Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Role of Cyber Forensic in Crime Investigation

Munira M. Rampurawala*
Department of Computer Science, Dr. D.Y. Patil Arts,
Commerce and Science College,
Pimpri, Pune, Maharashtra, India

Anjali R. Vairagar
Department of Computer Science, Dr. D.Y. Patil Arts,
Commerce and Science College,
Pimpri, Pune, Maharashtra, India

Abstract - Cyber forensics, also known as computer forensics is a branch of digital forensic science focused on finding, preserving, analyzing and presenting digital evidence stored in computers and other electronic devices. Its main goal is to conduct legally sound investigations. This ensures that digital evidence remains reliable, authentic and can be used in courts. While cyber forensics is often linked to cybercrime investigations, it also plays an important role in civil disputes and regulatory cases where digital data acts as vital evidence. With rapid technological advancements the nature and scale of cybercrime have grown significantly, and traditional investigative methods have become less effective. The widespread use of digital systems in daily life and business has opened up new opportunities for cyber abuse and criminal exploitation. Many modern crimes are either fully based on technology or evolved versions of traditional offenses. In this context, cyber forensic science has become essential to the criminal justice system. It allows for faster, more accurate and efficient investigations. This research paper looks at the importance of cyber forensics in criminal and legal investigations, especially focusing on cyber forensic practices in India. It also highlights the need for ongoing research to tackle new cyber threats in our changing digital world.

Keywords : ***Cyber Forensics, Digital Forensic Science, Cyber Crime Investigation, Cyber Forensic Investigation Techniques, Cyber Crime Detection, Criminal Justice in India, Cyber Laws in India, Technology-Driven Crimes, Cyber Security and Forensics.***

1. INTRODUCTION :

Cyber forensics also known as digital forensics, involves identifying, collecting, preserving, analyzing and presenting electronic evidence to investigate cybercrimes. It combines ideas from computer science, cybersecurity, criminal investigation and law. This makes it essential for modern crime investigations because of the fast growth of digital technologies.

Today people use digital devices like computers, smartphones, cloud platforms and network systems in their daily lives. Because of this many criminal activities leave digital traces that can be examined during investigations. Cyber forensics allows investigators to recover and analyze this evidence using specialized tools while keeping it intact for legal proceedings.

Key aspects of cyber forensics include:

- Collecting and preserving digital evidence such as emails, system logs, browsing history, financial transactions and deleted files.
- Investigating cybercrimes, including malware attacks, ransomware, phishing and Advanced Persistent Threats (APTs).
- Analyzing data generated by new technologies like blockchain, digital currencies and the Internet of Things (IoT).
- Maintaining a proper chain of custody to ensure evidence is admissible in court.
- Assisting law enforcement authorities and the criminal justice system in uncovering the truth and ensuring lawful proceedings.

Cyber forensic professionals must have technical skills, analytical abilities, cybersecurity knowledge and an understanding of legal procedures. They face challenges such as dealing with encrypted data, password-protected systems, hidden or deleted files and analyzing large amounts of digital information under tight deadlines. Despite these challenges cyber forensics is crucial for detecting cyber threats, preventing future attacks and ensuring reliable digital evidence is presented in court.

2. LITERATURE REVIEW :

The rapid growth of digital technology and the widespread use of the internet have changed the nature of crime. Many traditional crimes now include digital elements, while new types of cybercrime have emerged, such as hacking, online fraud, identity theft and cyberstalking. In this changing landscape, cyber forensics or digital forensics, has become crucial for modern crime investigation. Cyber forensics involves systematically identifying, collecting, preserving, analyzing and presenting digital evidence in a way that ensures it is reliable and can be used in court. Previous research shows the vital role of cyber forensics in discovering digital evidence from computers, mobile devices, networks and online platforms. Scholars explain that cyber forensics is a structured investigative process that focuses on keeping a record of evidence and preventing data alteration or

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

tampering. Following established forensic standards is important. If proper procedures are not followed, digital evidence may be challenged or rejected in court, making it harder to prosecute cases.

The literature also highlights how effective cyber forensics is in finding and solving cybercrimes. Digital forensic techniques allow investigators to recover deleted data, analyze system logs, trace IP addresses, examine emails and recreate digital crime scenes. Studies show that cybercriminals often leave behind digital traces, which can be detected through forensic analysis. Therefore, cyber forensics is key to identifying suspects, establishing timelines and connecting digital activities to criminal actions. Another important theme in current studies is the rising need for specialized technical skills. Researchers argue that investigators must have a strong understanding of computer systems, networks, encryption methods and malware analysis. As criminals increasingly use advanced tools like encryption and anonymization techniques, cyber investigations have grown more complicated. Continuous training, modern forensic tools and effective teamwork between investigators, forensic experts and legal authorities are essential.

Legal and ethical issues related to cyber forensics have also received a lot of attention. Concerns about privacy, jurisdictional conflicts, and differences in cyber laws across countries present significant challenges. Since digital evidence often crosses borders, accessing data stored on foreign servers can be challenging. Researchers emphasize the importance of stronger legal frameworks and better international cooperation to ensure legal and effective evidence collection.

Despite extensive research, gaps still exist in the literature. Limited focus has been placed on forensic investigations involving new technologies like cloud computing, Internet of Things (IoT) devices and encrypted communication platforms. Additionally, there is a lack of universally accepted forensic standards and a need for structured training programs, especially in developing countries. Overall, while cyber forensics is widely seen as essential to modern crime investigation, more research is needed to tackle technological, legal and capacity-building challenges.

3. RESEARCH METHODOLOGY :

The present study aims to analyze the role of cyber forensics in contemporary crime investigation. With the rapid growth of technology, cybercrimes are increasing steadily, making digital evidence a crucial part of criminal investigations. This research focuses on understanding how cyber forensic techniques help in identifying, collecting, preserving, and presenting digital evidence in a manner that is legally acceptable in courts. A qualitative research approach has been adopted for this study, as the objective is to understand the concepts, methods and practical applications of cyber forensics rather than dealing with numerical data. The study is mainly based on secondary data. Information has been gathered from reliable and authentic sources such as research papers, academic journals, books, government reports, cybercrime case studies, legal documents and trusted websites related to cybersecurity and digital forensics. These sources helped in developing a clear understanding of forensic tools, investigation procedures, and the practical role of cyber forensics in solving crimes. The collected data has been analyzed using descriptive and comparative methods. Various research studies and case examples were reviewed and compared to identify common findings, challenges and recent developments in the field of cyber forensics. The analysis also explains how cyber forensic techniques assist law enforcement agencies in tracing cybercriminals, recovering deleted or hidden data, examining digital devices, and presenting digital evidence effectively during legal proceedings. Due to time constraints and limited access to professional cyber forensic experts, primary data collection methods such as interviews or surveys were not used. Therefore, the research relies entirely on secondary data analysis. Throughout the research process, proper academic standards were maintained, and all sources were appropriately cited to avoid plagiarism and ensure ethical research practices. The study has certain limitations. Since it is based on secondary data, it does not include real-time investigation experiences or direct interaction with forensic professionals. Access to confidential case information was also restricted. Despite these limitations, the study provides valuable insights into the significant role of cyber forensics in crime investigation and highlights its growing importance in the digital age.

4. TYPES OF CYBER CRIMES IN INDIA :

The rapid growth of digital technologies, internet connectivity, online banking and e-governance services has significantly raised the risk of cybercrimes in India. As the country shifts toward a digital economy, cybercriminals are taking advantage of technological weaknesses to carry out sophisticated crimes. Cybercrime refers to illegal activities conducted via computers, digital devices or networks. The major types of cybercrimes common in India are summarized below:

i. Hacking and Unauthorized Access :

Hacking involves illegal access to computer systems, servers or networks to steal, change or destroy data. Attackers often take advantage of security gaps in websites, databases or

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

organizational networks. In India, both government and private organizations have experienced hacking incidents, leading to data breaches, financial losses and reputational damage.

ii. Phishing and Online Financial Fraud :

Phishing is one of the most common cybercrimes in India. Criminals pretend to be trusted entities like banks, government agencies or e-commerce platforms to trick individuals into disclosing sensitive information such as OTPs, passwords, card details or UPI credentials. With the quick rise of digital payments and mobile banking, online financial fraud has increased. Fake emails, SMS messages and cloned websites are often used to deceive victims.

iii. Identity Theft :

Identity theft involves the unauthorized use of personal information. In India, cases of improper use of Aadhaar numbers, PAN details, banking information and social media accounts are on the rise. Offenders may create fake profiles, apply for loans or engage in illegal activities using stolen identities, causing financial losses and reputational harm to victims.

iv. Ransomware Attacks :

Ransomware is malicious software that limits access to data and demands payment for restoration. Indian hospitals, schools and businesses have increasingly been targeted. These attacks disrupt vital services and lead to significant financial damage. Payments are often requested in cryptocurrency to prevent tracking.

v. Cyber Terrorism :

Cyber terrorism uses digital platforms to threaten national security, promote extremist ideology, or disrupt critical infrastructure such as banking systems, power grids and government services. This act is considered a serious crime under the Information Technology Act, 2000, as it seeks to create fear, instability and social disruption.

vi. Social Media Crimes :

The widespread use of social media has given rise to crimes like cyberbullying, harassment, stalking, defamation, and the spread of misinformation. Fake news and deepfake content present new challenges. These crimes particularly impact women and young users, raising worries about online safety and privacy.

5. STEPS INVOLVED IN CYBERCRIME INVESTIGATION :

In today's digital India, technology is advancing rapidly. With this growth comes an increase in tech-related crimes. Many cases fall under the IT Act of 2008, which was updated in 2010. Some of these cases include data theft, hacking, unauthorized access, adult content, intellectual property theft, cyber terrorism and viruses. Cybercrime poses a serious threat to businesses, national security and individuals.

The following outlines the process of cybercrime investigation.

1. Questioning :-

The first step is to gather information about the crime. Investigators must determine why it happened, who committed it and how to proceed with the investigation.

2. Gathering Information :-

This involves monitoring webcams, wiretaps and sometimes obtaining evidence from the hacker's computers.

3. Computer Forensics :-

After questioning and gathering information, forensic tools are used to collect evidence. The evidence must be preserved carefully, as it will be presented in court.

Methods of cybercrime investigation include:

- Identifying suspects
- Tracking IP addresses
- Analyzing web server logs
- Tracking email accounts
- Attempting to recover deleted evidence
- Cracking passwords
- Searching for hidden data

A computer forensic investigator must follow specific methodologies to uncover the truth.

They must adhere to certain procedures to maintain the integrity of the evidence. It is crucial to collect evidence without disrupting the chain of custody. Once the evidence is collected, the original data should be kept secure, with work done on copies. The integrity of the data must be upheld by the forensic examiner. They should follow established steps when investigating cyber-related cases. The investigation process should protect the reputation of the examiner and the organization involved.

6. DIGITAL EVIDENCE & ITS LEGAL VALIDITY IN INDIA :

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

After explaining cybercrime investigation procedures, it is important to consider whether the collected digital evidence can be used in Indian courts. In India, evidence only holds value if it meets certain legal standards. Thus, understanding the legal validity of digital evidence links cyber forensic practices with acceptance in court.

Meaning of Digital Evidence :-

- Digital evidence refers to any data that is stored, created or transmitted electronically and can support or challenge facts in court.
- Unlike physical evidence, digital evidence is intangible and exists in devices like computers, smartphones, servers, networks and cloud platforms.
- It is very sensitive and can be easily altered, deleted or manipulated.
- Proper collection, preservation, and presentation are crucial to maintain authenticity and integrity.

Role in Cybercrime Investigations :-

Digital evidence helps with :

- Establishing timelines
- Identifying suspects
- Proving intent

Types of Digital Evidence :-

a. Emails and Electronic Communications :

Emails, chats, social media messages and instant messaging records. They help prove communication, intent and involvement in crimes.

b. Log Files :

System logs, server logs, firewall logs and application logs. These are used to trace unauthorized access and reconstruct cyber incidents.

c. CCTV and Video Recordings :

Digital surveillance footage stored electronically. This footage is commonly used in criminal investigations.

d. Mobile Device Data :

Call Detail Records (CDRs), SMS, WhatsApp chats, GPS location, photos, videos and app data. This data is useful in both cyber and traditional crimes.

e. Cloud and Online Data :

Emails, documents, backups and logs stored on cloud platforms. This type of data is increasingly important in modern investigations.

All types of evidence must be collected with the right forensic tools to ensure reliability.

Section 65B of the Indian Evidence Act

- This is the main legal provision governing electronic evidence in India.
- Electronic records, whether printed or stored on optical or magnetic media can be used in court if certain conditions are met.
- It requires a Section 65B Certificate, which must :
  - Identify the electronic record
  - Explain how it was produced
  - Provide device details
  - Confirm the device was functioning properly
- Without this certificate, electronic evidence is usually not admissible, except under special judicial circumstances.
- This ensures the authenticity and reliability of electronic records.

Information Technology (IT) Act, 2000

- This act gives legal recognition to electronic records and digital signatures.
- It establishes the legal framework for cybercrimes.
- The 2008 amendment strengthened provisions related to :
  - Data protection
  - Cyber terrorism
  - Intermediary liability

It works alongside the Indian Evidence. Act to support the validity of electronic evidence.

Judicial Interpretation

- Indian courts have stressed the need for strict compliance with Section 65B.
- Courts require valid certification to prevent fabrication and tampering.
- Judicial interpretation has evolved to balance technical requirements with justice, especially when obtaining certificates is challenging.
- This reflects a growing acceptance of digital evidence while ensuring safeguards are in place.

Challenges in Indian Courts :-

a. Lack of Technical Awareness :

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Judges, lawyers and investigators may not have the expertise needed to handle digital evidence.

b. Improper Handling of Evidence :

Not following forensic procedures can impact admissibility.

c. Section 65B Compliance Issues :

Mistakes in obtaining or drafting certificates often lead to rejection.

d. Risk of Tampering :

Digital data can be altered if it is not preserved properly.

e. Jurisdictional Problems :

Cloud data stored outside India creates procedural difficulties.

7. Tools & Techniques Used in Cyber Forensic :

The tools and techniques used by cyber forensic analysts focus on examining data, whether it is encrypted, deleted or hidden. Analysts apply various tools based on the situation and the nature of the case. These tools help produce evidence for court.

i. X-Ways Forensics:

This is a Windows-based licensed software (32-bit and 64-bit) that offers flexible and customizable search options. It is portable, cost-effective and efficient. It mainly helps recover deleted, corrupted and digital camera files.

ii. SLEUTH KIT:

This tool works on UNIX and Windows systems. It is used to analyze disk images, examine file systems deeply, recover files and assist in autopsy processes.

iii. SIFT (SANS Investigative Forensic Toolkit):

This is a free, open-source toolkit that includes essential investigation tools. It converts evidence into a read-only format to prevent alteration and supports malware analysis and indicators of compromise.

iv. EnCase:

This is a multipurpose tool that collects and examines active, latent and archival data without modifying it. It generates reports that can be used in court and supports encryption for secure data handling.

v. CAINE (Computer Aided Investigative Environment):

Built on Ubuntu Linux, it integrates various forensic tools and produces semi-automated reports. It conducts investigations in four phases and recovers deleted, damaged or virus-affected files.

vi. Forensic Toolkit (FTK):

This tool examines different data types, recovers deleted emails and content strings, decrypts encrypted data and saves digital images in various formats for reconstruction.

CYBER FORENSIC TECHNIQUES

- Cross-driven analysis:

This technique collects and analyzes data from multiple sources to manage large volumes of information.

- Live analysis:

This method examines a running system to bypass encryption and locate data sources.

- Deleted file recovery:

This process retrieves deleted files and other useful investigation data.

- Stochastic forensics:

This technique detects insider data theft that is hard to identify.

- Steganography:

This method identifies hidden messages embedded in images, text or videos.

8. CHALLENGES IN CYBER FORENSICS INVESTIGATION :

Rapid changes in technology have created significant challenges for traditional forensic science especially in cyber forensics. While modern technology improves investigative tools, it also makes collecting, analyzing and presenting digital evidence legally more complex.

Major challenges in cyber forensic investigations include:

i. Admissibility of Digital Evidence:

Proving that digital evidence is authentic and intact in court is hard. This kind of evidence can be easily changed or tampered with, which demands strict handling procedures and expert testimony. Fast technological changes make proper evidence collection and validation even trickier.

ii. Advancement of Encryption:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Current encryption techniques protect digital communications and data but also limit forensic access. Encrypted files and messages often hold key evidence, but decrypting them needs advanced knowledge, time, and legal permission.

iii. Anti-Forensic Techniques:

Cybercriminals use anti-forensic methods to hide, change, or destroy digital data. These techniques make it tough for investigators to find data sources and can make important evidence impossible to recover.

iv. Lack of Standardization:

Ongoing technological changes make it hard to set uniform forensic standards. Some guidelines exist, like those from NIST, but frequent updates are needed, which leads to inconsistencies in investigative practices.

v. Data Collection and Preservation Issues:

Digital evidence might differ between what's shown on a screen and what's stored on a disk. Metadata like timestamps can be faked or changed. Timelines may be unclear, and ISP caching can hide the original source of web content.

9. ROLE OF CYBER FORENSIC IN THE CRIMINAL JUSTICE SYSTEM :

Cyber forensics plays a key role in improving the modern criminal justice system. This is especially true as crimes increasingly involve digital devices, networks and online platforms. Research shows that electronic evidence is now essential for both cybercrime cases and traditional crimes where digital traces exist.

Key Roles of Cyber Forensics:

i. Identification and Collection of Digital Evidence :

Cyber forensic experts identify, collect and preserve digital evidence from computers, mobile devices, servers, cloud platforms and network systems. Research highlights that using proper evidence collection techniques helps keep data intact and avoids contamination.

ii. Preservation of Evidence Integrity:

Studies emphasize the need to maintain the chain of custody to ensure that digital evidence remains genuine and acceptable in court. Hash values, forensic imaging and write-blocking tools are common methods highlighted in research to ensure data reliability.

iii. Analysis and Reconstruction of Events :

Cyber forensics allows investigators to rebuild timelines, track communications, recover deleted files and analyze metadata. Research papers state that this analysis helps establish intent, identify suspects and clarify the sequence of criminal activities.

iv. Expert Testimony in Court :

Digital forensic experts provide technical explanations and opinions during trials. Their testimony helps judges and juries understand complex digital evidence. Scholarly works point out that expert interpretation is vital for meeting courtroom evidence standards.

v. Support to Law Enforcement and Prosecution :

Cyber forensics aids law enforcement agencies by delivering scientifically validated findings. It strengthens prosecution cases by presenting objective, verifiable digital proof.

vi. Protection of Legal Rights :

Research also shows that cyber forensics safeguards the rights of both victims and accused individuals by ensuring that investigations follow evidence-based practices and legal procedures.

10. CONCLUSION :

In today's digital world, nearly every activity leaves an electronic trace. As technology grows, cybercrimes like hacking, phishing, identity theft and ransomware are rising quickly in India. Traditional investigation methods alone can't handle these technology-driven crimes. This study shows that cyber forensics has become a vital tool in modern crime investigation.

The research looked into the concept, goals, and scope of cyber forensics, along with the steps involved in investigating cyber crime. Proper identification, collection, preservation and analysis of digital evidence are essential for ensuring its authenticity and admissibility in court. Legal rules like Section 65B of the Indian Evidence Act and the Information Technology Act, 2000 play an important role in validating electronic evidence. When handled correctly, digital records like emails, log files, mobile data and cloud information can strongly support prosecution and court decisions.

The study also covered key forensic tools and techniques used to recover deleted, hidden or encrypted data. The case study showed how mobile applications can keep valuable location and timestamp data that may serve as critical evidence.

However, challenges such as encryption, anti-forensic techniques, lack of standardization and limited technical knowledge still exist. Therefore, ongoing research, training and legal awareness are necessary. Overall, cyber forensics

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

greatly strengthens the criminal justice system by ensuring that digital evidence is reliable, scientific and legally sound.

11. REFERENCE :

[1] Agarwal, A., Gupta, M., & Gupta, S. (2011). Systematic digital forensic investigation model. International Journal of Computer Science and Security, 5(1), 118-131.
[2] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the Internet (3rd ed.). Academic Press.
[3] International Journal of Law Management & Humanities. (n.d.). International Journal of Law Management & Humanities. https://ijlmh.com
[4] International Journal of Scientific Research in Engineering and Management. (n.d.). International Journal of Scientific Research in Engineering and Management (IJSREM). https://ijsrem.com
[5] Kaur, R., & Kaur, K. (2020). Role of cyber forensics in investigation of cyber crimes. International Journal of Law Management & Humanities, 3(4), 1456-1465.
[6] National Institute of Standards and Technology. (2014). Guide to integrating forensic techniques into incident response (Special Publication 800-86). NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
[7] Solanki, V. K., & Rao, S. (2018). Digital forensics and cyber crime investigation in India. International Journal of Advanced Research in Computer Science, 9(1), 221-225.
[8] The Information Technology Act, 2000 (India).
[9] The Indian Evidence Act, 1872, § 65B (India).