Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

A Framework for Crime Detection and Diminution in Digital Forensics (CD3F)

Arpita Singh[1], Sanjay K. Singh[2], Nilu Singh[3] and Sandeep K. Nayak[4]
[1,2]Amity Institute of Information Technology, Amity University, Lucknow, India
[3]Department of Computer Science and Engineering,KoneruLakshmaiah Education Foundation
[4]Department of Computer Science & Application, Integral University, Lucknow, India
[*]Corresponding author: singharpita999@gmail.com

Article Info
Page Number: 531 - 552
Publication Issue:
Vol 71 No. 4 (2022)

Abstract
Cyber-attacks have become one of the world's most serious issues. Every day, they wreak serious financial harm to governments and people. As cyber-attacks become more common, so does cyber-crime. Identifying cyber-crime perpetrators and understanding attack tactics are critical in the battle against crime and criminals. Cyber-attack detection and prevention are difficult undertakings. Researchers have lately developed security models and made forecasts using artificial intelligence technologies to solve these concerns. In the literature, the authors explained numerous ways of predicting crime. They, on the other hand, have a problem forecasting cyber-crime and cyber-attack strategies. Here, in this paper author proposed a digital forensic investigation procedure that deals with cyber-crime. In this investigation, the process author explains digital forensics techniques for ensuring that digital evidence is located, collected, preserved, evaluated, and reported in such a way that the evidence's integrity is preserved. These sequential digital forensic stages affect a standard and accepted digital forensic investigation procedure, and each phase is influenced by sequential occurrences, with each event relying on tasks. Digital forensics investigation is a technique for ensuring that digital evidence is handled in such a way that the evidence's integrity is preserved. Sequential digital forensic stages affect a standard and accepted digital forensic investigation procedure, and each phase is influenced by sequential occurrences, with each event relying on tasks.

Article History
Article Received*: 25 March 2022*
Revised*: 30 April 2022*
Accepted*: 15 June 2022*
Publication*: 19 August 2022*

Keywords: - Cyber-crime, Digital forensics, digital evidence, Data analysis, Security and privacy, Cyber-attack.

Introduction

Information security has given users complete control over data by specifying who has access to it, who can govern it, and who may receive it [1]. People's lifestyles are changing as a result of technological advancements. For example, nowadays most people prefer online payment to traditional payment, access to social media, medical consultation through phone or video chat, online schooling, and so on. As technology advances and new services become available, the number of internet users grows, and an exponential increase in information causes its use, as well as misuse, resulting in cyber-attacks and cyber-crime. Cyber-attacks have an impact on the economic

systems of our countries. According to research by Mahindra SSG and ASSOCHAM, cybercrime costs India around 24,630 crores per year [2]. Attacks have become more complex as a result of technological advancements, and defending oneself is no longer as simple as installing anti-virus software.

The general concept of evidence preservation in the chain of custody has remained the same but the original process of investigation may vary.The preparation, examination, identification, collection, analysis, validation, acquisition, documentation, and forensic reporting of digital evidence in a court of law, is known as the digital forensics investigation process. The process of interpreting and imaging digital evidence from various electronic devices using scientifically sound and validated methodologies is an indestructible part of digital forensic investigation. Digital forensics is a rapidly growing field that uses a variety of analysis tools and computer investigative approaches to locate relevant legal evidence and hints [3].In general, digital forensics is a process that involves not only retrieving information about a reported incident but also properly processing that information so that experts can obtain all relevant clues and evidence, which can then be used to pursue your legal interests against someone or in any other situation. Finding evidence, keeping it, accurately documenting it, and presenting it in a court of law are all part of the digital forensic process. Although, because this is not a simple process, it might often take years to solve the issue. Furthermore, complex systems are making it harder to hit these days. We now have a complex methodology and enhanced technologies and techniques to determine if any pieces of evidenceare present or not. We now have a complicated methodology, as well as new technologies and techniques, to determine whether a criminal case has occurred and a huge amount of money isspent to solve the case [2].

Cyber-attacks and cyber-crimes are a serious worry for large countries such as the US and the UK, which have developed a number of security solutions to combat them[4]. Allcountries are seeking to secure and adapt to cyberspace security [5]. The security of critical infrastructure must be a top priority for countries [6]. In the year 2020, information taken from the Airbus Company's information system was sold on the dark web. Millions of people's medical information has been stolen, and several communities have declared a state of emergency as a result [7].With each passing day, the workforce grows insufficient in combating cyber-attacks, necessitating the search for new alternatives. Machine-learning approaches are being used by researchers to detect power outages caused by cyber-attacks [8] and to prevent the Internet of Things vulnerabilities [9]. Other applications include detecting spam and network attacks [10], detecting phishing attempts against banks [11], and increasing sexual crimes on social media [12] Stock prediction [13], risk mapping [14], and cyber profiling [15] are some of the sectors where these technologies have been used. Implementation areas include predicting crime trends and patterns [16], criminal identity detection [17], and crime prevention [18].

The authors suggest a framework called "Crime Detection and Diminution in Digital Forensics (CD3F)" in this study. The goal of this research article is to create a framework that connects the

stable and sequential aspects of the digital forensic investigation process. With the many operations of the investigation workflow comprising physical and investigative duties and judgments. The Digital forensic framework's intended role is to enable effective, focused, and fast risk identification and management. This CD3F framework contains and outlines eight major workflow stages, as well as the procedures and duties that each stage entails. The article is organized as follows:some of the current digital forensic investigation process models proposed by the researchers are elaborated on and discussed, followed by an explanation of why the digital forensic workflow should be mapped. The following section is about "Phases involved in proposed framework and explanation" and gives an overview of the framework, including all eight stages that the author proposes. "The suggested digital forensic guiding framework specifics" is the topic of the study's next session which focused on the CD3F framework workflow stages: forensic request, preparation, examination, identification, collection, analysis,acquisition, and forensic reporting. The discussion and critical evaluation of the proposed framework are covered in greater depth in the paper. The text is then concluded with some notes about the study's significance and the last half of this research article.

Literature Review

A description of all previously developed cyber forensics investigation frameworks that the authors investigated before developing the proposed framework is not possible due to space limits. Although some of the reviewed frameworks are described in this work, it should not be considered that the suggested model is based on them. In 2001 [19] authors proposed a framework where they have covered preparation, identification, permission, and communication were the four phases of the initial introduction model DFRWS. This paradigm was expanded into the SRDFIM framework, which includes additional steps such as scene securing, screening, scene documenting, evidence gathering, communication shielding, screening, preservation, analysis, and presentation [20].The FaaS Framework 2014 is based on the IDFPM framework [21], which begins with the collecting and authentication stages. Evidence acquired throughout the investigation will be stored in central storage, followed by the inspection phase in this suggested architecture. The analysisphase will be conducted with current analysistools, with the results being kept in a centralized database.

The DFRWS Investigation Model is used by the FBI. A fog IoT forensic framework (FOBI) is a network model that performs important operations such as data filtering and aggregation [22, 23]. Storage and processing resources are located at the network edge in this paradigm [24]. Fog protects data sent to IoT devices while also filtering traffic data. As a result, this architecture provides a number of benefits to IoT devices, including reduced network latency, faster and smarter responsiveness, more scalability, and greater security and privacy. Early detection of a cyber-threat or cyber-attack. It can be used to discover problematic IoT devices by including a fog layer in the framework [22] [25].Frameworks for research must also be adjusted as a result of technological advancements. As the author mentioned above, some frameworks are presented to combat crime using the most up-to-date technologies and techniques. With some rising issues, law agenesis is required for a framework that can combat crime and track down criminals' tracks. Cloud computing

is a new level of networking since it offers limitless processing capacity and storage, which poses security concerns [20].Cyber-attacks such as distributed denial of service (DDoS) attacks that deliver harmful packets [26] and phishing attempts that trick users on banking and shopping sites have increased dramatically. Furthermore, attackers are increasingly deploying malicious attack software (viruses, worms, trojans, spyware, and ransomware) that is installed on a user's computer without their knowledge or agreement [28]. Social engineering attacks are, once again, the most widespread of these attacks and one of the most difficult to counter. They are based on technical expertise, ingenuity, and persuasion, and are carried out by exploiting the victim's weakness. Kevin Mitnick, a well-known hacker who specializes in social engineering attacks, was able to break into most of the computers he targeted using this method [29].

This attack is mentioned as one of the main security vulnerabilities in the system by Breda, Barbosa, and Morais [30], regardless of how secure a technical system is. Similarly, assaults on IoT devices, which have expanded dramatically in recent years, have a significant impact on society. For security reasons, assaults and threats to the IoT structure should be understood [31]. As described in this paper, studies performed to analyze and combat cyber-attacks highlight the importance of crime prediction. Many jurisdictions' legal frameworks characterize the attacks listed above as banned criminal offenses. The task of combating crime and criminals is delegated to law enforcement agencies. Researchers provide numerous analysis and prediction approaches to the institutions undertaking the research. Many studies, for example, have used big data [32] and machine-learning [18] methods to analyze crimes. With artificial intelligence models, they have contributed to crime and crime-fighting institutions. Identifying the regions where crime can be perpetrated and the story behind it [33], predicting crime using spatial, temporal, and demographic data [34], and assessing crime using literacy, unemployment, and development index data [35] are just a few examples. A time series of crime data from San Francisco, Chicago, and Philadelphia was utilized to forecast crimes in the year’s ahead.K-nearest neighbors (KNN) and Naive Bayes (NB) classification models performed worse than Decision Tree (DT) [36]. Using the KNN and DTs, a crime prediction was made with an accuracy of 39 to 44 percent [38]. The location, kind, date, time, latitude, and longitude of crimes committed in the United States were used as input. The results of crime predictions using KNN Classification, Logistic Regression (LR), DTs, Random Forest (RF), Support Vector Machine (SVM), and Bayesian approaches showed that the KNN classification was the most accurate at 78.9% [37]. Thirty-nine distinct categories of crime statistics from San Francisco were used in the study. A model splitting crimes into two types, blue/white-collar crime and violent/non-violent crime, was built using Gradient Boosted Trees and SVMs. The categorization of blue-whitecollar offenses was done with great precision.

The study, however, did not produce significant results in terms of classifying violent and non-violent crimes [39]. The data was taken from a ten-year murder in Brazil. The RF approach was used to make 97 percent accurate predictions in order to examine the effect of non-Gaussian residuals and urban metrics on murders. Unemployment and ignorance were found to be significant factors in homicide in this study. The relevance of each factor in predicting the crime was also assessed [40]. Another study employed the type, timing, and location of crime data to predict crime

in certain Indian regions. It was decided to employ the KNN prediction algorithm. Robbery, gambling, accidents, violence, murder, and kidnapping crimes were predicted using this strategy.It was shown to be more successful than a previous study of a similar nature [41]. Using crime data obtained from social media networks, big data and machine-learning frameworks were created. Volunteered Geographic Information, web, and mobile crime reporting applications were used to collect the information. The NB algorithm was used to generate crime predictions from the collected data. The goal of these forecasts is to pinpoint the site of potential crimes so that they can be avoided [42].

The demographic and geographic data from past years' events were utilized to forecast terrorist attacks in India. Using artificial intelligence algorithms, this model predicted terrorist occurrences with a high degree of accuracy [43]. The data used to analyze cyber-crime was publicly available information from social media platforms such as Facebook and Twitter. The F-measure value, which is the degree of accuracy and precision, was used to compare the algorithms. The RF algorithm was shown to be the best fit in the circumstance, with an accuracy of 80%. Threats were identified automatically using a model that analyses cyber-crime [44]. Through the screening program, real-time crime data from the internet news was employed. The classification algorithms employed were SVM, Multinomial NB, and RF. The data was divided into two categories: criminal and non-criminal. The most essential aspect is that it now includes news analysis [45]. Machine-learning algorithms were used to classify data from cyber-crime incidents in India. The program, which was 99 percent accurate in predicting crimes, cut down on time spent on analysis and manual reporting [46]. Kaggle was utilized to obtain a universally compared intrusion detection dataset.
On the bases of the literature review, the authors observed and analyzed that cyber-attacks and crimes are vital to investigate since they inflict significant harm to persons and governments. The studies contributed significantly to the literature and, in particular, to the criminal investigation units. General crimes, cyber-crimes, and attacks are commonly employed as a dataset in these studies. The real dataset based on personal qualities is looked at to a lesser extent, and a framework for digital forensic inquiry is proposed as a result. Because of the importance of the fields investigated, the cyber-attack and perpetrator estimating approach is addressed.

Phases Involved in Proposed Framework andexplanation
Almost all major transactions are adopted by web applications. Their web environment is deployed by different purpose applications like we have different applications for social surfing, cloud storage, emails, online marketing, etc. With all these bundles of online applications, online frauds and online crimes are increasing swiftly [21]. Many online actions are punishable by a court of law. To justify any case or prove any complaint experts fetch data present in digital devices known as digital evidence. While the process of investigation, experts have to collect and analyze many devices and their data, which makes this process difficult. The process of investigation may vary from device to device and case to case. One process used for investigation in one case for one device may completely be different from other cases and another device. Hence it is really hard to

find a compatible investigation process for digital devices. Cloud storage and online disk, where users can store their data are generation problems during the investigation. Forensic devices are getting advanced day by day, but anti-forensics development has obstructed the path of digital forensic investigation [22].
The proposed framework is about crime detection and control. The primary goal of crime detection and diminution in digital forensics (CD3F) is to help the investigator explain how specific digital evidence is discovered on a device. Despite the existence of numerous frameworks in the current literature, the CD3F methods and nomenclature have yet to be properly standardized. Attempts to standardize computer investigative process frameworks in the past appear to have not been fully successful for a variety of reasons. The authors' main reason for failing is that they used their own vocabulary instead of seeking to discover the most common language that can be accepted universally by digital forensic investigators.The suggested model's first phase, "Forensic analysis," examines case reporting and determines whether a digital forensic investigation is required for the same. The "preparation" phase follows, which focuses on the initial preparation for the case by examining the required set of acts and getting a search warrant or other necessary authority. The "examination" phase follows, which focuses on searching for evidence at the crime scene or in a location where evidence might be found. The "identification" and "collection" phases were devoted to locating and gathering prospective evidence shards. The "analysis" phase focuses on reviewing and analyzing the acquired material in order to collect evidence that can aid in the "analysis" phase. The final phase is "forensic reporting," in which the investigator reports the evidence discovered throughout the investigation. The proposed digital forensic model has the following phases -

Forensic Request-This is the first stage of the digital forensic process when incidence is reported and higher authorities hand over the case to digital forensic experts. The forensic request phase of a digital investigation begins when an incident is detected by either internal events such as an intrusion detection system or external events such as a crime reported to the police. The occurrence must be confirmed or denied after it has been discovered and reported. However, once the incident is confirmed, the investigators must be notified so that the first response can begin. The digital forensic investigation may be of these two kinds-
Public digital forensic Investigation, in Public digital forensic investigation method government body, is responsible for the investigation of the registered case request. During this investigation of a criminal case, the investigator must have a sound knowledge of local city/town, state, country, and country laws related to the criminal case and all cyber-crime laws and all standard legal processes of investigation [23].
Private or Corporate digital forensic Investigation - Whereas private investigation deals with private lawyers and companies who look after legal issues and that particular company policy violation. In such an investigation, the investigation must take care of business and should not suffer and the investigator should minimal interrupt to company employees during the investigation. Investigators cannot seize the evidence, rather than seize it, they acquire memory images and allow the system to go back to work [23].

Preparation-The next phase is to get prepared with the tools and methods which will be used further for the process and if required train and build the forensic expert team for the investment. It is also suggested in this phase that if a search warrant or other documents are required try to obtain the initial level of this model. These documents will help in the further investigation process. Basically, in this phase investigator identify the incidence and calculate possible risk assessment. Investigators determine which software and what kind of hardware will require for investigation. He/ she will also try to define if any specific tool will be required for the investigation process to fetch information that will be further used as 'evidence.

Examination-In this phase of the investigation, the investigator will lock the crime scene's physical environment. The digital forensic expert will try to secure all correlated logs, data, and volatile evidence like laptops, mobile phones, andhardware and he/she will also ensure that condition of electronic devices won't get altered by any means.Investigators aim to examine and identify similar past investigations in this phase. If they find one, they study it and follow the footprint of that investigation, which can help them during the investigation from a secure physical location. Investigators also verify the extent of the damage/impact of the incident and ensure that non-digital evidence such as fingerprints is protected. Observe and document the physical scene, device positions, device locations relative to one another, and device conditions, including power status.

Identification & Collection- The next phase in this model explains about identification and collection of digital evidence after performing examinationof evidence around the crime scene. After the collection of evidence from the crime scene, an important and necessary step is to preserve all evidence so that they can utilize it further for examination (if required) and their integrity will remain constant. Detailed information regarding the evidence will be included into the evidence gathering form during this step. If electronic evidence is being used, a deeper inquiry into the device's volatile data will be required. If volatile data is needed, execute a live acquisition of volatile data first, then verify if non-volatile data is needed, and then perform a live acquisition of non-volatile data. Make a duplicate copy of the data you just got and double-check it. This phase will involve labelling the evidence discovered, as well as packing and transporting the evidence. The evidence is then placed in a legal custody room with labels and security measurements. Maintaining and preserving the chain of custody is essential.

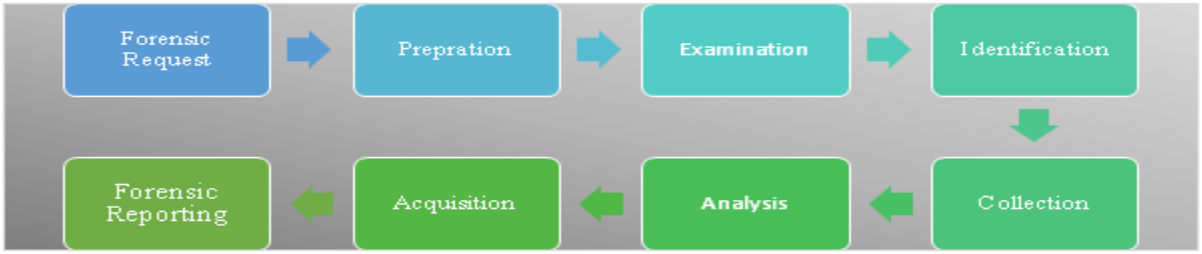

Fig 1 - The Proposed Digital Forensic Guidance Model

Analysis-This phase focuses on the process of examining digital evidence that has been discovered. During the analysis, the examiner assembled the evidence to gather information, and after reviewing the information, the examiner may develop certain conclusions for final reporting. During this phase, the investigator gathers unprocessed data and devices from the linked investigation and compares them to the condition of the device obtained through the related investigation. Investigator Extracts data from gathered devices using physical, logical, and dead acquisition methods.

Acquisition-This is a critical stage in the digital forensic investigation process. In this case, digital forensic professionals will attempt to gather all unprocessed data and devices from the investigation. After successfully collecting physical and logical data, he will make duplicate copies of all collected data so that the original data is not affected, and only the investigator will execute all operations and analyses on the copied data. During this phase, the investigator compares duplicate data to the original in terms of timestamp and reconstructs the data taken from devices. Only the investigator selects an analysis approach from a list of options, such as data hiding analysis, log analysis, timeframe analysis, application and file analysis, and so on. Finally, reconstructs the chronology of crimes in order to provide a clear picture and discover missing links in order to locate relevant evidence.

Forensic Reporting-This is the final phase of the digital forensic investigation framework, and it entails reporting and drawing conclusions from all previous phases, as well as all essential material. The conclusion will be drawn and reported to the court of law. This is the final phase of the CD3F architecture; investigators prepare a detailed report that can be understood by laypeople, choose the target audience, gather evidence, and maintain the chain of custody throughout this phase. Closer documents will be handed provided by the investigator, along with the time and date of release, as well as to whom and by whom they were released. This evidence will be presented in a court of law to assist in the resolution of the case.

There are primarily eight steps in the proposed digital forensic guiding model that describe the investigative process. This digital forensic investigation technique entails obtaining digital data for inspection in order to use the information discovered as evidence in reopened cases. The type and format of this digital record can vary. Smartphone data, a list of all phone calls made, desktop files, recorded video and audio files, a bit of signal strength from a mobile SIM station's base station, all electronic mail chats, installed and attacked virus, and so on [24]. Once investigators have obtained these records, the most important next step is to create copies of all evidence, which will then be examined and analyzed so that the integrity of the original evidence is not compromised and no issues are raised about its integrity.

The Proposed Digital Forensic Guidance Framework Details

This model is influenced by previous existing models as well as some physical forensic models so that model can encounter the challenges from the electronic evidence to make them admissible in a court of law. This framework has two major contributions. First, it describes a

framework that is trying to cover previous events and the state of electronic devices at the primitive and abstract level of investigation. Second, it provides detailed steps for each phase, so that it can use as a reference investigation framework. The following goals were used to define the model:

• The framework is designed based on the theoretical foundations of digital forensic investigation so that current and future work in digital forensics science can be used.

• The framework must be general with high opinion based on the technology being investigated so that this theory could be applied to upcoming as well as existing technologies.

• The framework must be adept at events, supporting systems, and storage locations at arbitrary levels of abstraction so that complex systems can be represented.

• The framework designed as per it is capable of describing past events and states so that all electronic evidence can be represented.

After obtaining a forensic request for a registered or reported case digital forensic investigation progress gets triggered. Here is the description of the phases of the proposed investigation model in brief.

Preparation Phase

The initial understanding of the problem, as well as the appropriate tools, are all part of the preparation phase. This step is used to get authorization and approval, as well as a search warrant and legal notification to people who have expressed concern, before developing a suitable plan. Here's a rundown of the steps involved in the planning phase.

1. Identify or detect incidence and possible risk assessment of the reported case.
2. Actuate Computer Emergency Response Team (CERT) divide preliminary assignment and maintain legal activity coordinated plan before arriving at the crime scene.
3. If required obtain a search warrant and permission from concerned authorities.
4. Formulate paperwork according to the requirement of the case and gather all needed requirements and identify requirements.
5. Develop an onsite plan which includes policies and individual responsibilities.
6. Select approach and strategy for collection, preservation, examination, and analysis of evidence.
7. Have any information about the suspected operation system.
8. Determine the kind of software and hardware for investigation. Specific tool, accumulate evidence collection, and packaging equipment and materials.
9. If more information does not require further processing. Then move to the next step of digital forensic investigation.

ExaminationPhase

The second phase focuses on protecting the crime scene from illegal entry and preventing contamination of the evidence. An early investigation by the investigators to assess the crime scene, identify potential sources of evidence, and devise a search strategy. This phase entails

photography, sketching, and crime-scene mapping, as well as the adequate recording of both physical and digital crime scenes. The brief of the examinationphase is as follows -

1. The most first step is to secure the crime scene's physical environment & secure all correlated logs, data, and volatile evidence. Laptops, hardware, and secure narrative description. Don't alter the condition of electronic devices.
2. Try to analyze and find similar previous investigations if find one thenstudy a similar investigation & follow the footprint of that investigation that can help during the investigation from the secure physical environment in step 1.
3. Place labels over all the drive slots and power connections and take preliminary photographs of the crime scene.
4. Select narration technique (written, audio or video) to delineate the search area and detect unauthorized activity and report it.
5. Validate the damage/ impact of incidence and ensure the protection of non-digital evidence like fingerprints.
6. Evaluate whether any movement appears in evidence, determine devices on the network and make a complete evolution sheet.
7. Observe & document the physical scene, the position of devices, the location of devices relative to each other, and the condition of devices including power status.
8. Take written notes on what appears on the screen, take snapshots of the screen, and the active program should videotape.
9. Take photographs before and after examination of evidence. Label properly each evidence.
10. Maintain and seize evidence log that includes a brief description and photographic log. Prepare a chain of evidence.
11. Start Identification & collection.

Start Identification & collection Phase

In the identification phase investigator needs to disable all other possible communication methods for the devices. Some communication technologies, such as WiFi or Bluetooth, may be enabled even if the device appears to be turned off. This may result in the overwriting of existing data, so such scenarios should be avoided. In evidence, both volatile and non-volatile evidence could be present. To preserve its integrity, the required precautions must be performed. A brief of the identification and collection is given below-

1. Firstly, check to be collected evidence are physical or electronic?
2. If evidence is physical then apply the tag on an Identified object as evidence like removable media, cables, publications, and all computers. Or if the evidence is electronic then check whether the device is running or not.
3. Fill evidence collection form with detailed information about the evidence.
4. If electronic evidence is running, then checking for volatile data of the device will require further investigation.

5. If volatile data is required, then perform live acquisition of volatile data then check non-volatile data is required then perform live acquisition of non-volatile data.
6. Check whether found device data is stable. If yes, then remove the power source whether battery or main switch. If no, then perform a normal system shutdown.
7. Decide the most appropriate way to acquire data and then acquire data from the device.
8. Make a duplicate copy of the acquired data and verify.
9. Check whether all required data has been acquired. If yes, then seize found device.
10. Record and return the connection of the device. Label the evidence found then pack and pack and transport the evidence.
11. Store the evidence in a legal custody room with labels and security measurements. Maintain and preserve the chain of custody.

Analysisand Acquisition

Examining the content of the acquired evidence and extracting information for presentation in court is what a forensics specialist does. This consists of both volatile and non-volatile data.The acquisitionis more of a technical evaluation undertaken by the investigation team based on the findings of the digital evidence inspection and the reconstruction of event data. The brief of this phase is given below-

1. Collect unprocessed data and devices from the related investigation.
1. Identify operating systems used in incidence & choose data extraction techniques for examination & analysis of evidence.
2. Check documents obtain by related investigation with the condition of the device.
3. Perform physical, logical extraction, and dead acquisition on data from collected devices.
4. Make duplicate copies of all acquired data from electronic devices.
5. Authenticate duplicate data with the original one in their timestamp
6. Reconstruct the extracted data from devices.
7. Choose the analysis technique - Data hiding analysis, log analysis, Timeframe analysis, Application & file analysis, etc.
8. Reconstruct the sequence of crimes to produce a clear picture & try identifying missing links
9. Compare acquired evidence with proven facts and with physical forensic results
10. Documentation & Preserve chain of custody in storage
11. Store evidence in a secure custody room.

Reporting & presentation

A report containing a full overview of the various procedures done during the investigation and the conclusion reached is presented to the proper authorities during the presentation phase. When a crime is committed, it is presented to a court of law, and when an event occurs, it is presented in court. At the conclusion of the investigation, an evaluation is conducted, and the results are

utilized to update or repair any shortcomings discovered during the inquiry. Brief of this phase is given below-

1. Write a comprehensive report which can understand by the layman as well
2. Determine the target audience and put together evidence and preserve the chain of custody.
3. Present evidence according to rules of law enforcement.
4. Preserve evidence for further requirements.
5. Handover closer Documents, with time & date of release, to whom & by whom released.

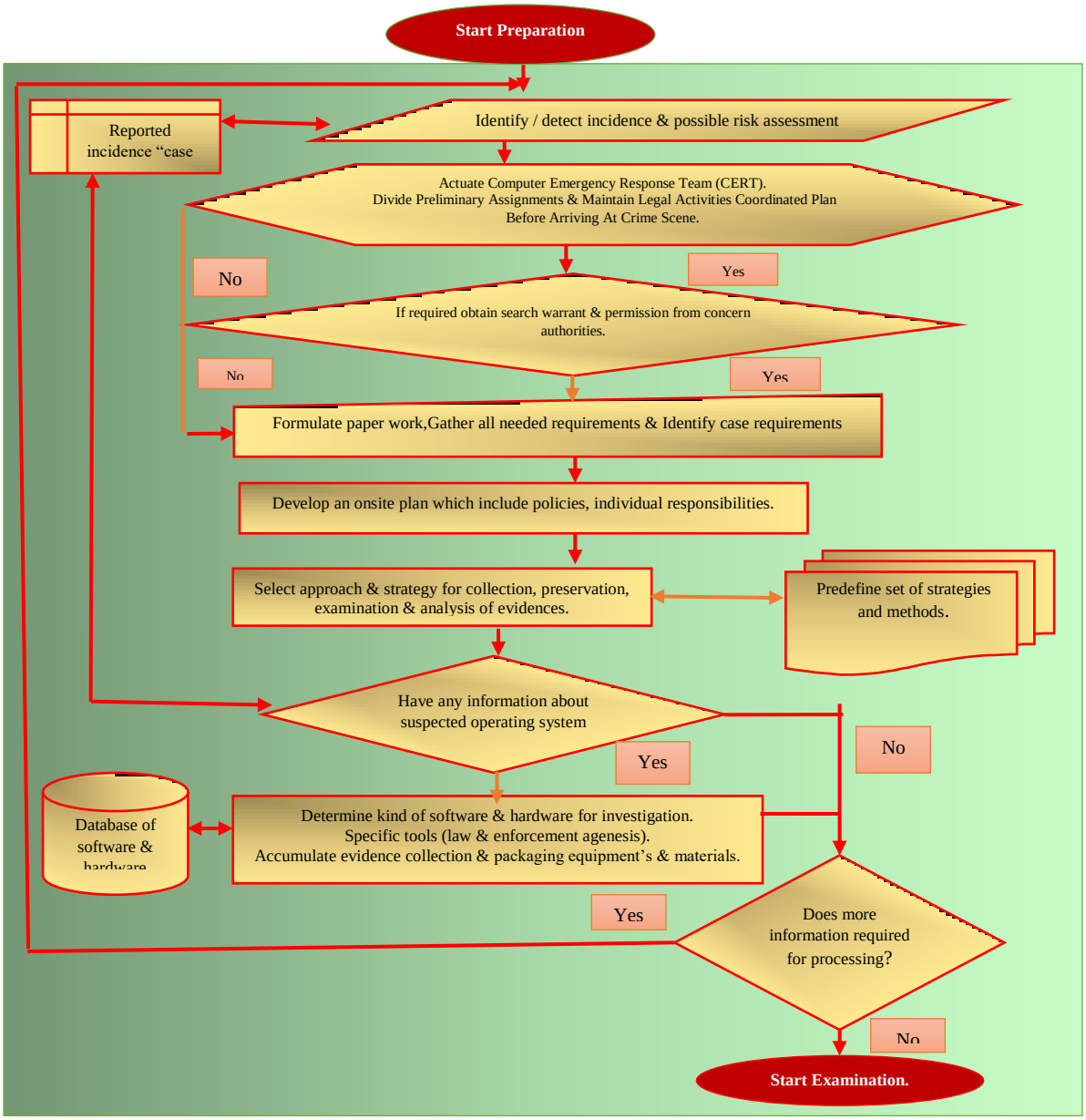

Fig2: Dataflow Diagram for Preparation Phase of digital Forensic Investigation Model

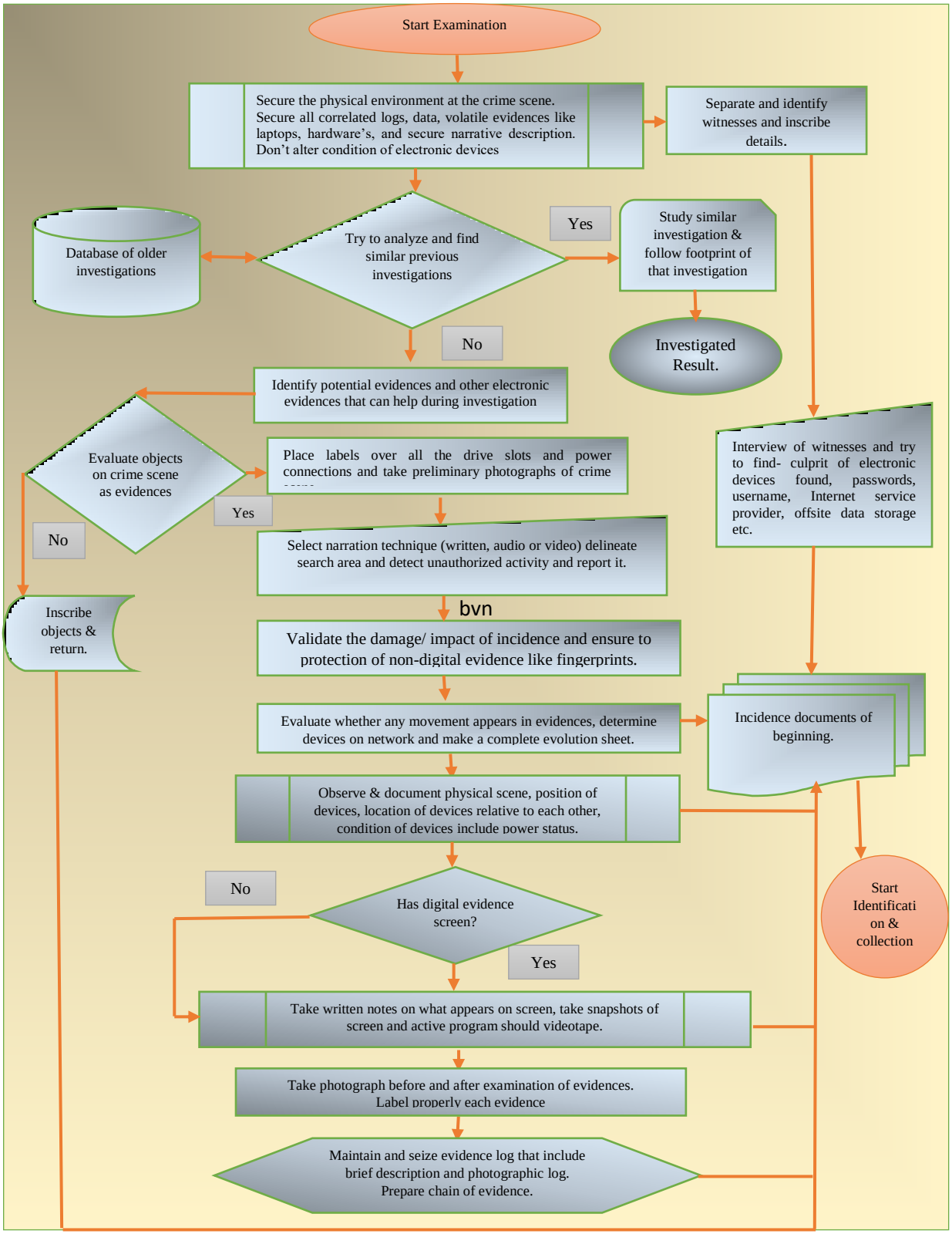

Fig 3: Dataflow Diagram for Examination Phase of digital Forensic Investigation Model

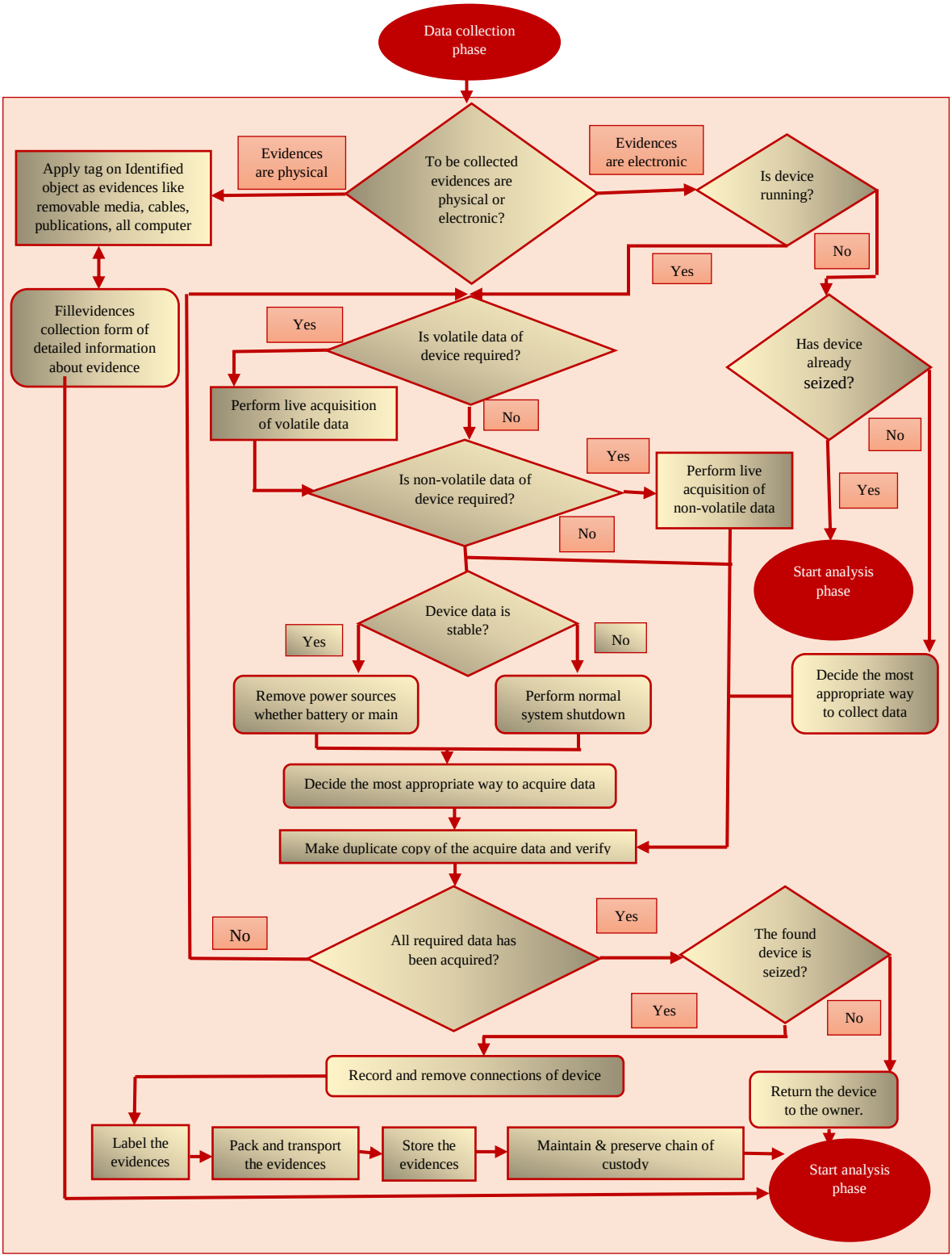

Fig 4: Dataflow Diagram for collection Phase of digital Forensic Investigation Model

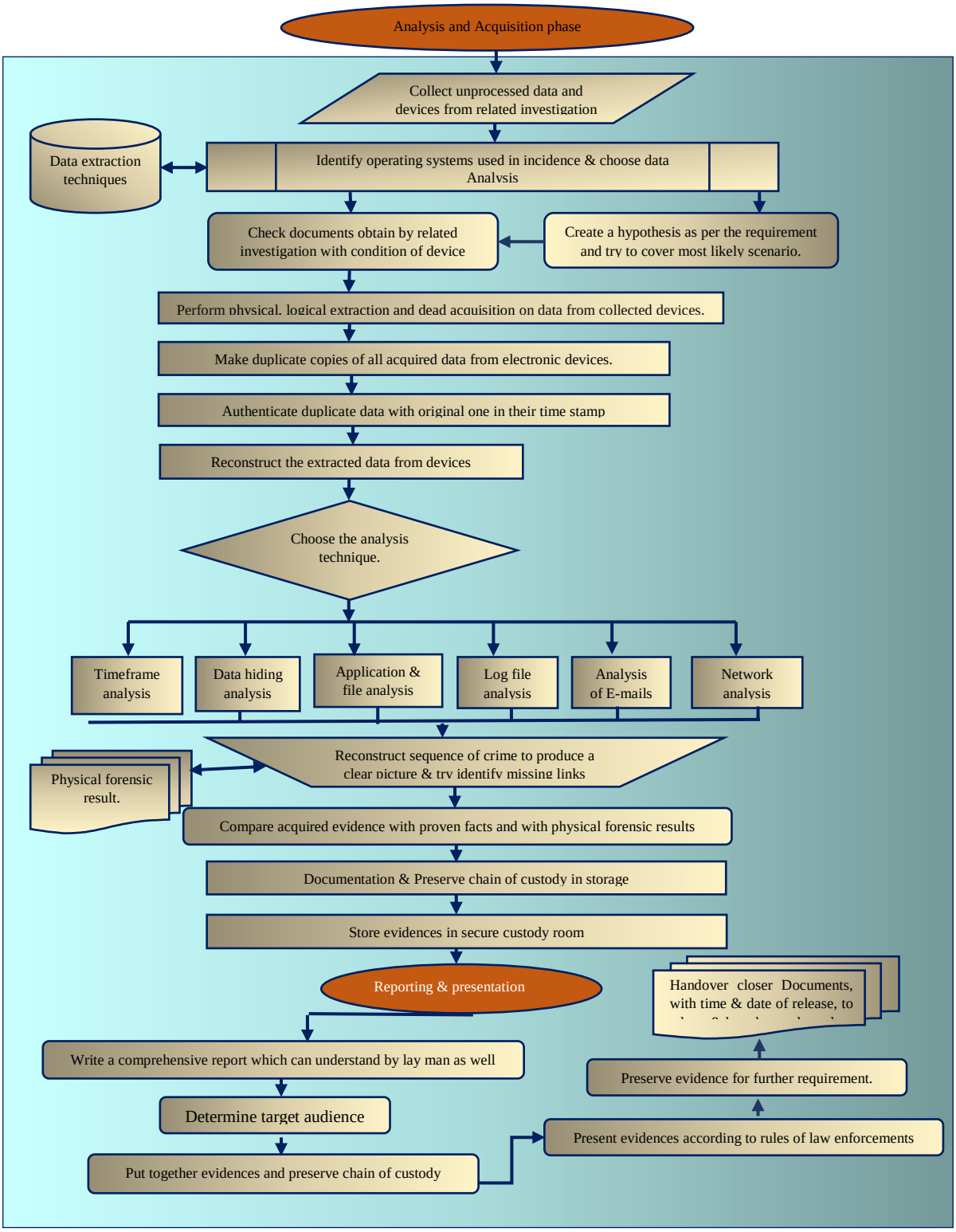

Fig 5: dataflow diagram for analysis, acquisition, reporting, and presentation phase of digital forensic investigation model

Discussion

Dimpe and Kogeda [47] examined the earlier proposed models and found the integrity of evidence can be preserved by documentation of each action performed during the investigation. To serve this purpose they proposed a generic investigation framework. This framework is focused on the integrity of evidence, while collecting evidence in the collection phase this phase will be divided into sub-phases – acquisition, transport, and storage. The author claimed that they explained requirements during the digital forensic investigation to make investigation work easy and explained standers. But setting investigation standards cannot solve all problems and challenges faced by investigation officers.Dimpe and Kogeda analyze the need for documentation for the integrity of evidence, but their main focus was on standardizing phases of investigation and developing skills for the investigator. But even we have national and international courses and training systems for professionals. If through documentation only the investigator can save the integrity of evidence, then we will not be facing any of such problems yet. Hence, we proposed standards and an easy framework by analyzing the earlier proposed one that accommodates everything which could be considered and followed in the investigation process.

Bulbul, Yavuzcan, and Ozel suggested a model named "Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM)" which focused on procedures of crime scenes [48]. This multi-stage model tries to offer a series of evidence collection procedures and multiple tasks for the crime scene to support the investigation process. This proposed model is having some new suggested tasks like Crime scene examination, Evidence search, Potential evidence acquisition, System assurance, managerial activities Hypothesis and validation,Physical management of evidence, and System, Organization of potential evidence [48]. This model was a basic workflow without any validation and verification. The model was designed to help organize and individual investigators, but this was a very complex puzzled workflow and this model was incapable to focus on all electronic devices and all electronic pieces of evidence with needed to be collected during the investigation.

Ohaeri and Esiefarienhe proposed a digital forensic model for network security management and information system. In this model digital forensic investigation stages were implemented as a security mechanism. The basic thought behind this model was to provide a detailed knowledge of the digital forensic technology practices in institutions, organizations, or companies [49]. The model is claimed to ensure uniqueness and effectiveness while succeeding to provide adequate, reliable, and effective security. But this model is not successfully achieving its goal of real-time dealing with the investigation. It is just like a traditional search method for investigation. According to the author data integrity is justified while keeping the laws and rules of digital evidence but the model seems to fail in proper documentation of evidence. This can be raised finger on the integrity of evidence.

Graeme Horsman proposed DERDS framework to support the digital forensic investigation. This model serves with logical decisions and the investigator those are experienced but lack

confidence. This guidance model is a process flow for making the right judgment with the help of found digital evidence. The DERDS framework delivers 3 corridors- inferences, assumptions, or conclusions, for an investigator to test and search for the consistency of digital investigative [50]. But this model capacity is depending on the ability of the investigator or researcher. DERDS framework always needs a doorkeeper for proceeding further in the investigation and for key decisions during the investigation process.

Author suggested a digital forensic investigation framework in our proposal, hoping to provide an optimistic method to researching cyber-attacks. This structure is mostly made up of four-fold. First, it aids in the digital forensic investigation model's preparation phase. Second, is the digital forensic inquiry model's examinationstep. The digital forensic investigation model's third phase, is collection. The fourth phase of the digital forensic investigation process is the examination, acquisition, reporting, and presentation. We proposed a simple and standard methodology that includes accurate documentation at each stage and attempts to cover all parts of the investigation.

Critical evaluation of proposed framework

The proposed framework is based on holistic approach which is able to focus and combine all aspects of digital forensic investigation. The processes provided in the proposed framework is vital in investigation and provides more advantages. The proposed framework tries to cover all aspect of investigation process and all predefined frameworks processes which shows that this framework is enough comprehensive to cover whole aspects of investigation. One of the important benefit of the proposed framework is fetching out potential evidence forensically for improve admissibility in a court of law. Table 1 is showing a comparison of the CD3F framework with some pre-existing framework

TABLE 1. Comparison of the proposed framework from pre-existing frameworks

	Framework	**Year**	**Contribution**	**Loophole**	**Comparison from the proposed framework**
[1]	Systematic Digital forensic Investigation Model [29]	2011	Model work for dynamic evidence & reconstruct events.	The process is similar to old process like only the terms used are different.	Proposed framework provide a less complex investigation path way to the investigator as well as compatible with the advance technology.
[2]	Integrated Digital Investigation Process Model[30]	2011	Identifies the need for interaction with resources in right way.	Proposed Interaction tool needs proper training & patience.	Proposed framework can be used in any digital forensic investigation with only basic training of investigator.
[3]	Generic Digital forensic Framework[25]	2013	Set standard requirement for digital forensic investigation.	Explained standard does not satisfy promise.	Framework explains set of slandered required in each phase.
[4]	An analytical crime scene Proceeding Model (ACSPM)[26]	2018	Talk about management of digital evidence & crime scene investigation	Only focused on crime scene procedure.	Proposed framework is focused on every aspect of investigation like crime scene investigation, evidence collection, analysis, lab examination etc.

[5]	Digital Evidence Reporting and Decision Support (DERDS) framework[27]	2019	Guidance model for the investigator, when to report findings to minimize unsafe disclosure of evidence	Not 100% error-free& may not agree to report all evidence so that evidence may get lost.	Clearly report all evidence so that it requires reinvestigation, evidence recall is unbiased.

Significance of Study

The framework highlighted certain phase commonalities that may be regrouped to make the framework more logical. For example, Survey and Recognition could be part of Preparation, Documenting the Crime Scene could be part of Securing the Crime Scene, and Communication Shielding could be part of Securing the Crime Scene because these two independent phases in this model are actually part of Securing the Crime Scene. It's also possible to mix examination with analysis. These phrases were employed as different activities in the model, although their definitions are not just comparable, they also complement one other, which can lead to confusion if they are separated.The following are some advantages of the proposed framework.

- In the proposed framework, a standardized process is used. This makes higher chances of extracting the potential evidence during the investigation.
- The proposed framework is based on a holistic approach and the framework is also able to incorporate the existing frameworks, and thereby this framework could be used as a harmonized model during IoT environment investigation.
- Throughout the whole process of the proposed framework integrity of collected potential evidenceispreserved.
- The proposed framework provides a less complex investigation pathway to the investigator as well as is compatible with advanced technology.
- From a reinvestigation point of view, all useful information and all extracted evidence preserve digitally.

In the proposed framework, all processes can be executed continuously and also insuring the evidence admissibility in a court of law. The authors have involved the concurrent processes in the proposed framework as per guided in ISO/IEC 27043: 2015 standards. A comparison with existing models by the table is also been done in this paper which will further bring out the efficiency of the proposed framework.

Conclusion

The author provided a framework for digital forensics in this study. As technology advances, so does the number of incidences of cybercrime. Over previous models, the suggested framework's level of comprehensive processes for each phase independently offers unique benefits. This is a framework that consists of steps that the investigator must follow during the investigation. It is a generic/universal framework that is not dependent on technology or limited to a set of tools. As a result, it will not be constrained by current technologies. The suggested framework is

technology-neutral, it may be used in a variety of research platforms and scenarios. This framework could also be utilized in a variety of digital forensics cases. This study will help the different stack holders to detect the crime at a very early stage (as explained in the examination phase, step 2) by following the old recorder investigation footprint. This detection at an early stage can reduce the detection time of the crime and hence can reduce the further process time in the digital forensics investigation.

References

[1] Mousa, M. Karabatak and T. Mustafa, "Database Security Threats and Challenges," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116436.

[2] The Hindu business (17 January 2018), India lagging in cyber security awareness. Available at : [https://www.thehindubusinessline.com/info-tech/india-lagging-in-cyber-security-awareness/article9046626.ece] access on – 2 June 2021

[3] P. Čisar and SanjaMaravićČisar, "Methodological frameworks of digital forensics," 2011 IEEE 9th International Symposium on Intelligent Systems and Informatics, 2011, pp. 343-347, doi: 10.1109/SISY.2011.6034350.

[4] Goel S. 2020. National cyber security strategy and the emergence of strong digital borders. Connections: The Quarterly Journal 19(1):73–86 DOI 10.11610/Connections.19.1.07.

[5] Reid R, Van Niekerk J. 2014. From information security to cyber security cultures—information security for South Africa. Piscataway: IEEE, 1–7.

[6] CISA. 2020. Critical infrastructure sectors. Available at https://www.cisa.gov/critical-infrastructuresectors (access on April 11, 2022)

[7] Check Point Security Report. 2020. Check point research. Available at https://research.checkpoint. com/

[8] Wang D, Wang X, Zhang Y, Jin L. 2019. Detection of power grid disturbances and cyber-attacks based on machine learning. Journal of Information Security and Applications 46(27):42–52 DOI 10.1016/j.jisa.2019.02.008.

[9] Zolanvari M, Teixeira MA, Gupta L, Khan KM, Jain R. 2019. Machine learning-based network vulnerability analysis of industrial Internet of Things. IEEE Internet of Things Journal 6(4):6822–6834 DOI 10.1109/JIOT.2019.2912022.

[10] Canbek G, Sagiroglu Ş, Temizel TT. 2018. New techniques in profiling big datasets for machine learning with a concise review of android mobile malware datasets. In: 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT). 117–121.

[11] Moorthy RS, Pabitha P. 2020. Optimal detection of phising attack using SCA based K-NN. Procedia Computer Science 171(5):1716–1725 DOI 10.1016/j.procs.2020.04.184.

[12] Ngejane CH, Mabuza-Hocquet G, Eloff JH, Lefophane S. 2018. Mitigating online sexual grooming cybercrime on social media using machine learning: a desktop survey. In: 2018

International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD). Piscataway: IEEE, 1–6.

[13] Gurjar M, Naik P, Mujumdar G, Vaidya T. 2018. Stock market prediction using ANN. International Research Journal of Engineering and Technology 5:2758–2761.

[14] Wheeler AP, Steenbeek W. 2020. Mapping the risk terrain for crime using machine learning. Epub ahead of print 24 April 2020. Journal of Quantitative Criminology DOI 10.1007/s10940-020-09457-7.

[15] Zulfadhilah M, Prayudi Y, Riadi I. 2016. Cyber profiling using log analysis and k-means clustering. International Journal of Advanced Computer Science and Applications 7(7):430–435 DOI 10.14569/IJACSA.2016.070759.

[16] Biswas AA, Basak S. 2019. Forecasting the trends and pattems of crime in Bangladesh using machine learning model. In: 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT). Piscataway: IEEE, 114–118.

[17] Bharathi ST, Indrani B, Prabakar MA. 2017. A supervised learning approach for criminal identification using similarity measures and K-Medoids clustering. In: ICICICT. Piscataway: IEEE, 646–653.

[18] Lin YL, Chen TY, Yu LC. 2017. Using machine learning to assist crime prevention. In: 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI). Piscataway: IEEE, 1029–1030.

[19] M. Reith, C. Carr, and G. Gunsch, “An examination of digital forensic models” international journal of digital evidence, 2002.

[20] S. A. Ali, S. Memon, and F. Sahito, “Challenges and solutions in cloud forensics” in Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing. ACM, 2018, pp. 6–10

[21] S. Raghavan, “Digital forensic research: current state of the art”,‖ CSI Transactions on ICT, vol. 1, no. 1, pp. 91–114, 2013.

[22] Al-Masri, E., Bai, Y., & Li, J. (2018). “A Fog-Based Digital Forensics Investigation Framework for IoT Systems”. 2018 IEEE International Conference on Smart Cloud (SmartCloud). doi:10.1109/smartcloud.2018.00040

[23] Bonomi, F., Milito, R., Zhu, J. and Addepalli, S., 2012, August. Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing (pp.13-16). ACM.

[24] Islam, M. J., Mahin, M., Khatun, A., Debnath, B. C., &Kabir, S. (2019). Digital Forensic Investigation Framework for Internet of Things (IoT): A Comprehensive Approach. 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT). doi:10.1109/icasert.2019.8934707

[25] Luan, T.H., Gao, L., Li, Z., Xiang, Y., Wei, G. and Sun, L., 2015. Fog computing: Focusing on mobile users at the edge. arXiv preprint arXiv:1502.01815.

[26] Kaur Chahal J, Bhandari A, Behal S. 2019. Distributed Denial of service attacks: a threat or challenge. New Review of Information Networking 24(1):31–103 DOI 10.1080/13614576.2019.1611468.

[27] Sahingoz OK, Buber E, Demir O, Diri B. 2019. Machine learning based phishing detection from URLs. Expert Systems with Applications 117(4):345–357 DOI 10.1016/j.eswa.2018.09.029.

[28] Biju JM, Gopal N, Prakash AJ. 2019. Cyber attacks and its different types. International Research Journal of Engineering and Technology 6(3):4849–4852

[29] Mitnick KD, Simon WL. 2009. The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers. Hoboken: John Wiley & Sons

[30] Breda F, Barbosa H, Morais T. 2017. Social engineering and cyber security. International Technology, Education and Development Conference 3(3):106–108

[31] Kagita MK, Thilakarathne N, Gadekallu TR, Maddikunta PKR, Singh S. 2020. A review on cyber crimes on the Internet of Things. arXiv. Available at http://arxiv.org/abs/2009.05708

[32] Rewari S, Singh W. 2017. Systematic review of crime data analytics. In: International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). Piscataway: IEEE, 3042–3045

[33] Hassan M, Rahman MZ. 2017. Crime news analysis: location and story detection. In: 20th International Conference of Computer and Information Technology (ICCIT). Piscataway: IEEE, 1–6

[34] Zhao X, Tang J. 2017. Exploring transfer learning for crime prediction. In: IEEE International Conference on Data Mining Workshops (ICDMW). Piscataway: IEEE, 1158–1159

[35] Vineeth KRS, Pandey A, Pradhan T. 2016. A novel approach for intelligent crime pattern discovery and prediction. In: International Conference on Advanced Communication Control and Computing Technologies (ICACCCT). Piscataway: IEEE, 531–538.

[36] Feng M, Zheng J, Han Y, Ren J, Liu Q. 2018. Big data analytics and mining for crime data analysis, visualization and prediction. In: International Conference on Brain Inspired Cognitive Systems. Cham: Springer, 605–614.

[37] Bharati A, Sarvanaguru RAK. 2018. Crime prediction and analysis using machine learning. International Research Journal of Engineering and Technology 5(9):1037–1042

[38] Kim S, Joshi P, Kalsi PS, Taheri P. 2018. Crime analysis through machine learning. In: 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). Piscataway: IEEE, 415–420.

[39] Chandrasekar A, Raj AS, Kumar P. 2015. Crime prediction and classification in San Francisco City. Available at http://http://cs229.stanford.edu/proj2015/228_report.pdf.

[40] Alves LGA, Ribeiro HV, Rodrigues FA. 2018. Crime prediction through urban metrics and statistical learning. Physica A: Statistical Mechanics and its Applications 505:435–443 DOI 10.1016/j.physa.2018.03.084.

[41] Kumar A, Verma A, Shinde G, Sukhdeve Y, Lal N. 2020. Crime prediction using K-nearest neighboring algorithm. In: 2020 International Conference on Emerging Trends in Information Technology and Engineering. Piscataway: IEEE, 1–4.

[42] Jang-Jaccard J, Nepal S. 2014. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences 80(5):973–993 DOI 10.1016/j.jcss.2014.02.005.

[43] Verma D, Yarlagadda R, Gartner SS, Felmlee D. 2019. Understanding patterns of terrorism in india (2007–2017) using artificial intelligence machine learning. International Journal of Technology, Knowledge, and Society 15(4):23–39 DOI 10.18848/1832-3669/CGP/v15i04/23-39

[44] Arora T, Sharma M, Khatri SK. 2019. Detection of cyber crime on social media using random forest algorithm. In: 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC). Piscataway: IEEE, 47–51

[45] Ghankutkar S, Sarkar N, Gajbhiye P, Yadav S, Kalbande D, Bakereywala N. 2019. Modelling machine learning for analysing crime news. In: 2019 International Conference on Advances in Computing, Communication and Control (ICAC3). 1–5

[46] Ch R, Gadekallu TR, Abidi MH, Al-Ahmari A. 2020. Computational system to classify cyber crime offenses using machine learning. Sustainability 12(10):4087 DOI 10.3390/su12104087.

[47] P. M. Dimpe and O. P. Kogeda, "Generic Digital Forensic Requirements," 2018 Open Innovations Conference (OI), 2018, pp. 240-245, doi: 10.1109/OI.2018.8535924.

[48] Bulbul, H.I., Yavuzcan, H.G., and Ozel,M., Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM), Forensic Science International, Volume 233, Issues 1–3, (2013) Pages 244-256, ISSN 0379-0738, doi:10.1016/j.forsciint.2013.09.007.

[49] I. U. Ohaeri and B. M. Esiefarienhe, "Digital Forensic Process Model for Information System and Network Security Management," 2018 International Conference on Computational Science and Computational Intelligence (CSCI), 2018, pp. 65-70, doi: 10.1109/CSCI46756.2018.00020.

[50] HorsmanG. ,Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework, Digital Investigation, Volume 28, (2019), Pages 146-151, ISSN 1742-2876, doi. :10.1016/j.diin.2019.01.007.