2 Cyber Crime Investigation Techniques and Legal Procedures

Himanshu Bhatt*
Cyber Crime Investigator.
*Corresponding Author: bhatthimanshu851@protonmail.com

Abstract

In today's digital world, cybercrime is becoming a major concern for individuals, businesses, financial institutions, and government as the world is getting digitalized and everything is going online. Cybercrime is increasing rapidly with advanced techniques and technologies. If cybercrime is on the rise, then is a need for solutions. It requires investigation techniques along with a systematic plan which, includes digital forensics, cyber intelligence, information gathering, incident response, disaster management and legal proceeding. This research dwells into the cyber techniques used in cybercrime investigation, such as the collection, preservation, and analysis of digital evidence, open-source intelligence, internet protocol address, social media investigation, device forensics, and digital trail reconstruction. It also deals with the legal procedures involved in the identification, gathering, preservation, and presentation of electronic evidence during a criminal investigation. It highlights the significance of upholding the integrity and authenticity of digital evidence so that the investigation is conducted in compliance with Indian legal and judicial requirements. The difficulties presented by anonymization technologies, encrypted communications, transnational cybercrime, the ever-changing nature of digital platforms, and the ephemeral nature of electronic evidence have also been addressed in this chapter, since these elements create difficulties for investigators' efforts to identify digital offenders and to collect legally admissible evidence. It also offers a structured approach to understanding the interrelation between technical investigation techniques and legal structures. This study also highlights the importance of proper evidence handling, documentation, and investigative coordination for cybercrime investigators with special references for law enforcement, academicians and digital forensics enthusiast.

Keywords: Cyber Crime, Cyber Investigation, Cyber Law, Digital Evidence, Artificial Intelligence, National Security.

Introduction

The internet, smartphones, cloud computing, social media platforms, digital payments, and online services have drastically changed our communication and day-to-day activities in today's digital age. Nevertheless, this tremendous growth in the development of technologies is also opening new doors for cybercriminals. Cybercrime isn't just about hacking or unauthorized access anymore; it now includes financial fraud, identity theft, social media abuse, ransomware, data breaches, online harassment, impersonation, cyberstalking, cryptocurrency-related crimes, and Artificial Intelligence. AI is being heavily misused today, as a single prompt can generate ready-made content. The biggest difference between cybercrimes and traditional crimes is that there are no geographical boundaries. The victim could be in another state, the suspect operating out of another state or country, digital data stored on a foreign server, and communications passing through multiple intermediary systems.

To mitigate this challenge, cybercrime investigation requires not only technical knowledge but also digital forensics, intelligence gathering, legal understanding, evidence preservation, and investigative judgment. A successful cybersecurity investigation is not limited to merely identifying an IP address or locating a social media profile. Rather, the investigator must establish exactly what happened during the incident how and when it occurred, which digital systems were involved, who might be responsible, what evidence is available, and whether that evidence has been legally and properly preserved or not. The primary objective of this article is to explore the major techniques used in cybercrime investigation and to investigate the legal procedures that are followed in India. The article discusses digital evidence, digital forensics, OSINT, IP investigation, financial fraud investigation, evidence preservation, chain of custody, and legal aspects of electronic evidence.

Understanding Cyber Crime Investigations

Cybercrime investigation is a systematic process that involves identifying, collecting, preserving, examining, analysing, and presenting digital information related to suspects who commit digital crimes. Digital evidence can be available in various forms, including;

- Smartphones
- Computers and Laptop
- Email Accounts
- Social Media Platforms
- Messaging Applications
- Cloud Storage

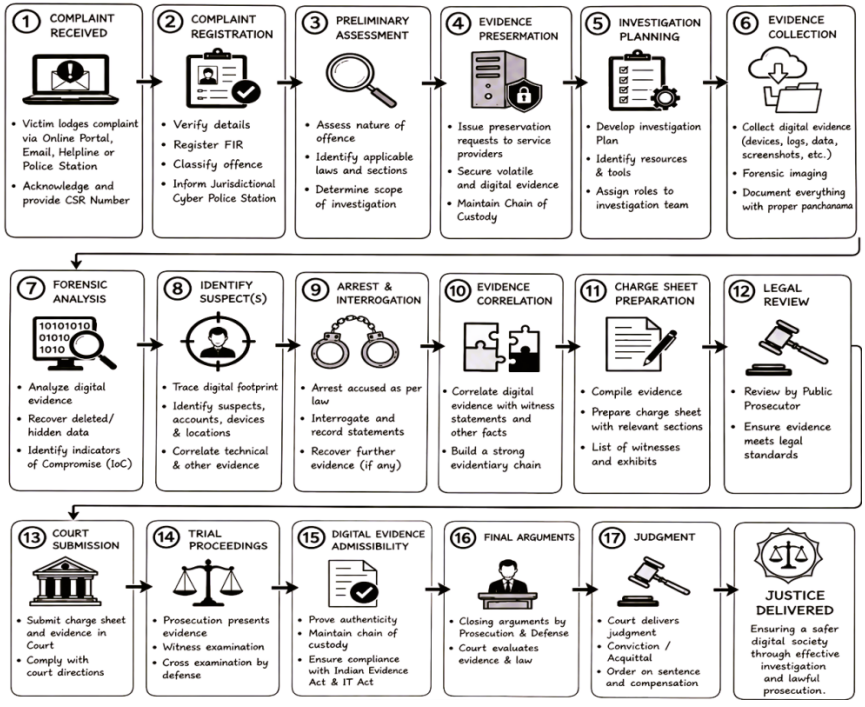
ISBN: 978-93-49468-02-3

- Server Logs
- Domain Registration Information
- Payment and Transaction Records
- CCTV
- Metadata
- Device Identifiers
- Cryptocurrency transaction records
- IP Addresses
- An investigator's objective is not merely to gather as much information as possible; rather, the primary objective is to identify evidence that is relevant, reliable, legally obtained, and properly preserved.

Major Stages of Cyber Crime Investigation.

A structured cybercrime investigation is divided into several interconnected stages. Every stage has its own importance, and weakness of any stages affect all investigation.The basic process can be understood something like this:

Figure: Cyber Crime Investigation Flow Chart Diagram



Source: Compiled and Created by Author

ISBN: 978-93-49468-02-3

Normally, cybercrime investigation starts after reporting of incident. At the initial stage, the investigator needs to identify some important questions, like:

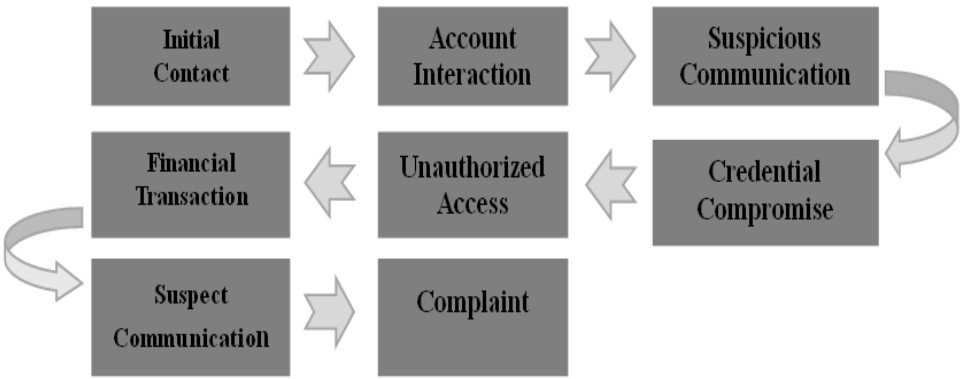
- What is the nature of incident?
- When did the incident occur?
- Who is the victim?
- Which digital platforms were used and devices involved?
- Which Accounts, URLs, or Email Address are available?
- Is the victim still receiving threats?
- Is there an immediate risk of evidence disappearing or not?
- Does the case involve financial loss, identity theft, harassment, threats, or any other offenses?
- Under which jurisdiction or authority does the case fall?

The initial assessment is the most important part of the cybercrime investigation because digital evidence can a volatile, accounts can be deleted, posts removed, logs overwritten, device reset, and cloud data can be tampered.

Incident Timeline Reconstruction

Timeline reconstruction is one of the important techniques in cybercrime investigation. In this process, investigator arranges the various digital events in chronological order. For examples;

Figure: Timeline Reconstruction



Some Information is useful for developing the timeline, such as

- Message timestamps
- Login Records

ISBN: 978-93-49468-02-3

- Email Headers
- Transaction Timestamps
- Server Logs
- Application Activities
- Device Artifices
- Social Media Activities
- CCTV Records

For instance, if an unauthorized login attempt occurs on an account at 20:15, and suspicious IP is recorded at 20:16 suspicious and a financial transaction takes place at 20:20, the investigator examines the technical and temporary relationships between these events to gather evidence. However, the identity or involvement of a particular individual cannot be conclusively established merely by the matching of event timestamps. Additional evidence is required. Digital evidence has been broadly divided into different categories:

Volatile Data

- **Identification of Digital Data**

Volatile data is essential data that disappear, when system shuts down. For example;

  - Data on RAM (Random Access Memory)
  - Active network connections
  - Running processes
  - Logged-in sessions
  - Temporary system information

- **Non-Volatile Data**

This information remains stored after the system shuts down. For example;

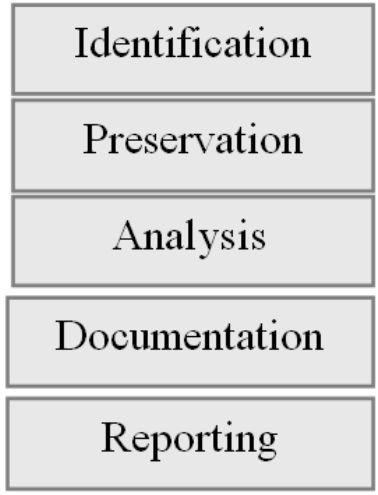
  - Storage Devices like hard drives, SSDs, etc
  - Cloud-stored files
  - Application databases
  - Memory cards

Digital Forensics

Digital Forensics is a part of cybercrime investigation. It involves the scientific examination of devices and digital data to identify relevant evidence for the investigation. A typical forensic process can be understood as follows in Figure 3:

ISBN: 978-93-49468-02-3

Figure 3: Process of Digital Forensics



It is important to protect the original evidence from unnecessary modification. Whenever we investigate evidence, we always create an image of the evidence from the storage media through forensic acquisition; after that, we investigate on that image of the storage media, with the reduction of tampering of original evidence.

Mobile Forensics

In today's world, smartphones have become highly important sources of evidence for cybercrime investigations. This is because most people store their personal and important data on their mobile phones largely because of convenience; they fit right in a pocket, making them easy to carry anywhere. Ultimately, mobile phones have become an integral part of our lives. Modern smartphones employ robust security mechanisms. Therefore, investigators should follow proper forensic procedures and applicable legal requirements, rather than attempting unauthorized access. Mobile forensics is one of the branches of digital forensics that involves identifying, acquiring, preserving, examining, and analysing digital evidence from smartphones and tablets, nowadays mobile phones are extensively used for communication, banking services, social media, authentication, photography, location services, and online transactions.

In mobile forensic examination the investigator has to consider the device's hardware, operating system, applications, user data and associated digital artifacts. Evidence sources include contacts, call logs, SMS, emails, photographs, videos, documents, browser history, application data, chat records, location-related information, Wi-Fi connections, Bluetooth activity and other available artifacts. The available evidence may vary significantly depending on the nature of the investigation and the configuration of the device.

ISBN: 978-93-49468-02-3

- **Encryption and Security Challenges in Mobile Forensics**

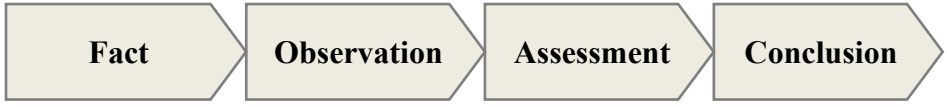
Major challenges in mobile forensics include device encryption, screen locks, biometric authentication, secure hardware, and application-level encryption. Modern smartphones prioritize security, making it technically difficult for investigators to access the data on the device.Apart from this, cloud synchronization also complicates the investigation. A complete version of the information available on the device may sometimes reside in a cloud account or an associated service. In such cases, it becomes important to obtain relevant records in accordance with the applicable legal authority and appropriate procedures.

OSINT in Cybercrime Investigation

OSINT stands for Open-Source Intelligence means which collects and analyse data from public sources to produce intelligence. The primary use of OSINT in national security, law enforcement, and business intelligence and is to answer classified, unclassified, or proprietary intelligence requirements. *Common sources include:*

- Search Engines
- Public Websites
- Social Media Platforms
- Public Record
- Domain Information
- News Reports
- Public Repositories

OSINT investigations have an important distinction to maintain. The following flow chat shown below:



For example: If the same username is found on two public profiles, that is merely an observation. Based on this observation, it does not conclude immediately that same usernames belong to one person. Some additional indicators are examined:

- Username reuse
- Profile images
- Posting Pattern
- Associate websites
- Contact Identifiers

ISBN: 978-93-49468-02-3

Evidence Preservation

The role of evidence preservation is the most crucial partin cybercrime investigation because digital evidence can be altered, modified or remotely modified, and overwrite. When there is a legitimate risk of relevant data disappearing, evidence preservation should begin as early as reasonably possible. In cybercrime cases, evidence can exist in various forms such as, mobile phones, computers, hard-drives, USB devices, memory cards, CCTV footage, emails, social media content, chat records, server logs, cloud data, IP records, and financial transaction records. Investigators must first determine which data is relevant to the investigation and identify which pieces of evidence might be volatile or time sensitive. Key elements in the evidence preservation process include identification, documentation, secure collection, acquisition, storage, and access control. Unnecessary interaction with digital devices should be avoided, as certain activities performed on them could alter the evidence. In the cases, a forensic copy is created through forensic acquisition, enabling examination to be conducted without directly modifying the original evidence.

Cryptographic hash values are used to verify the integrity of the evidence or forensic images; the hash value is generated from the digital representation of the evidence and aids in subsequent verification. Along with the evidence, associated metadata, timestamps, acquisition details, and relevant technical information must also be properly documented. The importance of preservation becomes even greater in cases involving social media. Social media posts, messages, account information, server logs, or other online records can be deleted, modified, or expire over time. Therefore, timely preservation requests or other appropriate measures are considered in accordance with applicable legal procedures. Evidence preservation should be considered closely connected to the chain of custody. Preservation protects the evidence, whereas the chain of custody maintains a documented record of its movement and handling—from collection through to examination and presentation. Ultimately, the objective of evidence preservation is not merely to save digital data. Its aim is to ensure that the evidence remains appropriately protected against alteration, loss, contamination, or unauthorized access during the investigation, and that its integrity and reliability can be demonstrated during subsequent examination or judicial proceedings.

Chain of Custody

Chain of custody is the most essential process in every investigation for evidence documented. Chain of custody refers to maintaining a complete, documented history of the evidence—from its collection through to its examination and presentation. The main purpose is to demonstrate that the evidence being presented later is the same evidence that was originally collected, and that its integrity has been maintained or not. The chain of custody proves the integrity of a

ISBN: 978-93-49468-02-3

piece of evidence. Basic workflow of Chain of Custody - Collection, Examination, Analysis, Reporting. Example–If a mobile phone is seized during a cybercrime investigation, the investigator must document on the device like manufacture, model, IMEI, physical condition, power status, seizure location, date, and time. Subsequently, the device is placed in appropriate packaging and secure storage to prevent tampering. Details regarding the handover and receipt are recorded when the device is submitted to the forensic laboratory. During the forensic examination, the acquisition methodology and integrity validation information are also documented. Chain of custody is not merely an administrative formality; it is a crucial investigative mechanism that supports the reliable, integrity, and evidentiary value of digital evidence.

Legal Framework within India

Cybercrime investigation in India does not operate under a single law. Depends on the nature and circumstances of the cybercrime, legal, frameworks such as Information Technology (IT) Act 2000, Bharatiya Nyaya Sanhita, 2023 (BNS), Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and Bharatiya Sakshya Adhiniyam, 2023 (BSA) plays a significant role. Apart from these, other special laws, rules, and regulations also apply in specific cases.

- **Information Technology Act**

The Information Technology Act, 2000 in India is the primary legislation that addresses digital records, digital transactions, and various cyber-related offences and contraventions. The IT Act grants legal recognition to digital records and, in certain circumstances, can also apply to offences committed in outside of India. In the context of cybercrime investigation, the provisions of the IT Act are relevant in areas such as unauthorized access, computer-related offences, identity theft related offences, digital records, intermediary responsibilities, and examination of digital devices. Identifying the relevant section of the IT Act and proving the offense are two different things.

Essence of Information Technology Act

- IT Act 2000 addressed the following issues:
  - Legal recognition of electronic documents.
  - Legal recognition of digital signature
  - Offenses and Contraventions
  - Justice dispensation system for cybercrimes.
- ITAA. 2008 is often referred as the enhanced version of IT Act, 2000 as it additionally focused on Information Security.
- Several new sections on offences like cyber terrorism, data protection was added in ITAA, 2008.

ISBN: 978-93-49468-02-3

- **Information Technology Act Amended**

India introduced major changes to the Information Technology Act, 2000, to address emerging challenges. These changes were implemented through the Information Technology (Amendment) Act, 2008. The IT Amendment Act, 2008 significantly expanded India's cyber law framework and strengthened the legal provisions regarding electronic transactions, various types of cyber offences, data security, intermediary liability, and government powers. The Information Technology (Amendment) Act, 2008 was a major legislative amendment to the Information Technology Act, 2000. The amendments have played a significant role in updating India's cyber law framework to keep pace with the rapidly evolving digital environment this includes;

  - Legally addressing the emerging cybercrimes
  - Strengthening the data protection and information security
  - Defining the legal responsibilities of intermediaries
  - To specifically address the serious crimes like cyber terrorism
  - Providing stronger provisions against online obscenity and sexually explicit content.
  - Strengthening legal powers for cyber investigations

- **Bharatiya Nyaya Sanhita**

The Bharatiya Nyaya Sanhita, 2023 is the new criminal code of India. It came into effect on 01 July 2024, after being passed by the Parliament in December 2023, replacing the Indian Penal Code of 1860. In cases of conventional offences using digital technologies such as cheating, criminal intimidation, forgery, stalking, or other offences—the relevant provisions of the BNS may apply depending on the facts. It is important for a cybercrime investigator to understand that not every cybercrime falls solely under the Information Technology Act, 2000.

Depending on the facts of the case, provisions of both the BNS and the IT Act may be relevant. The investigator must first identify the actual criminal conduct, then determine the applicable legal provisions, and subsequently establish the case using the available digital evidence.

- **BNS and Digital Evidence**

The BNS primarily establishes what constitutes a criminal offence, whereas the Bharatiya Sakshya Adhiniyam, 2023 (BSA) is relevant regarding the evidentiary treatment of digital footprints. Similarly, the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) is important for criminal investigation and procedure. Cybercrime investigation can be broadly understood as follows; BNS – What is an Offence?BNSS – How will the investigations and procedures be conducted?

ISBN: 978-93-49468-02-3

BSA – How will the evidence be established?IT Act –Technology/cyber-specific provisions.

- **Bharatiya Nagarik Suraksha Sanhita**

The Bharatiya Nagarik Suraksha Sanhita, 2023 provides the framework for criminal investigation and procedure. Procedural requirements concerning complaints/FIRs, investigations, search and seizure, statements, investigation-related procedures, and court proceedings are relevant to cybercrime investigations. Proper compliance with procedural safeguards during the seizure or investigation of digital devices is crucial, as the process of collecting evidence is just as important as the reliability of the evidence itself.

- **Bharatiya Sakshya Adhiniyam**

The Bharatiya Sakshya Adhiniyam, 2023 is significant in cybercrime cases because electronic and digital records frequently serve as a major source of evidence in modern investigations. The BSA recognizes the electronics and digital records within the evidentiary framework. In the framework of BSA, emails, server logs, computer/laptop records, smartphones, data, messages, websites, location-related digital information, and other digital records are important evidence. Therefore, for an investigator, merely collecting digital evidence is not enough; it is also essential to properly document the source, method of acquisition, integrity, and preservation of the evidence, as well as the applicable evidentiary requirements.

- **Digital Evidence under BSA**

In modern criminal investigation, electronic evidence often becomes a central component. For instance, in an online fraud case where victim receives a message from unknown number, the investigator does not merely gather screenshots; the investigation also involves examining records like, device information, account details, timestamps, session logs, and other support evidence. The objective of this approach is to establish the source of the evidence, determine whether the evidence genuine or not, and ascertain the connection of the available evidence to the accused or the incident.

Forensic Examination of Digital Evidence

In cybercrime investigations, the scientific examination of electronic evidence is crucial. Section 79A of the IT Act provides a framework for the central government to notify specific departments, bodies, or agencies as 'Examiners of Electronic Evidence' for the purpose of obtaining expert opinions on evidence in electronic form. The practical significance of this is that technically complex digital evidence is examined and explained by forensic experts. The recovery of deleted and hidden data is also crucial components of digital forensics.While suspect may delete files, but recoverable artifacts often remain on storage media or within the application databases under certain circumstances. Forensic examiners can use available

ISBN: 978-93-49468-02-3

techniques to identify deleted, fragmented, or hidden information. Recovered data is not automatically considered complete or an authentic conclusion until its integrity and context are evaluated alongside additional evidence. The final stage of a forensic examination involves analysis, interpretation, and reporting. The forensic examiner must clearly document technical findings and distinguish facts from assumptions so that the report can clearly outline the acquisition methodology, tools, and techniques used, relevant findings hash verification where applicable, limitations, and conclusion.

Common Challenges of Cybercrime Investigations

Investigators always face numerous technical, legal, and practical challenges during cybercrime investigations. One of the biggest challenges is anonymity and attribution, as criminals use VPNs, proxies, Tor networks, fake identities, and compromised accounts to hide their actual identities and locations. It is difficult to conclusively establish an individual's identity based solely on an IP address, username, or online profile, especially when shared networks, public Wi-Fi, NAT, or stolen credentials are involved. Furthermore, encryption and secure communication technologies make it challenging for investigators to access digital evidence. Another significant challenge in cybercrime is the volatile nature of data; it can be deleted, modified, overwritten, or remotely removed. Social media posts, account information, and server logs become unavailable after a limited period, necessitating timely preservation. Cross-border jurisdiction also complicates investigations, particularly when the victim, suspect, service provider, and server are in different countries. Such cases require additional procedures to secure legal cooperation and obtain information. At the same time, rapidly evolving technology, cloud services, cryptocurrency, AI-generated content, and multiple digital identities are creating new challenges for investigators. In cybercrime investigation, it is crucial to corroborate technical findings with independent sources, maintain the integrity of evidence, and clearly distinguish facts from assumptions.

Future of Cybercrime Investigation

There is a possibility that cybercrime investigations will become complex in the future because technologies are developing rapidly. Important technologies include:

- Artificial Intelligence
- Deep fakes
- Internet of Things
- Cloud Computing
- Cryptocurrency
- Metaverse Technologies
- Autonomous Systems

ISBN: 978-93-49468-02-3

Future cybercrime investigators will need interdisciplinary knowledge. Law + Digital Forensics + Cybersecurity + OSINT + Data Analysis + Intelligence + Evidence Management, Artificial Intelligence and Machine Learning will play a crucial role in future cybercrime investigations. AI-based systems can assist investigators in analysing vast amounts of digital evidence, identifying suspicious patterns, reconstructing digital timelines, and establishing connections between various accounts, devices, and transactions. However, AI outputs cannot automatically be treated as conclusive evidence; it will be essential to verify every significant finding through human expertise, forensic validation, and independent corroboration. In future, investigating AI-generated content and Deep fakes will also become a major challenge. Because of fake videos, manipulated images, and synthetic voices, distinguishing between genuine and fabricated content could prove difficult. Investigators will need to analyse media provenance, metadata, audio-video consistency, compression patterns, and other forensic indicators.

However, detecting signs of manipulation in content and conclusively identifying the creator of that manipulation will be two distinct investigative questions. Cloud forensics and IoT forensics will also become important components of future investigations. In today's digital environment, information is not stored solely on a single computer or mobile phone but is distributed across cloud platforms, applications, connected devices, and multiple servers. Therefore, investigators must develop the expertise to identify, obtain, and preserve digital evidence from cloud infrastructure and IoT ecosystems through appropriate legal procedures. With the increasing use of cryptocurrency and digital assets, the importance of blockchain analysis will also grow. Investigators can understand the movement of funds by tracing blockchain transactions and analyse relationships between different wallet addresses. However, linking a specific blockchain address directly to a real-world individual requires additional corroborative evidence.

In the future, cybercrime investigations will shift towards real time and proactive intelligence. Investigations will not be limited merely to collecting evidence after a crime has occurred; instead, efforts can be made to identify potential cyber threats at an early stage by leveraging threat intelligence, suspicious behaviour patterns, fraud indicators, and information-sharing mechanisms. International cooperation will also be a major component of future cybercrime investigations. Cybercrimes often span multiple countries—with the victim in one country, the suspect in another, and the digital infrastructure located in a third. In such cases, cooperation among law enforcement agencies, technology companies, financial institutions, and international bodies will be crucial for obtaining digital evidence and tracing criminal networks.

ISBN: 978-93-49468-02-3

Conclusion

Thus, Cybercrime investigation is a multidisciplinary process that is not limited to technical knowledge only. However, a successful investigation requires a combination of digital forensics, OSINT, network analysis, financial investigation, evidence preservation, legal procedures, intelligence analysis, and professional reporting. The central principle of cybercrime investigation states that digital evidence should be relevant, reliable, properly obtained, properly preserved, and properly explainable. An IP address only does not establish a suspect's identity. A screenshot only does not prove account ownership. Only username does not prove identity. Similarly, facial resemblance solely is not conclusive proof that two individuals are the same person. It is essential to evaluate every piece of digital evidence within its context and, wherever possible, corroborate it using multiple independent sources. As cybercrime evolves, investigators must continuously update their technical capabilities. At the same time, maintaining legal safeguards, privacy principles, evidence integrity, and investigative neutrality will remain equally important. Ultimately, the objective of a cybercrime investigation is not merely to uncover digital traces. The main goal is to transform those traces into reliable, properly documented, and legally obtained evidence capable of withstanding professional and judicial scrutiny.

References

1. Information Technology Act, 2000.
2. National Cyber Crime Reporting Portal, Ministry of Home Affairs, Government of India.
3. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India.
4. National Investigation Agency, Ministry of Home Affairs, Government of India — Cyber Terrorism and related National Security Investigations.
5. Ministry of Electronics and Information Technology, Government of India.
6. Indian Computer Emergency Response Team. Digital Threat Report 2025–26. Ministry of Electronics and Information Technology, Government of India.
7. Indian Computer Emergency Response Team. CERT-In Advisories – 2026. Ministry of Electronics and Information Technology, Government of India.

ISBN: 978-93-49468-02-3