*, *term priority-based score*, and *TF-IDF score*; whereas remaining parameters are computed using files' features such as *creation time*, *modification time*, *access time*, *access frequency*, *file type*, *file depth*, and *file name*. After rank computation, top- k files are considered for initial investigation, where value of k is determined by the investigator. Starting with a small k value for initial investigation, investigator may proceed to increase the value of k if further files need to be investigation.

Lemma 3: The evidence ranking phase of P2DF preserves the privacy of the suspect.

Proof: Since files are ranked based on various parameters, instead of investigating all data/files of the suspect, investigator may start with a small set of (top- k) files that are most relevant to the crime under investigation, and thereafter more files can be considered in a phased manner if further evidences need to be acquired. Moreover, the relevant key terms are searched in private relevant data without decrypting the related files. Hence, in this phase too, the privacy of the suspect is preserved.

5. CONCLUSION AND DISCUSSION

In this study, we have presented a privacy-preserving digital forensics (P2DF) framework, which facilitate the forensic investigation officers for investigating digital crimes in an integrated manner without breaching the privacy of the suspect. The P2DF framework targets to devise efficient algorithms to identify and correlate important digital evidences from voluminous and varied data efficiently. Most of the available frameworks meet some issues related to evidence storage. Due to the multi-dimensional nature and high complexity of data, it is not easy to access evidence in a convenient manner. Such problem may also create various complications while producing the exact evidence whenever asked for. Development and integration of a data warehouse to store processed data seems very useful to apply subsequent analysis using OLAP operations at different levels of granularity. The proposed framework ensures data integrity and reliability through an audit trail mechanism, recording all activities of the investigators to ensure that they have not exceeded the defined scope of the investigation. Such mechanism could also be useful for the court of law to verify the reliability of the identified digital evidences. Evidence ranking is another important constituent of the P2DF framework. The traditional frameworks dedicated to digital forensics investigation consider each evidence with the same importance. Such assumption may create complication while presenting a fact. The P2DF framework includes evidence ranking module to rank the evidence according to their relevance to the crime under investigation. Evidence ranking allows fast access to the evidence. Moreover, it is also useful to concise the findings for a better presentation in court of law.

REFERENCES

- Abulaish, M., & Haldar, N. A.-H. (2018). Advances in Digital Forensics Frameworks and Tools: A Comparative Insight and Ranking. *International Journal of Digital Crime and Forensics*, 10(2), 95–119. doi:10.4018/IJDCF.2018040106
- Al-Rowaily, K., Abulaish, M., Haldar, N. A.-H., & Al-Rubaiana, M. (2015). BiSAL – A Bilingual Sentiment Analysis Lexicon to Analyze Dark Web Forums for Cyber Security. *Digital Investigation*, 10, 53–62. doi:10.1016/j.diin.2015.07.006
- Anwar, T., & Abulaish, M. (2014). A Social Graph Based Text Mining Framework for Chat Log Investigation. *Digital Investigation*, 11(4), 349–362. doi:10.1016/j.diin.2014.10.001
- Armknecht, F., & Dewald, A. (2015). Privacy-preserving email forensics. *Digital Investigation*, 14, S127–S136.
- Baryamureeba, M. V., & Tushabe, F. (2004). The Enhanced Digital Investigation Process. *Proceedings of the Digital Forensic Research Workshop*, 1-9.
- Beebe, N. (2009). Digital Forensic Research: The Good, the Bad and the Unaddressed. *Proceedings of the IFIP International Conference on Digital Forensics*, 17-36.
- Beebe, N., & Clark, J. (2005). Dealing with Terabyte Data Sets in Digital Investigations. *Proceedings of the IFIP International Conference on Digital Forensics*, 3-16.
- Beebe, N. L., & Clark, J. G. (2005). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. *Digital Investigation*, 2(2), 147–167. doi:10.1016/j.diin.2005.04.002
- Bui, S., Enyeart, M., & Luong, J. (2003). *Issues in Computer Forensics*. Santa Clara University Computer Engineering.
- Burmester, M., Desmedt, Y., Wright, R., & Yasinsac, A. (2002). Security or Privacy, must we choose? *Proceedings of the Symposium on Critical Infrastructure Protection and the Law*, 1-8.
- Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*, 2(2), 1–20.
- Carrier, B. D., & Spafford, E. H. (2004). Defining Event Reconstruction of Digital Crime Scenes. *Journal of Forensic Sciences*, 49(6), 1291–1298.
- Chen, H., Chung, W., Xu, J. J., Wang, G., Qin, Y., & Chau, M. (2004). Crime Data Mining: A General Framework and some Examples. *Computer*, 37(4), 50–56.
- Ciardhuáin, S. O. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence*, 3(1), 1–22.
- Croft, N. J., & Olivier, M. S. (2010). Sequenced Release of Privacy-Accurate Information in a Forensic Investigation. *Digital Investigation*, 7(1-2), 95–101.
- Dehghantanha, A., & Franke, K. (2014). Privacy-Respecting Digital Investigation. *Proceedings of the 12th Annual International Conference on Privacy, Security and Trust (PST)*, 129-138.
- Garðnkel, S. L. (2010). Digital Forensics Research: The next 10 years. *Digital Investigation*, 7, S64–S73.
- Gupta, A. (2013). Privacy Preserving Efficient Digital Forensic Investigation Framework. *Proceedings of the Sixth International Conference on Contemporary Computing*, 387-392. doi:10.1109/IC3.2013.6612225
- Halboob, W., Abulaish, M., & Alghathbar, K. S. (2014). Quaternary Privacy-Levels Preservation in Computer Forensics Investigation Process. *Proceedings of the 6th International Conference for Internet Technology and Secured Transactions*, 777-782.
- Halboob, W., Mahmood, R., Abulaish, M., Abbas, H., & Saleem, K. (2015). Data Warehousing Based Computer Forensics Investigation Framework. *Proceedings of the 12th International Conference on Information Technology - New Generations (ITNG)*, 163-168.

- Hibshi, H., Vidas, T., & Cranor, L. (2011). Usability of Forensics Tools: A User Study. *Proceedings of the Sixth International Conference on IT Security Incident Management and IT Forensics*, 81–91. doi:10.1109/IMF.2011.19
- Hou, S., Uehara, T., & Yiu, S. (2011). Privacy Preserving Confidential Forensic Investigation for Shared or Remote Servers. *Proceedings of the 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 378-383.
- Ieong, R. S. C. (2006). FORZA – Digital Forensics Investigation Framework that Incorporates Legal Issues. *Digital Investigation*, 3, 29–36.
- Köhn, M., Olivier, M. S., & Eloff, J. H. P. (2006). Framework for a Digital Forensic Investigation. *Proceedings of the ISSA2006 from Insight to Foresight Conference*, 1-7.
- Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated Digital Forensic Process Model. *Computers & Security*, 38, 103–115. doi:10.1016/j.cose.2013.05.001
- Law, F. Y. W., Chan, P. P. F., Yiu, S. M., Chow, K. P., Kwan, M. Y. K., Tse, H. K. S., & Lai, P. K. Y. (2011). Protecting Digital Data Privacy in Computer Forensic Examination. *Proceedings of the Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 1–6. doi:10.1109/SADFE.2011.15
- Lee, H., Palmbach, T., & Miller, M. (2001). *Henry Lee's Crime Scene Handbook* (1st ed.). Academic Press.
- Mohay, G. (2005). Technical Challenges and Directions for Digital Forensics. *Proceedings of the First IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 155-161. doi:10.1109/SADFE.2005.24
- Palmer, G. (2001). *A Roadmap for Digital Forensic Research*. Tech. Rep. 1, Digital Forensic Research Workshop (DFRWS), Utica, NY.
- Parsonage, H. (2009). *Computer Forensics Case Assessment and Triage*. Nottinghamshire Police.
- Raghavan, S. (2013). Digital Forensic Research: Current State of the Art. *CSI Transactions on ICT*, 1(1), 91–114.
- Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, 1(3), 1–12.
- Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrot, S. (2006). Computer Forensics Field Triage Process Model. *Journal of Digital Forensics. Security and Law*, 1(2), 19–38.
- Seyyar, M. B., & Geradts, Z. J. M. H. (2020). Privacy impact assessment in large-scale digital forensic investigations. *Forensic Science International: Digital Investigation*, 33, 200906.
- Srinivasan, S. (2006). Security and Privacy in the Computer Forensics Context. *Proceedings of the International Conference on Communication Technology*, 1-3.
- Tran, N. H., Le-Khac, N. A., & Kechadi, M. T. (2020). Lightweight privacy-preserving data classification. *Computers & Security*, 97, 101835.
- Willassen, S. Y., & Mjøltnes, S. F. (2005). Digital Forensics Research. *Teletronikk*, 101(1), 92–97.
- Williams, J. (2012). ACPO Good Practice Guide for Digital Evidence. Metropolitan Police Service, Association of Chief Police Officers of England, Wales & Northern Ireland.
- Yasin, M., & Abulaish, M. (2013). DigLA – A Digsby Log Analysis Tool to Identify Forensic Artifacts. *Digital Investigation*, 9(3-4), 222–234. doi:10.1016/j.diin.2012.11.003
- Zhang, J., & Wang, L. (2009). Application of Case-Oriented Evidence Mining in Forensic Computing. *Proceedings of the International Conference on Multimedia Information Networking and Security*, 103-106.
- Zhang, S., Wang, G., Bhuiyan, Z. A., & Liu, Q. (2018). A Dual Privacy Preserving Scheme in Continuous Location-Based Services. *IEEE Internet of Things Journal*, 5(5), 4191–4200.

Muhammad Abulaish received PhD degree in Computer Science from Indian Institute of Technology (IIT) Delhi in 2007. He is currently an Associate Professor at the Department of Computer Science, South Asian University, Delhi. His research interests span over the areas of data analytics and mining, social computing, and data-driven cyber security and forensics. He is a senior member of the IEEE, ACM, and CSI. He has published over 100 research papers in reputed journals and conference proceedings.

Nur Al Hasan Haldar is currently a Ph.D. student at the School of Computer Science and Software Engineering, The University of Western Australia, Perth, WA. He is keenly interested in developing analytical frameworks using data mining techniques for varied applications, including social network analysis, cyber forensics, web surveillance, and biomedical informatics. His research interests are in the areas of social computing, data analytics, machine learning, graph modeling, and digital forensics.

Jahiruddin received the Ph.D. degree in computer science from Jamia Millia Islamia (A Central University), New Delhi, India, in 2012, where he is currently Associate Professor with the Department of Computer Science. He has published over 20 research papers in various journals and conference proceedings. His research interests include text mining, computational biology, and social network analysis.