NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 9, ISSUE 4, Apr. -2022

AN APPROCH FOR MANAGEMENT OF DIGITAL CRIME SCENE

Atul B. Patil
Associate-Risk Advisory/Digital Forensic,
Nangia Andersen LLP, Bangalore, India
* patilatul19.1991@gmail.com

ABSTRACT

For every law enforcement agency investigator, cyber forensic professional's and investigators facing a challenge of Digital Crime Scene. In day-to-day life, the accused person or victim person may use high technology to ease their respective jobs. So, both persons can have the different intentions for using the technology. Accused person may be aware about technology used but the victim person might be unaware about the technology used such as digital payment options called digital wallet, different mobile application looking a very attractive or the application used for remote connection. Digital wallet is one of simplest example of cash transactions and the purpose may be commit a crime either intentionally or unintentionally. This kind of crimes are executed with secure locations with different digital medias such as hard drives, pen drives, hidden cameras, server's, skimmers etc. So, to investigate this kind of crime such as data leaks from server, laptop, computers, corporate digital medias the investigator or concerned authority should raid the location along with Digital Forensic Expert, search and seizure warrant or permission letters. So, the objective of this paper is to explain the requirements and summarize the guidance for law enforcement agencies or corporate entity about management of digital crime scene- procedures, roles for investigator and cyber forensic expert, documentation required on digital crime scene. This article is very useful to the students looking career in Digital forensics, law enforcement agencies and corporate digital forensic service provider.

Keywords: Digital Crime Scene Management, Digital Forensics, Crime Scene, Digital Forensic Expert.

INTRODUCTION

Digital Forensic is a challenging part in now days to the investigators, professionals, investigator agencies who is facing crime scene given by victims or culprits. So, everyone should need to handle crime scene very carefully. Digital forensics is the process to get the evidence by processing the digitally stored data. The Fig.1 shows the digital forensics phases [1] need to execute.

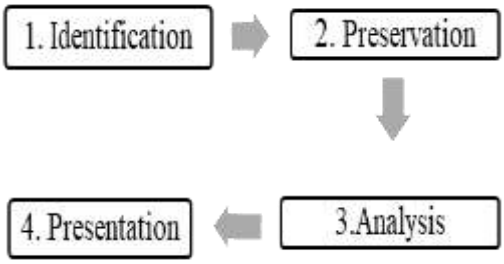

Figure 1: Phases of Digital Forensics Process

Digital forensic is process executing in phase wise manner such as identification, preservation, analysis, and presentation.

These phases are illustrating with following process:

1. **Identification:** This phase work is related to identification of digital storage media relates to any crime scene or in any crime which may contains several information either official or personal.

2. **Preparation:** This phase relates to the preparation for the identified place of scene, digital storage media with the required amount of power, digital forensic equipment's, search and seizure warrants, requisition letters for the cyber forensic experts and cyber forensic kit.
3. **Preservation:** This phase work is related with the preservation of data from digital media. After processing phase of preparation for scene or the suitable media, it should be important to prepare the things for data preparation by making necessary arrangements and decisions by the investigators and digital forensic expert. So, the data should preserve by acquisition of digital media in forensically sound manner by preserving the integrity of the source digital media.
4. **Analysis: -** After the data preservation phase the acquired data image can be used for forensic processing of data. So, the recovered and restructured data by forensic software can used for analysis.
5. **Presentation: -** This phase work is executed after analysis of the data. In this phase the actual evidence could be present in terms of report or power point presentations to the concerned authority.

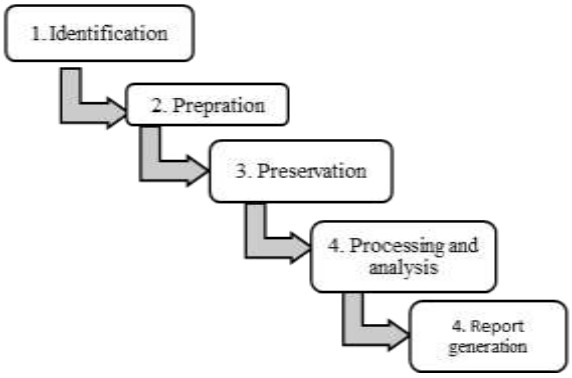

Figure 2: Digital Forensics Process

The Fig.2 represents the phases of digital forensic process.
Following images in the Fig.3, Fig.4 and Fig.5 are the few types of digital storage media available to market used for data storage, reproduce and communication. The available media is with different shape and size. Fig.3 is the new eras computer and old computer systems available with different shape and size, fits at suitable locations.

Figure 3: Computers New vs Old

Figure 4: Different Data Storage Media's

Fig.4. are the different available types of storage media such as hard disks, pen drive, dongle, SSD disk, compact disc, digital versatile disc, and floppy disc. Every storage media is available with more storage space and compact shape.

Figure 5: Micro Video Recorder and Sound Recorder

The author [2] summarised the different branches of digital forensics which can be in picture at any time and any crime scene locations. Following are the branches of digital forensics:

- **Computer Forensics: -** Computer Forensics [3] is the branch of digital forensics in which process followed for identification of the digital storage media tools relates to computer, laptop, servers. Then the data is preserved by acquisition of data in forensic image followed to analysis and reporting of the evidence.

- **Mobile Forensics: -** Mobile Forensics [4] is the branch of digital forensics in which the devices used for communication need to identify and extract the data in forensically sound manner. The extraction could be an any type like logical extraction, physical extraction, file system extraction, android backup extraction, apk downgrade extractions etc.

- **Network Forensics: -** Network Forensics [5] is most important to look for cyber security and the investigation after the any random incident which cause damaged to the any personal data or organization data. This branch works completely about the analysis of network logs, IP address and other required data relates to network or communication over the internet.

- **e-Discovery Forensics: -** e-Discovery Forensics [6] is nothing but the processing of electronically stored information over the cloud, email analysis, internet history. The author describes the best practice for the e-Discovery forensics process execution steps.

- **Social Media Forensics: -** Social Media Forensics [7] is about to collect evidence over the social networking platform, and other websites used for the content uploading such as Facebook, Twitter, Instagram, and LinkedIn. The author summarised the procedures for the social media forensics to collect evidence which might be helpful for the legal proceedings.

- **Drone Forensics: -** Drone Forensics [8] is the new branch of digital forensics where the drone is used as unmanned arial vehicle used for an investigation or used may be for different purpose such as medical and parcel delivery. This unmanned arial vehicle is with SD cards, internal storage, Flight Control System, Sensors, controller, cameras, batteries, paddles, and motors.

- **Audio/Video Forensics: -** Audio/ Video Forensics [9] is the branch of digital forensics relates to identification of the speaker from tape of conversation and its authentication based on its different parameter such as frequency, critical listening, spec to graphic analysis.

LITERATURE REVIEW

Nowadays world comes together stays together with the help of internet. Many of the daily routine work is ease down by the internet and new technology with compact storage media. It is not required to access the personal information or official information by physically digital storage media, it could be access over the internet accessing through the remote desktop application, through the malicious applications. This information can be further used for commitment of any crimes, suspicious transactions, threatening to someone, any activity cause any loss personally or officially. The blog [10] explains very briefly that cyber-crime increased by the remote application desktop software, raising the level of connectivity, raising the level of connectivity so that risk of attach is rising rapidly. Also, there are many organizations with more vulnerability exist to for cyber-attack due to the relaxed control environment, revised process and changing the work profiles. The author [11] explains the typical methodology used for cyber-crime such as remote access of the any digital device, social engineering, email or website phishing, unauthorized access to personal information through malware/open ports in network, ransomwares.

A. Importance of Digital Crime Scene Management

To prevent the cyber-attacks on personal digital media, all business houses, corporate organizations it is necessary to take preventive actions that evidence should not be executed. It is chance for data breach, personal or organizational financial loss. If there will be any incident took place, it is necessary to carry out the digital forensic process to understand the details route cause of incident so everyone aware about the incident with loop false if any existing in organizational IT infrastructure. It is important step to identify the culprits or unintentional victims for any cyber attach or involvement of any cybercrime.

Digital crime scene management is important to maintain the integrity of digital evidence after identification of the digital media on the crime scene. It is very helpful to maintain and preservation of all document

processes of the crime scene by analysing the background of the case, eyewitnesses, facts along with the digital storage media. Digital evidence acts 1872 does not contain the direct relevance for the digital storage media evidence, so preserving the evidence should be done according to the Indian Information Technology ACT 2000 with predefined set of procedures and rules. Any kind of digital forensic crime scene can educate the investigator and digital forensic experts or the person who connected with the case, because each case is different, and its investigation method is also different.

B. Digital Forensic Principle

The work done by investigator, digital forensic expert for digital forensic process execution is very crucial as the new technology is being always challenging. The digital evidence should be handled very carefully if we miss out on something with new technologies procedures, it might possible that there will be alteration of data or deletion of data with the new timestamps. In [12], the following are the basic principles explained which investigator and digital forensic expert should follow:

1. All the basic general procedures should be followed when the investigator and digital forensic expert should work with the digital media for extraction of evidence.
2. The digital evidence should not be altered or modify during the seizing of digital media.
3. Use the faraday bags and evidence bags to secure the digital evidence damaged by externally by any force, water or remote access by mobile phone, computers, or any accessible digital evidence. All the communication devices should put on airplane mode.
4. Whenever it is necessary to access the original evidence, it should be done by a trained cyber forensic expert only using the necessary write blockers so that evidence cannot be tempered.
5. All the activity of handling of the digital evidence for seizure, access storage or transfer of the digital evidence must be fully documented with all timestamp details of handling and preserved. It should be available for review.
6. A person is responsible for all activities carried out for digital evidence extraction while it is in custody of the respective responsible person.
7. Any agencies, who is responsible for search, seizure, accessing, storing, or transferring of digital media should comply with the above principles.

C. Indian Eviddence Act 1872 for an electronic device

The Indian Evidence Act 1872 was introduce and passed by Imperial Legislative Council in India during the British empire ruling. It contains the set of rules and procedures which governing the admissibility of evidence in the Indian courts of law. Since Imperial Legislative Council passed Indian Evidence Act in 1872, it is retained ass in original format except a certain amendment made time to time.

The section 65(B) of Indian Evidence Act 1872 describes a particular framework that governs the admissibility of an electronic evidence. Accordance with the legal framework for electronic evidence under 65(A) of an Indian Evidence Act, the content of an electronic records needs to prove as evidence accordance with the requirements mentioned in section 65(B). Later chapter will explain the complete requirements and information of 65(B) certificate and Chain of custody. These documents required compulsory for the admissibility of evidence to the court.

D. Exploring the available international guidelines:

Following are the few standard guidelines defined for law enforcement and information technology security perspective only to conduct the digital forensic process on the crime scene as well as in the forensic lab.

The NIST [13], presents some guidelines from an information technology view to help the organization for security incident investigation and preventive action against it by performing digital forensics guidelines along with the preparations.

The Interpol [14], gives some standard guidelines given for law enforcement seize a different kinds of digital evidence Digital forensic process either crime scene or forensic lab.

The guidelines given by the U.S Department of Justice [15] for digital crime scene with different steps need to carry out by the cyber forensic expert such as planning, preparations in accordance with received leads for crime scene and digital storage media by the authorized person. A forensic expert should be adjusting the crime scene in accordance with the conditions, available equipment, warrant and experience because each scene of the crime has different scenarios and conditions.

The author [16] represents a model of crime scenes investigation. This paper summarized the different available guidelines for crime scenes issued by a different organization or published in journals. The author presents the digital crime scene models with detailed phases information dedicatedly.

The ISO/IEC 27037:2012 [17] is standards guideline for information technology-security techniques that gives a guideline for the identification, collection, acquisition, and preservation of digital forensic evidence. It is a Standard organization accepted worldwide.

All investigators and cyber forensic experts should complete all processes required documentation of the crime scene along with photography adhere to Indian Law. So, there is no chance to the culprit for benefit of the doubt from the court.

Approach for Management of Digital Crime Scene

A. Importance of Digital Crime Scene Management

To prevent from the cyber-attacks, all business house, corporate organization, government organization everyone realized that it is necessary to prevent cyber data breaches on their valuable information assets. It is also required and important to carry out a forensic analysis of suspected attacks on their information and ensure that the criminals are identified to take the necessary preventive actions.

Digital crime scene management is important to maintain the integrity of digital evidence. It is very helpful to maintain and preservative of all document processes of the crime scene by analysing the facts, eyewitnesses, backgrounds of the case along with the digital storage devices. Indian Evidence Act 1872 does not contain the direct relevance for the digital storage media and the evidence found from it, so preserving the evidence should be done according to the Indian IT act 2000 predefined set of procedures and rules [18].

B. Information Technology Act 2000, in India

According to the Information Technology Act 2000 of Indian law, a cyber-crime is an any illegal activity to access or target the any digital media or any digital storage device with compromise the security of the system or data processed by any device used. The major amendments are done by year 2008 and introduce the Intermediary Guidelines Rules 2011 and Information Technology -Intermediary Guidelines and Digital Media Ethics Code Rules 2021 introduce by Government of India. In [19] few offences explained as per law and amendments made in Information Technology Act 2000 as given below:

1. Alteration of data from the original source of the computer.
2. Accessing the any digital media using unauthorised way.
3. Obscene information publication in electronic format.
4. Direction of controller to a subscriber to extend facilities to decrypt the information.
5. Accessing the protected system unauthorised way.
6. Penalty for falsification.

7. Violation of data privacy and confidentiality.
8. Publication of false digital signature certificate.
9. Any information published for counterfeit purpose.
10. Act to apply for offence or contravention committed outside India.
11. Tampering the evidence or removal.
12. Penalties or confiscation not to interfere with other penalties

Table 1 having the summary of the important sections in Information Technology Act 2000 given in below table:

Table 1: Important Section in Information Technology Act 2000

Sr. No.	Sections	Offences
1.	65	Tampering with the computer source document or information
2.	66	Hacking the digital media by using any digital media such as Computer or laptops
3.	66B	Receiving Stolen computer or any communication device
4.	66C	Use of the credential of another person's or organization
5.	66D	Cheating using computer resources.
6.	66E	Publishing the Obscene images or private images and Contents of others
7.	66F	Act of Cyberterrorism
8.	67	Publishing Information which is obscene in electronic form
9.	67A	Publishing images containing sexual acts
10.	67B	Publishing Child porn or predating children online
11.	67C	Failure to maintain the records
12.	68	Failure or refusal to comply with orders
13.	69	Failure or refusal to decrypt data
14.	70	Securing access or attempting to secure access to protected systems
15.	71	Misrepresentation
16.	72	Breach of confidentiality and privacy
17.	72A	Disclosure of information in breach of lawful contract
18.	73	Publishing false electronic signature certificate particulars
19.	74	Publication for fraudulent purpose
20.	75	Act to apply for offence or contravention committed outside India
21.	76	Confiscation
22.	77	Compensation, penalties, or confiscation not to interfere with other punishment.
23.	77A	Compounding of offences
24.	77B	Offences with three years' imprisonment to be bailable
25.	78	Power to investigate offences.

The preservation of cybercrime evidence helps us to improve our IT infrastructure by identification of loopholes, also it should help for preventing future cyber-attacks. Any kind of digital forensic crime scene can educate the investigator and cyber forensic experts or the person who connected with the case, because each case is different, and its investigation method is also different. The following components would help establish Cyber Crime Management:

- Identification of Incident and the approach to response it.
- Interpretation and analysis of logs.
- Establishing 'evidence' relations in the network.
- Training and awareness for updating the skill set for minimize the impact of cyber-attacks on information assets.
- Investigation of reported Cyber Frauds and Cyber Crimes.

- Cyber Forensic Lifecycle – Development and implementation of policies and processes.

So, with the given components and mentioned basic principle in literature survey needs to execute on the crime scene. To complete a successful crime scene the forensics tools, play an important role for maintain the integrity of the evidence. Open-source and commercial tools are available for digital forensics. The next chapter describes the digital forensic tool. The flow chart for digital crime scene management is given in figure no Fig- 6.

C. Digital Forensic Tools

The website [20] contains collective information about the Digital forensic tools with different filters such as type of license, type of forensic work. This website contains information such as URL of websites for different digital forensic tools, whether the tool is commercial or open source. This information is available for digital forensic and its branches such as computer forensic, mobile forensics, network forensics cryptocurrency analysis and other tools.

In [21,22] the author summarized the important digital forensic tools and its available features. The digital forensic tool is mainly used for retrieving the evidence to have protection and care against identity theft, money laundering, preserving privacy, protection against black mailing, threatening, prevention from sexual harassment and many other cybercrimes.

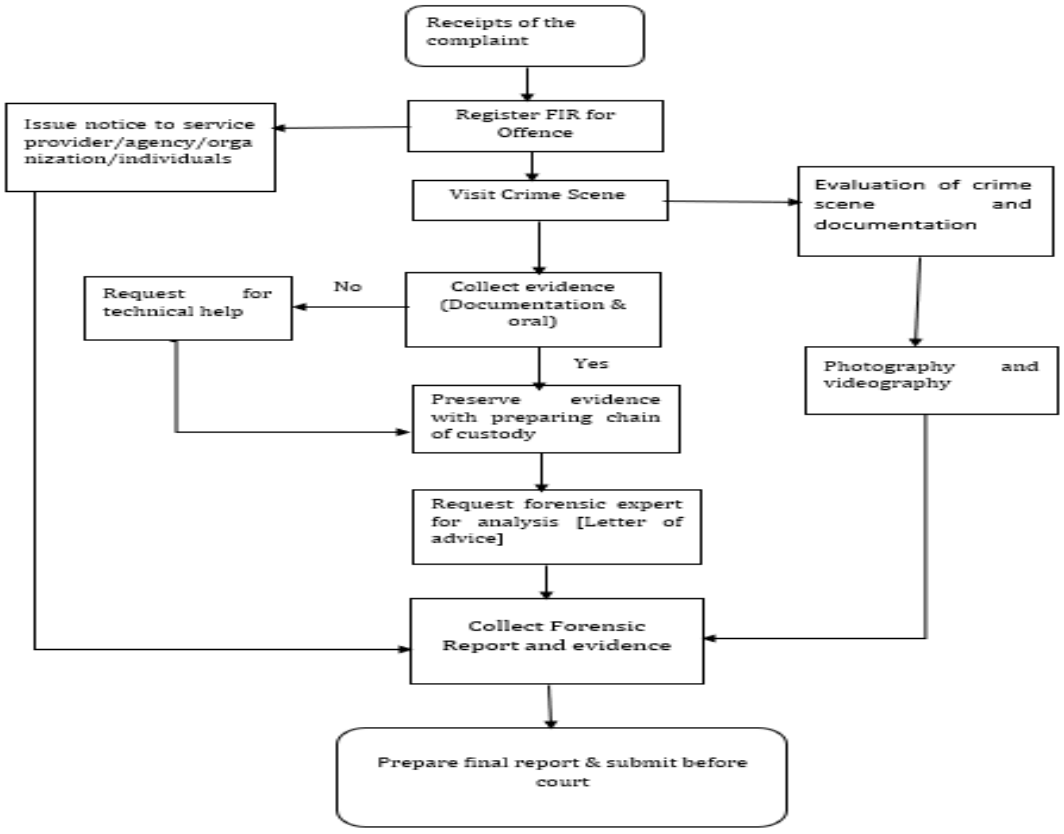

Figure 6: Flow Chart Digital Crime Scene Management

Following are the few important digital forensic tool used in Digital Forensic Investigation:

1. **EnCase Forensics:** - EnCase forensic [23] solutions by Open Text Company used for computer forensics. It's user friendly having powerful features to triage, collect process the data and provide deleted data, email analysis, internet artifacts analysis. Now in latest versions of v22 it supports for cloud accounts data acquisition such as Gmail, google drive etc.

2. **Access Data FTK Toolkit: -** FTK toolkit [24] is one of the powerful tools used for the analysis of hard disk data, mobile data, e-discovery with inbuilt features of data indexing. This tool is owned by now Exterro Company.

3. **Magnet Axiom: -** Magnet Axiom [25] tool used for hard disk data analysis, mobile data analysis, cloud data analysis. It's a powerful feature of carving and cryptocurrency analysis features.

4. **UFED4PC:** The tool UFED4PC is a product of company Cellebrite [26] used for mobile data extraction and analysis with features of Image carving, location carving, access to cloud data with valid tokens. The company has other different products used for digital forensics like Mac OS devices called as Cellebrite Digital Collector.

5. **Oxygen Detective: -** Oxygen Forensic Detective [27] is an all-in-one forensic tool built to extract, decode, and analyze data from multiple digital sources. it can also find and extract different artifacts, system files as well as credentials from Windows, macOS, and Linux machines.

6. **SANS Investigation Forensic Toolkit (SIFT): -** SIFT [28] was developed by an international team of experts which is widely used as an open-source. It is discovered as an incident response workstation and later made available publicly.

Following table 2 is the list of available tools used for Digital Forensics Commercials and open source.

Table 2: Popular Forensic Tools

Sr. No	Name of Tool	CT/OT
1.	Encase Forensics	CT
2.	Access Data FTK	CT
3.	Magnet Axiom	CT
4.	Intella Professional	CT
5.	Nuix	CT
6.	OS Forensics	CT
7.	Atola Forensics	CT
8.	Belka soft X	CT
9.	X-Ways Forensics	CT
10.	Detago Forensic Platform	CT
11.	Blackbag Backlight	CT
12.	UFED4PC	CT
13.	Oxygen Detective	CT
14.	XRY Forensics	CT
15.	Mobiledit	CT
16.	MD-RED	CT
17.	Paraben E3:DS	CT
18	Mobilyze Tool	
19.	PC3000	CT
20.	DVR Examiner	CT
21.	Video Investigation Portable	CT
22.	X1 Social Discovery	CT
23.	Page Vault Browser	CT
24.	Directory Lister	CT
25.	AMPED V	CT

Sr. No	Name of Tool	CT/OT
26.	Autopsy	OT
27.	SIFT	OT
28.	Sluth Kit	OT
29.	CAINE	OT
30.	PALADIN	OT
31.	Xplico	OT
32.	Digital Forensic Framework	OT
33.	RegRipper	OT
34.	Kali Linux OS	OT
35.	Deft Zero	OT
36.	Network Miner	OT
37.	Network Mapper	OT
38.	Forensic Acquisition of Website	OT
39.	Volatility	OT
40.	BulkExtractor	OT
41.	WireShark	OT
42.	Encrypted Disk Detector	OT
43.	Linux DD	OT
44.	GuyImager	OT
45.	DumpZilla	OT
46.	FTK Imager	Free Use
47.	Encase Imager	Free Use
48.	Cuckoo Sandbox	OT/CT
49.	Cyber Triage	OT

The Sr no mentioned from 1 to 11 used for computer forensics and few of them for analyzing the mobiles data too. Also, Sr. No. 11 to 17 used for mobile forensics and 18 to 49 are a miscellaneous tools used for live storage media analysis, computer, and mobile forensic analysis.

The forensic tools such as FTK Imager, Encase Imager used for software digital forensic imaging tools and Tableau Duplicator TD2u, Logicube Falcon, Ditto tools, SOlO5 are the few hardware tools used as acquisition tool for digital storage media. The miscellaneous tools available for digital forensics such as Wireshark, network miner, hash calc, Exif Tools are used to extract the metadata of the files.

During any investigation or any digital forensic process execution whatever the evidence is retrieved by the investigator or Digital Forensic Expert, that evidence should be submitted before the court with necessary procedures and rules of Indian Evidence Act 1872 and the written certificate of 65(B) which is certified by the device owner or any responsible person for the complete IT infrastructure of the Digital Forensic Expert who processed the data to retrieve the evidence. In [29], the admissibility of electronic evidence to the court is explained in detail and approaching steps to the electronic evidence along with the rule and section mentioned in Information Technology Act 2000.

Another important document for digital forensic crime scene is chain of custody, which needs to submit to the court. The chain of custody indicates about the responsible persons who handles the evidence during the Digital Crime Scene duration for particulars of the procedures. This document is also most important Digital Forensic Expert who mentions the complete procedures to be followed by him or her during the digital crime scene. This document is representing the state of evidence during the handling of the evidence and investigation of the case.

D. Management of Digital Crime Scene

The environment place where the possibly digital evidence can be retrieved in the form of digital storage media such as hard disk, pen drive, memory card, mobile phone and any other digital media called Digital Crime Scene. In other words, we can also be summarized as any location where the digital storage media is used or identified as the device used for any illegal activity access of information or process of information. This location is anything like home, office, shop, serious criminal offense location such as murder, cloud storage. The next section Contains a complete information about the Chain of custody (COC) and 65(B) certificate required for digital crime scene and what information should requires including in it.

E. Chain of Custody (COC)

The Chain of Custody [30,31] one of important document for presenting evidence and report before courts. It is very important to remove out the any doubts which may indication of evidence tampering during the digital crime scene evidence handling by the any responsible person for the case. Following are the major factors that needs to inclusive in Chain of Custody (COC):

1. Save the date and time entering to crime scene.
2. Record the description of the evidence handed over to you along with date and time with the purpose of receiving it.
3. Save the date and time that original evidence handed over by you to the investigator in charge of crime scene for seal its safe custody.
4. Make the entry for each original evidence.
5. Mention the bit-by-bit clone date and time as start time and end time with the date.
6. Make the photography of the original evidence.
7. Perform the verification of clone image hard disk and mention the calculate and verified hash value to confirm bit by bit data clone is complete without fail.

8. Take the sample screenshots of the digital images.
9. Make an entry for all data processing of digital evidence from forensic Images.

The following is the best practice for digital forensic crime scene aspects. Every investigator and digital forensic expert should follow as given below:

1. Never work with original evidence.
2. Use the new clean media for a forensic process such as hard disk or pen drive.
3. Document any extra scope of information which very useful relates to case.

The Chain of Custody (COC) contains the following information without fails:

1. Mention the information of reporting agency or law enforcement agency.
2. Mention the case submission number or case identification number,
3. Mention the IPC sections or CrPC section under which case is register.
4. Date and time of Chain of Custody preparation.
5. Include the identity and signatures of the Digital Forensic Expert.
6. Include the identity and signature of investigator.
7. Include separately the list of submitted items for examination of digital storage media along with information such as serial number, make, model number, capacity of storage device.
8. Mention the finalization part as reports and evidence handed over to investigators along with date and time.

After the Chain of Custody (COC) next important document is the form 65(B) certificate. This certificate should sign by the person who is extracting the device data and processing for extraction of evidence for hand over to the investigation agencies for primary investigation or cyber forensic expert who is going to produce the report or the device owner.

F. 65 (B) Certificate

It is a certificate of information contains the details of the data reproducing as evidence steps and digital devices handled by the responsible person during the certain period. This information contains electronic record that is printed on paper, stored in digital storage media, or copied to optical or magnetic media produced by computer or laptop.

The digital storage media shall be admissible to any proceedings without proof or production of the original, that means any digital storage media used for producing the evidence should be mentioned in the certificate along with the status or condition of that device, period of the use of device, details of the storage media used for any annexures or any facts that which can state into report that should be a piece of direct evidence and it would be directly admissible to court [32]. 65(B) certificates shall be considered as document if the certain conditions mentioned below are fulfil.

a) The annexure or any information as evidence produced by the computer during the analysis of case where the digital storage media such as computer or laptops was regularly used to store the processed information for an activity carried out of digital forensics by any responsible individual person having control over that computer or laptop or any digital storage media.
b) The any information in form of an electronic records derived was regularly stored into digital storage media during the said period of case analysis activities of digital storage media.
c) The any information reproduced during the said period of case analysis using any digital storage media such as computer or laptop operated and working properly.
d) If that system not working properly then it is also required to mentioned that the said case analysis duration the system is not operated or working properly.

e) These non-working or non-operational of digital media such as laptop or computer does not effect on accuracy of evidence fed into digital media as annexure.

The certificate should contain the following things of statements:

1) The statement should be mentioned in such way that it was produced by identifying the electronic record having the statement of actual evidence.
2) The particulars of information of any device involved for producing the electronic record showing that it was produced through any digital media such as computer or laptop.
3) Detail information of evidence contain the information of digital media such as make, model, serial number, the capacity of storage media, notation marked for it.
4) Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

G. Role of Cyber Forensic Expert and Investigators

The investigator role is as follows:

1. As the complaint received by the complainant, the investigator should do the pre-investigation assessment.
2. Based on the complaint register the FIR with the respective offenses.
3. Secure the scene of crime by conducting a raid or identifying the location so nobody can enter within premises, and nobody can try to tamper the evidence.
4. If there is a requirement for help from the forensic expert, ask them for help with sufficient information required them to conducting a forensic procedure.
5. On need basis issue the notice to other organizations or the premises outside jurisdictions for preserving the evidence.
6. Collect the primary analysis report from them for further investigation and ask them for the final report based on interrogation of victims, persons relate with the case.
7. Once a final report is received by the cyber forensic expert, complete the investigation, and present all evidence in courts.

Fig 7 is the flow chart illustrate complete role of cyber forensic experts. The next part is a summary and guidelines for a cyber forensic expert.

The Cyber forensic expert's role should be following:

1. Seek a request letter for digital forensic help on the crime scenes from the respective agencies.
2. Check that sufficient information is received or not by respective agencies for conducting digital forensic service.
3. Acquire/extract the digital evidence in forensic image format so the integrity should maintain.
4. Check and verify the forensic image for bad sectors present if any and hash value useful for the integrity of evidence.
5. Check completely digital evidence either the sufficient information is present or not.

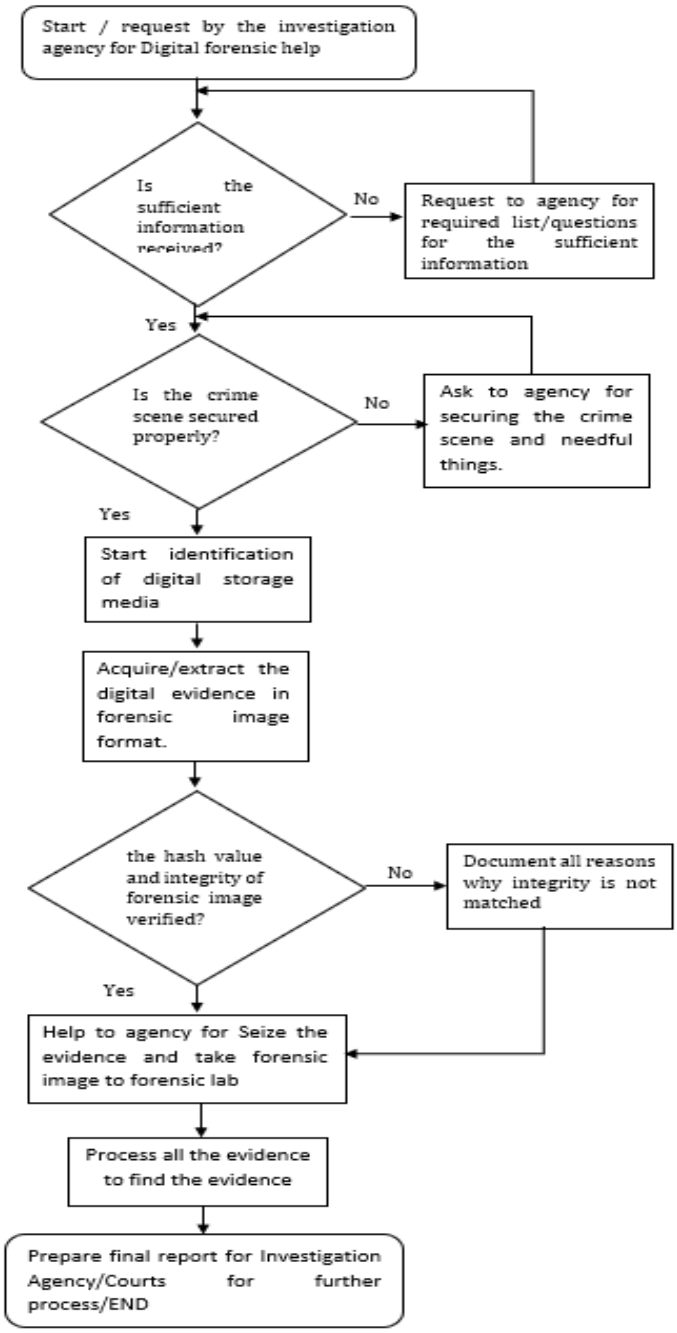

Figure 7: Role of Cyber Forensic Expert

6. Conduct an interview or handover the specific set of questions required for the investigation to the investigator.
7. Help investigator to seize the device by taken care of digital storage device that cannot be accessed by anyone over the internet or should not be physically damaged.
8. Report to the investigator if any other information is required to conducting digital forensic help such as passwords, background information of the device owner.
9. Document all events such as entering time to the scene of crime, handing over the digital evidence to the cyber forensic expert for the digital forensic process, handing over the evidence back to the investigator for seizure/safe custody and if possible, do the photography.
10. Take all the forensic images to the lab and process all data identify the conclusive evidence and artifacts and handover the evidence annexure to the investigator with detail reports.

11. At any point or any crime scene, the cyber forensic expert can adjust this practice based on the situation, request by the investigator, condition and any other circumstances which can be affected the crime scene.

H. Cyber Forensic Crime Scene Kit

1. A requisition letter or request letter from the competent authority asking for assistance or attend the Digital Crime Scene.
2. Case paper entry forms, Chain of custody forms and 65(B) certificate form should be required to enter the necessary details.
3. Blank hard disk of sufficient capacities, Compact Disc and Digital Versatile Disc needed to collect the digital evidence.
4. Screwdriver toolkit is required.
5. Hard Disk acquisition hardware and software tools.
6. Mobile acquisition hardware and software tools.
7. Cloud data acquisition tools.
8. Hard disk, mobile and cloud data analysis along with data extraction tools.
9. The forensic triage tools to analysis and exporting the preliminary reports with basic artifacts or information.
10. Print papers, printers, and packaging materials such as tapes, labels, cardboard boxes, faraday bags and bubble wrappers are required packaging and transport.

I. Challenges in Digital Crime Scene Managements

There will be lots of challenges facing by the investigator as well as a cyber forensic expert on the digital crime scenes. Few challenges are listed down as below:

1. **Presence of non-essential persons:** At crime scene location number of nonessential persons are present Sometimes it may be police officer even it is scene completely stabilized and unfortunately lead is leaked to common people or media, so it is very hectic for police persons to stop them to enter the nearby crime scene locations.

2. **Encryption of data: -** Nowadays encryption of digital storage media, the encrypted device is a major challenge to cyber forensic experts and investigators. Without a decryption key, we cannot decrypt the file data should not be in a readable format.

3. **Passwords: -** If the digital storage media is password locked then it takes a lot of time for decoding the password and enter a system. Nowadays a tool like Atola Forensics, password recovery software is available to crack passwords, but it takes a lot of time to check the different combinations of password attacks such as brute force attack, dictionary attack etc.

4. **Password protected mobile device**s: It is also the biggest challenge as the security levels and patch of the mobile device are improved. Also, the device is protected by the type of face lock, fingerprint lock, passcode, password, and pattern lock. The forensic tools such as Cellebrite UFED4PC, Oxygen Detective, XRY Forensics are also sometimes failed due to security patch to crack down the passwords.

5. **Ransomware Encrypted Files: -** It is the biggest challenge to everyone and mostly the popular and financially good organizations to secure their IT infrastructure. Nobody can enter their system illegally

or the intruder cannot attack by sending a malicious file or code. Their systems must be isolated with the trigger mechanisms that system infected by a malware attacks or ransomware attacks.

6. **High Speed and Volume of data: -** It is a challenge for everyone to process the huge amount of data for the identification of conclusive evidence. Nowadays data storage capacity is increasing so the time is also increased to process the data and for this, a good capacity with high configuration hardware is required for it.

7. **Complexity of data: -** The data could not be store at single locations, where the leads could be retrieved in such a way that data might be retrieved by virtual machines, cloud storage.

8. **Standard formats of artifacts: -** As the technology evolving daily, the research community tries to agree with the standard format and schema of digital artifacts.

CONCLUSION

This paper represents the best simple step for the digital forensic process carried out by cyber forensic experts and guidelines to investigators what exactly they require to do so. In Indian law, there will not be a specific guideline on how to conduct digital crime scenes but with the certain requirements of evidence against few rules need to follow certain steps as discussed above. So that the evidence should be admissible to respective investigation agencies/courts. Lots of challenges are they're for digital forensic process and this paper summarized to get the best process to retrieve the evidence and it is admissible to courts. Every crime scene is different in different aspects with the case and new technologies and needs to learn it.

REFERENCES

1) Roman, R.F.M., Mora, N.M.L., Vicuña, J.P.N. and Orozco, J.P., 2016. Digital forensics tools. International Journal of Applied Engineering Research, 11(19), pp.9754-9762.
2) Dasaka, M.S., 2019. A SYNOPSIS ON DIGITAL FORENSICS AND ITS INVESTIGATIVE STRATEGIES. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 8(2).
3) Villar-Vega, H.F., Perez-Lopez, L.F. and Moreno-Sanchez, J., 2019, December. Computer forensic analysis protocols review focused on digital evidence recovery in hard disks devices. In Journal of Physics: Conference Series (Vol. 1418, No. 1, p. 012008). IOP Publishing.
4) Sundar, K., Min Kyung, A. and Bing, Z., 2019. Smartphone Forensic Challenges.
5) Pilli, E.S., Joshi, R.C. and Niyogi, R., 2010. A generic framework for network forensics. International Journal of Computer Applications, 1(11), pp.1-6.
6) Krishnan, S. and Shashidhar, N., 2021. Interplay of Digital Forensics in eDiscovery. International Journal of Computer Science and Security (IJCSS), 15(2), p.19.
7) Krishnan, S. and Shashidhar, N., 2021. Interplay of Digital Forensics in eDiscovery. International Journal of Computer Science and Security (IJCSS), 15(2), p.19.
8) Kao, D.Y., Chen, M.C., Wu, W.Y., Lin, J.S., Chen, C.H. and Tsai, F., 2019. Drone forensic investigation: DJI spark drone as a case study. Procedia Computer Science, 159, pp.1890-1899.
9) http://www.forensicsciencesimplified.org/av/AudioVideo.pdf unpublished. Accessed on 15November 2021.
10) https://www.rsmuk.com/ideas-and-insights/why-cybercrime-is-increasing-and-how-to-stay-secure accessed on 15 November 2021

11) https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks accessed on 5th December 2021.
12) https://www.cs.purdue.edu/homes/ninghui/courses/426_Fall10/handouts/CS426_forensics.pdf accessed on 5th December 2021
13) Kent, K., Chevalier, S. and Grance, T., 2006. Guide to integrating forensic techniques into incident. Tech. Rep. 800-86.K. Elissa, "Title of paper if known," unpublished.
14) "GUIDELINES FOR DIGITAL FORENSICS FIRST RESPONDERS" Best practices for search and seizure of electronic and digital evidence document March 2021. https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf accessed on 6th December 2021
15) "Electronic Crime Scene Investigation: A guide for First responders, Second Edition", https://www.ojp.gov/pdffiles1/nij/219941.pdf accessed on 7th December 2021.
16) Abdalla, S., Hazem, S. and Hashem, S., 2007. Guideline model for digital forensic investigation.
17) https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en avvessesd on 7th December 2021.
18) https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf accessesd on 15th Dececmber 2021.
19) https://www.lawctopus.com/academike/offences-act-2000/ accessed on 25th December 2021.
20) https://www.dfir.training/tools-sw-hw accessed on 5th January 2022.
21) Jain, N. and Kalbande, D.R., 2014. A comparative study based digital forensic tool: complete automated tool. Int. J. Forensic Comput. Sci, 9(1), pp.22-29.
22) Ghazinour, K., Vakharia, D.M., Kannaji, K.C. and Satyakumar, R., 2017, September. A study on digital forensic tools. In 2017 IEEE international conference on power, control, signals and instrumentation engineering (ICPCSI) (pp. 3136-3142). IEEE.
23) "EnCase® Forensics USER GUIDE Version 8.07" by Guidance Software:May11,2018
24) "Forensic Tool Kit(FTK) User guide by Access Data": Document Date September 16,2020.
25) https://www.magnetforensics.com/docs/axiom/html/Content/Resources/PDFs/Magnet%20AXIOM%20User%20Guide.pdf accessed on 15th January 2022.
26) https://www.cellebrite.com/en/home/ accessed on 15th January 2022.
27) https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective accessed on 15th January 2022.
28) https://www.sans.org/tools/sift-workstation/ accessed on 20th January 2022.
29) https://districts.ecourts.gov.in/sites/default/files/Webinar%20on%20Admissibility%20of%20Electronic%20Evidence%20By%20Sri%20A%20Venkateshwara%20Rao.pdf accessed on 20th January 2022.
30) https://resources.infosecinstitute.com/topic/computer-forensics-chain-custody/ accessed on 5th February 2022.
31) https://www.linealservices.com/what-is-the-chain-of-custody-in-digital-forensics/ accessed on 5th February 2022.\
32) http://mja.gov.in/Site/Upload/GR/Title%20NO.190(As%20Per%20Workshop%20List%20title%20no190%20pdf).pdf accessed on 17th February 2022.