Digital Forensics

By Viral Parmar

The Hackers Meetup™
Let's Talk About Hacking

Who Am I

@viralparmarhack

Viral Parmar

ComExpo Cyber Security Foundation
Cyber Security Researcher
Mozilla Reps, Mozilla Foundation
Given 700+ session all over the world
Solved 500+case of cyber crime and aware more then 10 lakh people about privacy and security
Motto: Know hAckiNG, but no HaCKing.

COMEXPO CYBER SECURITY FOUNDATION

Crime Scene Investigation: Search and Seizure

Steps in Crime Scene Investigation
Panchanama (Seizure Memo) and Seizure Proceedings

The sequences of steps for digital crime scene investigations are

- Identifying and securing the crime scene
- Documentation of the scene of offence
- Collection of evidence
- Procedure for gathering evidences from Switched-off Systems
- Procedure for gathering evidence from live systems
- Forensic duplication
- Conducting interviews
- Labelling and documenting of the evidence
- Packaging and transportation of the evidences

Panchanama

Also known as ‘seizure memo’
Form filled wherever some material is seized by a forensic investigator

The Investigating Officer has to take additional care while conducting panchanama and seizure of digital evidences keeping in mind the nature of digital evidences

FORMAT FOR SEIZURE MEMO

SEIZURE MEMO

In pursuance of Section 26 of Bureau of Indian Standards Act, 1986 a search of M/s was undertaken on (date)

Name & Signature
of the inspecting officer
(authorized for search by CA)

During the search, M/s was found to be using the BIS Standard Mark and the following material was recovered and seized :

SL. NO	Description of the Material/Documents seized with details of marking with specific reference to Standard Mark	Quantity	Identification Mark
(1)	(2)	(3)	(4)

WITNESSES :
(signatures, date, name & address)
.
1.

2.

(Signatures, name and address of the person in charge of the premises searched for receiving this letter after search).

The material seized and sealed/packed as under :

Conducting Interviews

General Investigative Questions

- When did the incident first come to his (complainant) notice?
- How it was established that action in question has been performed by any outsider or some user has performed in excess of his privileges provided?
- What are the foreseen damages?
- Who could be the potential intruder (Prime Suspect)?
- What is the main reason of such doubt?
- What could be the major impact on the business?
- What are the major Systems which are required to run the critical functions of the business?
- What actions have been taken to identify, collect, preserve, or analyze the data and the devices involved?
- Have the evidences been collected by a trained person?

Seizure Proceedings

Guidelines:

- One of the technical people from the responder side along with two independent witnesses is part of the search and seizure proceedings
- Identify the equipment correctly
- Guide the IO and witnesses
- Please refer to the notes made during the pre-investigation assessment
- Cross verifying and correctly documenting the technical information
- Equipment, networks and other communication equipment at the scene of crime
- Time Zone/SystemTime has to be noted carefully in the panchanama, from the systems that are in ‘switched on’ condition
- Devices should not be switched on
- Serial number is to be allotted for each device
- Should be duly noted
- Panchanama, Chain of Custody and Digital Evidence Collection forms.
- Each device is to be photographed before starting of the investigation process at their original place
- Cubicle number or name room soundings etc.
- Photograph the Hard Disk Drive or any other internal part along with the system, once removed

- Paste the serial number with Crime number/section of law
- Note all the information about the system and data in the panchanama
- Includes searching and seizing
- Brief the witnesses regarding the tools used to perform search and seizure of the digital evidence
- Panchas (witnesses) must have some knowledge and ability to identify various digital devices
- Document the Chain of Custody and Digital Evidence Collection forms
- Make sure all the details mentioned in the forms are completely filled

Chain of custody

Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence

- People who have seized the equipment
- People in charge of transferring the evidence from the crime scene to the forensic labs
- People in charge of analysing the evidence etc.

CHAIN OF CUSTODY

DETAILS OF THE DIGITAL EVIDENCE

Crime number.....

Date of Seizure.....

Name of the I.O.....

Time.....

P.F.Number.....

TECHINAL INFORMATION

MANUFACTURER	MODEL	SERIAL NUMBER	PF NUMBER

DESCRIPTION

CHAIN OF CUSTODY

REASON/ACTION	RECEIVED FROM	RECEIVED BY	DATE	TIME	REMARKS

Guidelines for collecting evidence

- Physically inspect the storage medium — take photographs and systematically record observations.
- Guard against hazards like theft and mechanical failure.
- Use good physical security and data encryption.
- House multiple copies in different locations.
- Protect digital magnetic media from external electric and magnetic fields. Ensure protection of digital media particularly optical media from scratches.
- Account for all people with physical or electronic access to the data.
- Keep the number of people involved in collecting and handling the devices and data to a minimum
- Always accompany evidence with their chain-of-custody forms
- Give the evidence positive identification at all times that is legible and written with permanent ink.

Establishing the integrity of the seized evidence through forensically proven procedure by a technically trained investigating officer

- or with the help of a technical expert
- will enhance the quality of the evidence when the case is taken forward for prosecution.
- The integrity of the evidence available on a digital media can be established by using a process called as “Hashing”.
- Establish a baseline of contents for authentication and proof of integrity by calculating hash value for the contents.
- An identical hash value of the original evidence seized under panchanama and, the forensically imaged copy,
- Helps the IO to prove the integrity of the evidence.

Hashing program

- produces a fixed length large value (ranging from 80 – 240 bits)
- Represents the digital data on the seized media
- Any changes made to the original evidence will result in the change of the hash value
- Hashing is applying a mathematical algorithm
- A file/disk/storage media
- Produce a value that is unique like fingerprint to that file/disk/dataset
- Any changes that will be made in the file/dataset will in turn change/alter the hash value
- Hash value is usually alphanumeric

Forensic Collection of Digital Media

Identifying/Seizing of the devices needs to be forensically imaged for analysis

- Pre-investigation assessment must be complete and accurate before commencing the Crime Scene Investigation
- Be ready to identify all the relevant parties and equipment at the scene
- If the person at the scene of crime is not able to tell if the device is relevant for investigation, seize it

- Documentation tools
- Pen and paper for notes
- Stick-on labels etc.
- Disassembly and removal tools in a variety of nonmagnetic sizes and types
- Screwdrivers
- Wire cutters etc.
- Packaging and transporting supplies
- Bubble wraps
- Sturdy boxes etc.
- Other miscellaneous items
- Gloves
- Magnifying glass
- Small flashlight

Digital Evidence Collection Form			
Crime Number:		Date:	
PS/Circle/SDPO:		Time:	
IO Name		Item Number:	
Location :		Custodian / Suspect Name:	

Computer Information			
☐ Laptop	☐ Desktop	Manufacturer	
☐ HDD Only	☐ External HDD	Model Number	
☐ Others		Serial Number	
Time Zone		Asset tag	
BIOS Date and Time		Actual Date and Time	

Evidence Drive			
Acquired By		Date of Acquisition	
Signature of I.O		Time of Acquisition	

Acquisition Information			
☐ IDE	☐ SCSI	Manufacturer	
☐ SATA	☐ Other	Model Number	
		Serial Number	
		HDD Size	

Collection Details		Destination Drive Details	
Software used		Manufacturer	
Version		Model Number	
Write Protect Device Used		Serial Number	
Verified By		HDD Size	
Image File Name			
Notes			

Packaging and labelling of the evidence

Package and labeling refers to collection of the evidence

- Numbering them in a way that it would be easy to go back and retrieve the data at a later date/time
- Every piece of evidence needs to get a tag number
- Contains all the visible details on the evidence
- This information goes into evidence Database
- The IO has to choose packaging that is of proper size and material, to fit into the evidence

Various types of evidence need special packaging,

- Need to come to the scene prepared with a variety of evidence envelopes, bags, and containers
- The packaging should also be clean, and preferably new, to avoid contamination
- Each piece of evidence should be packaged separately
- Should be properly labeled, sealed, and documented
- Use anti-static bags to transport evidence
- These will protect and prevent any localized static electricity charge from being deposited onto the devices as the bags are handled

Transportation of the evidences

The dispatch and transportation of evidences is another crucial aspect that has to be kept in mind by the IOs

- Poor dispatching and transportation practices can physically damage the evidences collected and thereby rendering them useless
- Sometimes, the poor handling may result in alteration of the contents of the digital evidences due to shock and external electro-magnetic interferences

Two things to ensure while sending the evidences to the Forensic Science Laboratories

- The suspected computer storage media is carried by a special messenger and not by Registered / Insured post
- A fresh hard disk of approximately same capacity should also be submitted for forensic imaging along with the suspected storage media.

Legal procedure post-seizure of evidence

Once the digital evidence is seized during the course of investigation, it has to be brought to the notice of the jurisdictional court

- Obtain orders of the competent court to retain the seized properties in the custody of the investigating officer for the purpose of investigations
- Obtain necessary orders from the competent court to image the data
- Send the digital evidence for forensic analysis and expert opinion

In cases where the accused persons or the owners of the property seized approaches the court for release of the impounded properties

- IO should carefully prepare objections for such applications
- Ensure that no original evidences are returned which have a bearing on the prosecution of the case
- Unless the court specifically orders, releasing seized properties means releasing a forensically imaged copy

Four principles for dealing with digital evidence

1. No actions performed by investigators should change data
2. Individuals accessing original data must be competent to do so
3. An audit trail must be created and preserved documenting each investigative step
4. The person in charge of the investigation has overall responsibility for ensuring the laws and guidelines of the government

Expert Opinion from the Forensic Examiner

The forwarding letter to the FSL for scientific analysis and opinion should mention information like:

- Brief history of the case
- The details of the exhibits seized and their place of seizure
- The model, make and description of the hard disk or any storage media
- The date and time of the visit to the scene of crime
- The condition of the computer system (on or off) at the scene of crime
- Is the photograph of the scene of crime taken?
- Is it a stand-alone computer or a network?
- Does the computer have any Internet connection or any means to communicate with external computers?
- Were the BIOS date and time stamps taken, or not? If taken the date and time should be mentioned

Annexure 5-5: Requisition letter to FSL

Forwarding Note

(In all cases where examination of any material is required at the laboratory, a copy of this form duly filled in should accompany the exhibits.)

Case No.- /20xx	Police Station -
Section of Law -	Dist.-
Date - / /	State -

I. Nature of Crime

Nature of Crime.....

.....

Brief History .....

.....

Any other relevant details.....

II – List of Exhibits for Examination

Sr. No. / Barcode	Description of Exhibits	How, when, and by whom found	Source of exhibits	Remarks

III – Nature of Examination required

Sr. No. / Barcode	Description of Exhibits	Nature of Examination required	Date or any keyword or filter	Remarks

IOs are advised to pay additional attention to this section, as this plays a critical component in the investigation. Apart from requesting the information required for the investigation like files, deleted information, etc., from the digital evidence, lot of other information, which can be developed as supporting (secondary) evidence in the investigations like login time, users list, various applications installed, IP address, printers connected, etc.

IOs are suggested to contact the forensic lab professionals to understand what kind of information can be retrieved from these digital media which can be vital evidence.

Sr. No.	Full Name	Occupation	Sex	Date and Time of arrest	Whether bailed, court or Police Custody

Seal	Rank and Sign. of the I. O.
O/W No.-	Date - .....
Forwarded to the Director,.....	
Specimen Seal/s impression/s on exhibits or parcel/s	Sign and Designation of Forwarding Officer

Certificate of Authority

Certified that the Director .....

has the authority to examine the exhibits sent to him in connection with Case No.

..... u/s ..... Pol. St .....

Date ..... of .....State versus .....

Date:	
Place:	Sign and Designation of Forwarding Authority

Laws / Guidelines Relating To International Investigations

- Cyber Space and computers do not recognize national boundaries
- Law is bound by national boundaries
- Many a times the victim may be residing in one national boundary, the offender may be from another national boundary
- Investigators during the course of investigations need to resort to conduct investigations outside their national boundaries and as per the criminal law of the foreign country
- It is essential that, each Investigator handling cyber crimes possess the requisite knowledge of International investigations as prescribed under law and mandated by the Government.

Legal procedure to gather information from outside India

MLAT (Mutual Legal Assistance Treaty) and Letter Rogatory

- Guidelines have been issued by the Ministry of Home Affairs, Government of India
- The Code of Criminal Procedure (Cr.P.C) under Sec.166–A and 166– B provides for the process for making a request to any foreign country to help and assist in an investigation

Provisions of Law: 166-A Cr.P.C. Letter of request to competent authority for investigation in a country or place outside India

If an application is made by the investigating officer or any officer superior in rank to the investigating officer that evidence may be available in a country or place outside India

- Any Criminal Court may issue a letter of request to a Court or
- An authority in that country or place competent to deal with such request
- Identify any person supposed to be acquainted with the facts and circumstances of the case
- Record his statement made in the course of such examination
- Require such person to produce any document or thing which may be in his possession pertaining to the case
- Forward all the evidence collected or the authenticated copies to the Court issuing such letter

The letter of request shall be transmitted in such manner as the Central Government may specify in this behalf

Every statement recorded, or document or thing received shall be deemed to be the evidence collected during the course of investigation

Meaning of Letters Rogatory

A formal communication in writing sent by the Court in which action is pending to a foreign court or Judge Requesting the testimony of a witness,

- Witness residing within the jurisdiction of that foreign court,
- Witness may be formally taken thereon under its direction
- Transmitting to the issuing court making such request for use in a pending legal contest or action
- Request entirely depends upon the committee of court towards each other and usages of the court of another nation

Letter of request from a country or place outside India to a Court or an authority for investigation in India

- Upon receipt of a letter of request from a Court or an authority in a country or place outside India, the Central Government may, if it thinks fit
- Forward the same to the Chief Metropolitan Magistrate or Chief Judicial Magistrate
- Shall summon the person before him
- Record his statement or cause the document or thing to be produced
- Send the letter to any police officer for investigation, who shall investigate into the offence as if the offence had been committed within India
- All the evidence taken or collected or authenticated copies shall be forwarded by the Magistrate or police officer to the Central Government for transmission to the Court or the authority issuing the letter of request

Procedure for Sending Letter Rogatory

In order to conduct formal investigation and to collect evidence and gather material objects/documents, 3 scenarios are considered:

- Section 166–A of the Criminal Procedure Code, 1973 lays down the procedure of sending ‘Letter of Request’ (Letter Rogatory) through a competent Court
- Letter is forwarded within the ambit of Mutual Legal Assistance Treaty (MLAT) in criminal matters, Memorandum of Understanding (MoU) Arrangement, etc.,
- Treaties that exist between India and the requested country or on basis of reciprocity in cases where no such treaty or MoU exists
- No request for issue of a Letter Rogatory (Letter of Request) shall be brought before any Court by an Investigating Agency without the prior concurrence of the Central Authority

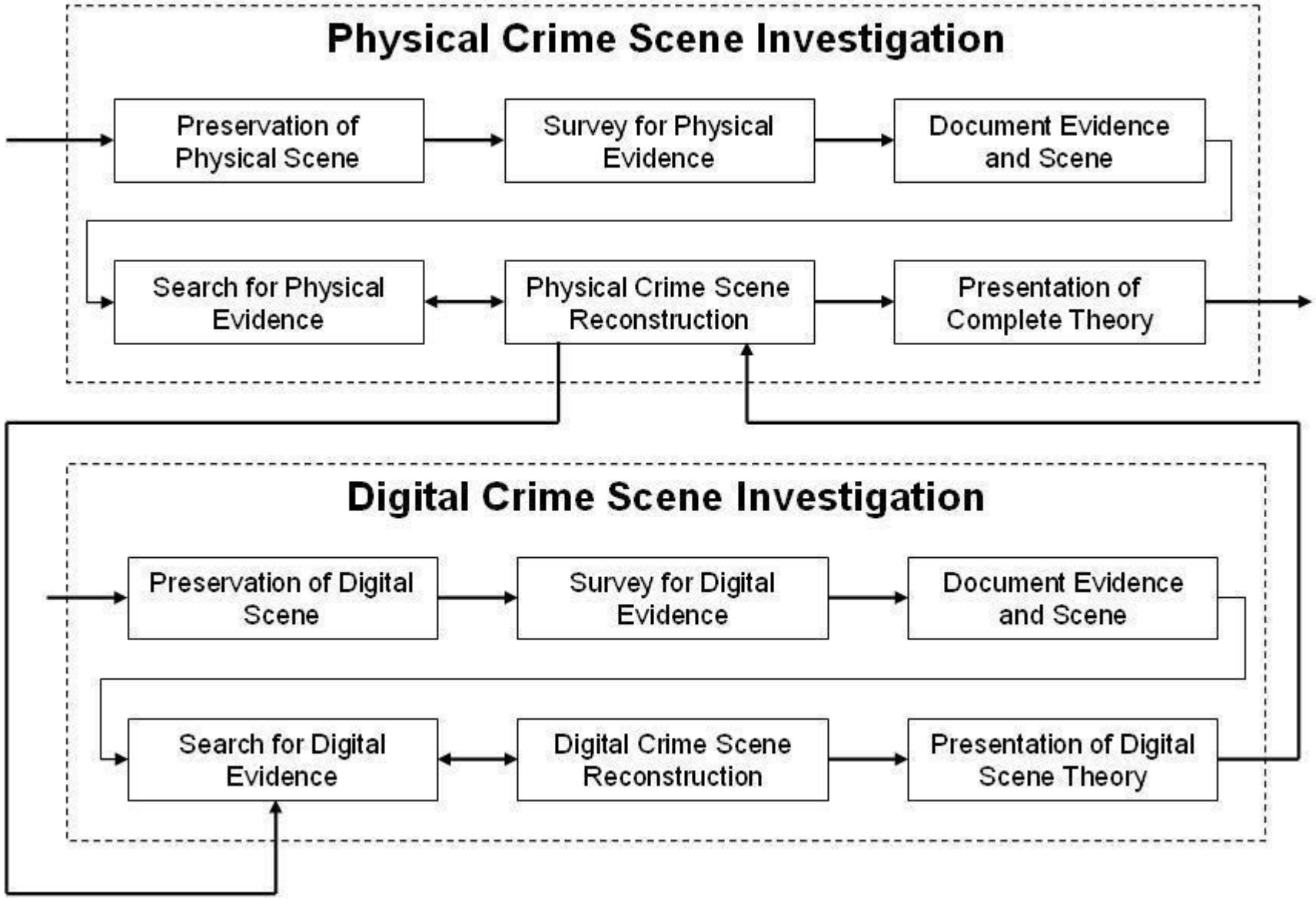
The request must incorporate the following details:

- The documents, Photographs, and objects, if enclosed with the Letter Rogatory, should be clearly marked and referred to in the body to enable the requested Authority to know clearly what is required to be done with them
- All the photocopied papers and documents enclosed must be legible and translated into the required language
- The Letter Rogatory should be neatly bound and page numbered
- The authenticated translated copies duly signed by a translator should be enclosed along with the original Letter Rogatory, if required to be submitted in a language as prescribed in the MLAT, MoU, Arrangement, or otherwise
- At least five copies of the Letter Rogatory should be prepared, including the original.
- Three copies along with the translated version, if any, are to be sent to MHA (Ministry of Home Affairs) along with a copy to the International Police Cooperation Cell of CBI.

Normally:

- The Investigating officer should obtain the NO OBJECTION CERTIFICATE from the Director of Prosecution /Department of Public Prosecution
- The NOC will be issued by Dept. of Prosecution after looking into the Dual Criminality Principle
- The Letter of Request along with the NOC obtained should be routed to the Interpol liaison officer, CBI through proper channel

How to Investigate



Legal Proceedings

- Cybercrime law identifies standards of acceptable behaviour for information and communication technology (ICT) users;
- Establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular
- Protects human rights
- Enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings)
- And facilitates cooperation between countries on cybercrime matters.
- Cybercrime law provides rules of conduct and standards of behaviour for the use of the Internet, computers, and related digital technologies, and the actions of the public, government, and private organizations;
- Rules of evidence and criminal procedure, and other criminal justice matters in cyberspace
- And regulation to reduce risk and/or mitigate the harm done to individuals, organizations, and infrastructure should a cybercrime occur.
- Accordingly, cybercrime law includes substantive, procedural and preventive law.

Phishing Fraud

Applicable Sections of Law
66C and 66D of Information Technology (Amendment) Act, 2008 and Section 420 of IPC – Identity theft, cheating by per- sonation using computer resources and cheating.

Pre-Case assessment:
After registration, the investigation has to be undertaken by an officer of the rank of Police Inspector or above (as per ITAA 2008).

Information gathered

From complainant: Self attested copies of the printout of phishing email along with full headers printed at the police station and soft copies of the same with date and time stamps. Details of the bank account of the victim.

From Bank:

- The account statement of the complainant, which included fraudulent transaction details.
- Transaction IP address of the fraudulent transaction.
- Details of the beneficiaries (company to which the amount was credited for the online purchase of the electronic gadgets)
- and, the delivery address of the electronic equipment.

From Website Hosting Company: Particulars of the persons responsible for hosting the phishing website.

[redacted]

Reconnect to Facebook

You connected Facebook to your Microsoft account so that you could stay in better touch with your friends. Unfortunately, we haven't been able to connect to your Facebook account lately.

Reconnecting is easy

Luckily, you can get things working again just by checking your Facebook connection settings and clicking **Connect with Facebook**. Sign in to Facebook from there, and you're done!

Reconnect now

Once you reconnect, you can chat with your Facebook friends, see their latest updates, share files, and more. Your Facebook connection is available in places where you sign in with your Microsoft account, including Windows 8, Windows Phone, Outlook.com, OneDrive, and Office 2013.

What happened?

You might have changed your password on Facebook or changed your Facebook privacy settings in a way that broke the connection. When you reconnect to Facebook, your connection settings will be restored.

Thanks for using your Microsoft account to bring the people who matter most together in one place. You can change your connection settings anytime and find more ways to connect at https://profile.live.com/services.

Fake, Obscene Account of Social Media

Applicable Sections of Law
Section 465, 469 of IPC (Forgery, Forgery for purposes of harming reputation) and Section 67 of IT Act (publication or transmission of obscene material in electronic form).

Pre-Case assessment:
Investigation to be done by an officer of the rank of Police Inspector or above (in case of ITAA 2008). Issues to be kept in mind while seeking / collection of information from complainant / accused / witnesses and service providers: The relevant date and timestamps, shall always be collected.

Information gathered
From complainant: Self attested copies of the printout of the fake profiles printed at the police station and soft copies of the offensive content with date and time stamps (self attested copies of the printout of the friendship requests received by Priya's friends and soft copies of the offensive content with date and time stamps

- Obtaining 3rd party information from service providers
- Collection of Evidences from Accused / Scene of Offence
- Search & Seizure of digital evidence

Data Theft

Applicable Sections of Law
Section 66 read with section 43 of the ITA 2000 and Section 66(B) of ITAA2008

Pre-Case assessment
Information collected from complainant

Information gathered
Obtaining 3rd party information from service providers
Search & Seizure of digital evidence

Kidnapping of Girl

Applicable Sections of Law

No applicable sections for “Missing Case” but, in case if there is suspicion that some known person might have kidnapped, in such cases section 363 of IPC is applicable.

Pre-Case assessment

SHO of the police station can register the case under 363 IPC and the investigation should be carried out by an officer not below the rank of Police Inspector.

Information gathered

- Proof for Age-Date of Birth
- Photograph of the missing person
- Physical features
- Languages known- to speak/write
- Mobile phone number-if available
- Email ID- if available

Investigation:

1. The IO sent a requisition letter to the mobile service provider under section 91 CrPC to provide the call details and tower locations details of the mobile phone used by the missing person
2. The call details thus obtained did not disclose any useful information because the mobile phone was switched off from the day the girl was missing and there were no entries found in the CDR.
3. The IO created an undercover email ID and sent a tracking mail to the missing girl's email ID that was shared by the complainant at the time of registering the complaint.
4. The tracking email was sent by using free tracking email service like www. Readnotify.com or www.didtheyreadit. com
5. The tracking mail thus sent was opened by the user and notification was obtained in the undercover email id cre- ated by the IO
6. The notification page carried information like
   - IP address
   - Date and time of opening the mail
   - No. of time opened etc
7. The internet service provider was identified and a requisition letter was sent to provide the physical address de- tails
8. The internet service provider provided the details
9. The IO made a visit to the address and found that the girl was residing with Naveen.
10. The IO arrested Naveen under the applicable sections
11. The IO recorded the statement of both the accused and victim and emphasized on reason for kidnapping in the statement and the conventional investigative procedures were followed.

Hacking using Malware

Applicable Sections of Law

Section 66C, ITAA 2008: Punishment for identity theft, Section 66D, ITAA 2008: Punishment for cheating by personation by using computer resource

Pre-Case assessment

attested copies of email/sms received from any source other than the legitimate bank. Bank statement (if available)

Information gathered

- Statement of the account of the complainant during the fraudulent activity period
- Transaction IP address of the subject transaction
- CAF form of the beneficiary account(in case if it is same bank)
- Details of the beneficiary bank(name of bank, branch, account number etc.,)

Website Blocking

Applicable Sections of Law

Section 69 A, empowers the competent authorities notified under ITAA 2008 to block public access of notified websites.

Pre-Case assessment:

Power to issue directions for blocking public access to any information through computer resource

- Where the Central Government or any of its officers, specially authorized by it in this behalf, is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states, or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of Sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public, or cause to be blocked for access by public any information generated, transmitted, received, stored, or hosted in any computer resource.
- The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.
- The intermediary who fails to comply with the direction issued under Sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

Information gathered

The investigating officer saved all the web pages in the subject website by using a special application by offline browsing and saved it into a CD-ROM. The IO also took the printout of the web pages.

Process for blocking Websites

Based on the above Government notification, the Police moved an application for the block- ing of the websites and submitted to the Government of India through the State Home Department.

GSR 781(E) of Gazette of India notification dated 27th Oct, 2009 prescribes the rules and process to be followed for blocking of websites. The detailed notification can be accessed at http://www.mit.gov.in/sites/upload_files/dit/files/downloads/ itact2000/Itrules301009.pdf.

Guidelines to prepare charge sheet

Inadequate skill in drafting the charge-sheet is one of the reasons which help the accused to get away with cybercrime committed by them. Many cases fail before the Courts of Law just because of the defective framing of charge-sheets. There are a number of incidents, where the IO has failed to file the charge sheet with all required information / documentation in cyber crimes and cases acquitted by courts of law.

Below are few guidelines for IO to include in the charge sheet.

- All the relevant information shared by the complainants during registering the FIR/course of investigation should be included in the charge sheet.
- Please make sure the sections mentioned in FIR are still applicable for the case OR it is advised to file a requisition to change of sections before the case including appropriate ITAA 2008 and other supportive IPC, special and local laws. (there are number of incidents, IO filing the charge sheet under wrong sections of IT Act)
- Make sure the search and seizure procedure along with Chain of custody and DEC form are included in the charge sheet.
- Make sure the nature of cybercrime and the necessary information / analysis requested from FSL or forensic examiner are incorporated properly in the charge sheet.
- Please provide the detailed information about the crime scene and the process IO followed to identify the systems used / affected in the crime.
- Please include all the technical persons who identified, produced and analyzed the digital in the case as witness.

Action Against Cyber Crime

- The Protection of Children from Sexual Offences (POCSO) Act had been amended in 2019 to include the definition of child pornography under Section 2(da) and punishment provided under Section 14 and Section 15 of the Act.
- Provisions to deal with cyber crime against children under Information Technology (IT) Act, 2000. Section 67B of the Act provides stringent punishment for publishing, browsing or transmitting of material depicting children in sexually explicit act, etc. in electronic form. Further, sections 354A and 354D of Indian Penal Code, 1860 provide punishment for cyber bullying and cyber stalking.
- Government periodically blocks the websites containing extreme child sexual abuse material (CSAM) based on INTERPOL's "worst of list" received through Central Bureau of Investigation (CBI), the national nodal agency for Interpol in India.
- The Government is implementing a comprehensive central sector scheme, namely "Centre for Cyber Crime Prevention against Women and Children (CCPWC)" to handle all issues related to check all cyber-crime against women and children including child pornography.
- National Cyber Crime Reporting Portal, www.cybercrime.gov.in has been launched by the Government to enable citizens to online report complaints pertaining to all types of cyber crimes with special focus on cyber crimes against women and children. Complaints reported on this portal are attended by the respective Law Enforcement Authorities of States. A nation-wide helpline number [155260] is also made functional to help public in filing complaints through the portal.

Digital Forensics

Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from the digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

Definition Application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence (information of probative value that is stored or transmitted in binary form) after proper search authority, chain of custody, validation with mathematics (hash function), use of validated tools, repeatability, reporting and possible expert presentation

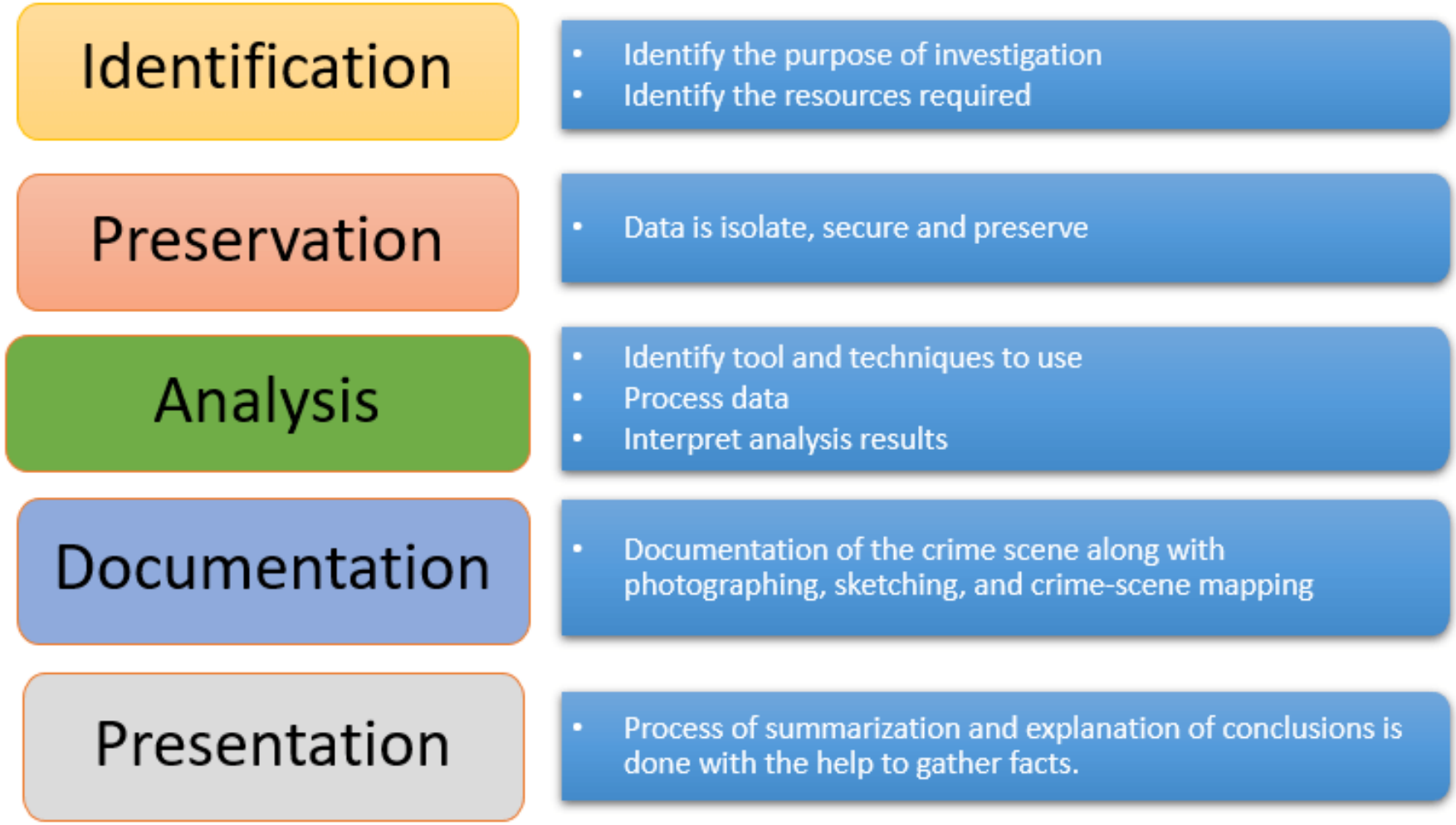
Objectives of Digital Forensics

- It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

Challenges for Digital Forensics

- The increase of PC's and extensive use of internet access
- Easy availability of hacking tools
- Lack of physical evidence makes prosecution difficult.
- The large amount of storage space into Terabytes that makes this investigation job difficult.
- Any technological changes require an upgrade or changes to solutions.

Process of Digital Forensics



Locard's Principle

Edmund Locard (1877–1966) was the director of the first (according to some) crime lab, in Lyon, France

Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it can diminish its value.

Locard's Exchange Principle: in the physical world, when perpetrators enter or leave a crime scene, they will leave something behind and take something with them.

Digital Evidence

Digital evidence act, The Bureau of Indian Standards Act, Digital devices are everywhere in today's world, helping people communicate locally and globally with ease. Most people immediately think of computers, cell phones and the Internet as the only sources for digital evidence, but any piece of technology that processes information can be used in a criminal way. For example, hand-held games can carry encoded messages between criminals and even newer household appliances, such as a refrigerator with a built-in TV, could be used to store, view and share illegal images. The important thing to know is that responders need to be able to recognize and properly seize potential digital evidence.

Gathering Evidence

Crime scene investigators document the crime scene. They take photographs and physical measurements of the scene, identify and collect forensic evidence, and maintain the proper chain of custody of that evidence. Once the crime scene has been thoroughly documented and the locations of the evidence noted, then the collection process can begin. The collection process will usually start with the collection of the most fragile or most easily lost evidence. Special consideration can also be given to any evidence or objects which need to be moved. Collection can then continue along the crime scene trail or in some other logical manner. Photographs should also continue to be taken if the investigator is revealing layers of evidence which were not previously documented because they were hidden from sight.

Guidelines for collecting evidence

- Physically inspect the storage medium — take photographs and systematically record observations.
- Guard against hazards like theft and mechanical failure.
- Use good physical security and data encryption.
- House multiple copies in different locations.
- Protect digital magnetic media from external electric and magnetic fields. Ensure protection of digital media particularly optical media from scratches.
- Account for all people with physical or electronic access to the data.
- Keep the number of people involved in collecting and handling the devices and data to a minimum
- Always accompany evidence with their chain-of-custody forms
- Give the evidence positive identification at all times that is legible and written with permanent ink.

Establishing the integrity of the seized evidence through forensically proven procedure by a technically trained investigating officer

- or with the help of a technical expert
- will enhance the quality of the evidence when the case is taken forward for prosecution.
- The integrity of the evidence available on a digital media can be established by using a process called as “Hashing”.
- Establish a baseline of contents for authentication and proof of integrity by calculating hash value for the contents.
- An identical hash value of the original evidence seized under panchanama and, the forensically imaged copy,
- Helps the IO to prove the integrity of the evidence.

Hashing program

- produces a fixed length large value (ranging from 80 – 240 bits)
- Represents the digital data on the seized media
- Any changes made to the original evidence will result in the change of the hash value
- Hashing is applying a mathematical algorithm
- A file/disk/storage media
- Produce a value that is unique like fingerprint to that file/disk/dataset
- Any changes that will be made in the file/dataset will in turn change/alter the hash value
- Hash value is usually alphanumeric

Forensic Collection of Digital Media

Identifying/Seizing of the devices needs to be forensically imaged for analysis

- Pre-investigation assessment must be complete and accurate before commencing the Crime Scene Investigation
- Be ready to identify all the relevant parties and equipment at the scene
- If the person at the scene of crime is not able to tell if the device is relevant for investigation, seize it

- Documentation tools
- Pen and paper for notes
- Stick-on labels etc.
- Disassembly and removal tools in a variety of nonmagnetic sizes and types
- Screwdrivers
- Wire cutters etc.
- Packaging and transporting supplies
- Bubble wraps
- Sturdy boxes etc.
- Other miscellaneous items
- Gloves
- Magnifying glass
- Small flashlight

Digital Evidence Collection Form			
Crime Number:		Date:	
PS/Circle/SDPO:		Time:	
IO Name		Item Number:	
Location :		Custodian / Suspect Name:	

Computer Information			
☐ Laptop	☐ Desktop	Manufacturer	
☐ HDD Only	☐ External HDD	Model Number	
☐ Others		Serial Number	
Time Zone		Asset tag	
BIOS Date and Time		Actual Date and Time	

Evidence Drive			
Acquired By		Date of Acquisition	
Signature of I.O		Time of Acquisition	

Acquisition Information			
☐ IDE	☐ SCSI	Manufacturer	
☐ SATA	☐ Other	Model Number	
		Serial Number	
		HDD Size	

Collection Details		Destination Drive Details	
Software used		Manufacturer	
Version		Model Number	
Write Protect Device Used		Serial Number	
Verified By		HDD Size	
Image File Name			
Notes			

Evidence Handling

Collecting and handling digital evidence is a crucial part in performing digital forensics. Not collecting the right evidence or mishandling evidence can lead to a perpetrator not getting convicted for their crime. Everything from the way digital evidence is collected to the way it is worked with and even stored plays a vital role in court proceedings. For example, once an incident is made apparent, it is advised that evidence gathering procedures be initiated. In this way, you will be more likely to gather all pertinent evidence before they become lost or deleted.

Chain of custody

Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence

- People who have seized the equipment
- People in charge of transferring the evidence from the crime scene to the forensic labs
- People in charge of analysing the evidence etc.

CHAIN OF CUSTODY

DETAILS OF THE DIGITAL EVIDENCE

Crime number.....

Date of Seizure.....

Name of the I.O.....

Time.....

P.F.Number.....

TECHINAL INFORMATION

MANUFACTURER	MODEL	SERIAL NUMBER	PF NUMBER

DESCRIPTION

CHAIN OF CUSTODY

REASON/ACTION	RECEIVED FROM	RECEIVED BY	DATE	TIME	REMARKS

Performing Digital Forensics

- Acquisition
- Validation & Verification
- Extraction
- Reconstruction
- Reporting

Acquisition

- Physical data copy
- Logical data copy
- Data acquisition format
- Command-line acquisition
- GUI acquisition
- Remote, live, and memory acquisitions

Validation & Verification

Validation: a way to confirm that a tool is functioning as intended

Verification: proves that two sets of data are identical by calculating hash values or using another similar method

Filtering

- Related process
- Involves sorting and searching through investigation findings
- Separate good data and suspicious data

Extraction

- Data viewing
- Keyword searching
- Decompressing
- Carving: technique of reassembling files from raw data fragments when no filesystem metadata is available
- Decrypting
- Bookmarking or tagging

Reconstruction

Purpose

Re-create a suspect drive to show what happened during a crime or an incident

Create a copy for other digital investigators if a

Methods of reconstruction

- Disk-to-disk copy
- Partition-to-partition copy
- Image-to-disk copy
- Image-to-partition copy
- Disk-to-image copy
- Rebuilding files from carving

Reporting

To perform a forensics disk analysis and examination, we need to create a report

- Bookmarking or tagging
- Log reports
- Timelines
- Report generator

Quality of Computer Forensics

- Legal Authority
- Integrity of Evidence
- Forensic Documentation
- Administrative Review
- Technical Review
- Validation Testing

Digital Evidence Assessment

The type of crime that we want to prove or disprove determines

- What evidence we need to analyse
- How the recovered information is to be used
- Related to inculpatory and exculpatory evidences

1. Evidence acquisition
2. Evidence examination
3. Documenting and reporting digital evidence

Evidence acquisition

- The physical removal of storage devices
- Using controlled boot discs to retrieve sensitive data without affecting existing stored data
- Ensuring functionality
- Taking appropriate steps to copy and transfer evidence to the investigator’s evidence repository
- Document and authenticate the chain of evidence

Evidence examination

Digital forensics investigators typically examine data from designated archives

- use a variety of methods and approaches to analyse information
- include utilising analysis software to search massive archives of data for specific keywords or file types
- retrieve files that have been recently deleted
- analyse data tagged with times and dates
- suspicious files or programs that have been encrypted or intentionally hidden

Documenting and reporting digital evidence

- Accurate record of all activity related to the investigation
- all methods used for testing system functionality and retrieving,
- copying, and storing data,
- all actions taken to acquire, examine and assess evidence

Purpose:

- Demonstrate how the integrity of user data has been preserved
- Ensures that proper policies and procedures have been adhered to by all parties involved
- The purpose of the entire process is to acquire data that can be presented as evidence in a court of law
- An investigator's failure to accurately document his or her process could seriously compromise the validity of that evidence and ultimately, the case itself