AG Publishing House

Investigative Frontiers Integration of Science Transforming Criminal Investigation

Year: 2026

Hunting Criminals in Cyberspace: Investigative Strategies for the Digital Era

Mr. Tejas D Vodeyar[1]

[1]*Forensic Expert Forensic Science Academay, Tirupati, Andhra Pradesh*

Abstract

The digital technologies, interdependencies, and Internet services are rapidly expanding, creating a serious challenge for cybercrime. This review provides an overview of the evolving cybercrime environment and the investigative methods used to detect, investigate, analyze, and prosecute cyber criminals in the digital age. It covers common types of cybercrime, the digital investigation process, and how digital forensics can be used to collect, preserve and analyze digital evidence. The review also emphasizes on new investigation techniques such as Open Source Intelligence (OSINT), Network and Malware Analysis, Artificial Intelligence and international cooperation in the context of Indian cybercrime environment. Also, it provides solutions to key issues like privacy, cloud computing, anonymous communication and jurisdiction. The review identifies the need for the adoption of innovative forensic tools, the use of standardized investigation protocols, and the collaboration between countries to improve cybercrime investigations and digital justice.

Keywords; Cybercrime Investigation; Digital Forensics; Digital Evidence; Open-Source Intelligence (OSINT); Cybersecurity.

[1] ISBN No. - 978-93-7640-081-2

1 Introduction

Digital technology has changed the world and revolutionised how modern society communicates, buys and sells, learns, goes to doctors, and accesses public services. The Internet, cloud computing, mobile devices, social media networks and the Internet of Things (IoT) have fostered an interconnected digital environment that enables economic and social development worldwide. The technological evolution also allowed the criminals more opportunities for crime, thus leading to more advanced types of cybercrime. While most early cybercrime was to break into computer systems or to simply distribute malware, today's cybercrime includes ransomware, phishing, identity theft, financial fraud, cyber espionage, distributed denial-of-service (DDoS) attacks, and attacks on critical infrastructure. Cybercrime is one of the fastest growing threats to governments, businesses and consumers everywhere, as cybercriminals continue to take advantage of new technology and new vulnerabilities.[2]

Hunting Criminals in Cyberspace is the process of systematically identifying, tracking, analyzing and prosecuting an offender in a digital environment. Cybercrime investigations differ from traditional policing in that a large portion of the investigation involves collecting digital evidence such as system logs, network traffic, email, cloud data, mobile devices, and online communications. Digital forensics, open-source intelligence (OSINT), threat intelligence, and network analysis are used by investigators to recreate crime scenarios, identify the culprit and provide compelling evidence that can be presented in court. The use of anonymity tools, encryption, and decentralized communication platforms by cybercriminals continues to grow in complexity, necessitating the application of more advanced investigative strategies and technologies to effectively combat them.[3]

Cybercrime investigation plays an important role in the protection of national security, economic stability, organizational assets and individual privacy. Cyber investigations serve governments in the fight against cyber terrorism, espionage, and attacks on critical infrastructure, and organizations to minimize financial loss, recover compromised systems, and maintain customer trust. Investigations erode identity theft, online fraud, cyber harassment and disclosure of

[2] D. Herlisya, “The Evolution of Cybercrime in the Digital Era: Legal and Security Implications,” Tripeco J. Soc. Sci. Humanit., vol. 1, no. 1, pp. 39–47, 2025, doi: 10.54012/jssh.v1i1.632.

[3] A. Mahboubi et al., “Evolving techniques in cyber threat hunting: A systematic review,” J. ofNetwork Comput. Appl., vol. 232, p. 104004, 2024, doi: https://doi.org/10.1016/j.jnca.2024.104004.

personal information on an individual basis. As such, cybercrime investigation is now an integral part of how law enforcement and cybersecurity are run today.[4]

Traditional investigations and cyber investigations have the same goal of identifying offenders and providing the courts with credible evidence, but they differ greatly in the approach to investigation. Traditional investigations are mostly based on physical evidence, biological evidence, witness statements and crime scene analysis. While cyber investigations involve collecting, preserving, analyzing and interpreting digital evidence found across computers, mobile devices, cloud platforms, and global networks, traditional investigations are more likely to rely on communication logs and handwritten notes. In addition, cybercrimes often cross borders and demand cross-border and technical cooperation and specific forensic skills to deal with jurisdictional and technical difficulties.[5]

2 Cybercrime Landscape and Digital Investigation Process

As digital technologies have advanced and grown, the cybercrime ecosystem has developed and matured and has become a complex ecosystem where criminals take advantage of interconnected systems to target for financial gain, espionage, disruption and personal reasons. Cyber crimes can be committed from a distance, anonymously and internationally, and are difficult to detect and prosecute because of the many ways they may occur. With the rise of cloud-based services, online banking, e-commerce, social media platforms and Internet of Things (IoT) devices, the attack surface has expanded and cybercriminals are attacking, individuals, businesses and government entities with greater speed and sophistication than ever before. Therefore, for a successful digital law enforcement and effective prosecution, it is important that the nature of cybercrime is understood and it has to be investigated using a structured approach.[6]

A. Common Forms of Cybercrime

Cybercrime refers to a broad spectrum of crimes that take advantage of digital technologies and communication systems. Phishing is an attack in which a fraudulent email, Web page, or message asks the recipient to provide sensitive information like banking details or login

[4] C. Horan and H. Saiedian, "Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions," J. Cybersecurity Priv., pp. 580–596, 2021, doi: https:// doi.org/10.3390/jcp1040029.

[5] G. K. Ayswariya and A. Rajan, "A Comparative Study on the Difference Between Conventional Crime and Cyber Crime," Int. J. Pure Appl. Math., vol. 119, no. 17, pp. 1451–1464, 2018.

[6] A. Kuzior, I. Tiutiunyk, A. Zielińska, and R. Kelemen, "Cybersecurity and cybercrime: Current trends and threats," J. Int. Stud., vol. 17, no. 2, pp. 220–239, 2024, doi: 10.14254/2071-8330.2024/17-2/12.

credentials. Ransomware is the type of attack that takes a victim's data and holds it for ransom, and can affect important processes and organizations. The crime of identity theft happens when someone illegally acquires your personal information to commit fraud, and financial fraud involves banking fraud with online banks, credit card fraud, cryptocurrency fraud, and business email compromise. Malware is a program designed to steal information, disrupt systems or gain unauthorized entry into systems, such as viruses, worms, spyware and trojans. Cyberstalking is the repeated harassment, intimidation, threat or monitoring of a person using a digital communications platform, often having a psychological impact and breaching privacy.[7]

B. Characteristics of Cybercriminals and Attack Methods

The threats come in all shapes and forms, including individual hackers, organized criminal groups, insiders, and state-sponsored hackers. They are frequently very knowledgeable in their technical skills and utilize software vulnerabilities, poor authentication systems, social engineering and human error to gain access into systems. These attacks are often times executed through several layers of phishing, deployment of malware, stealing credentials, botnets, and anonymous communication networks to maximize the attack's effectiveness while hiding the attacker's identity. Weaker attribution and law enforcement investigations are made even more difficult by the ubiquity of encryption, virtual private networks (VPNs), cryptocurrencies, and the dark web.[8]

C. General Stages of a Cyber Investigation

A systematic cyber investigation generally follows these stages:

i. Incident identification: Detecting and confirming the occurrence of a cyber incident.
ii. Evidence collection: Acquiring volatile and non-volatile digital evidence while maintaining its integrity.
iii. Evidence examination: Recovering, preserving, and organizing digital artefacts using forensic tools.
iv. Evidence analysis: Correlating evidence to reconstruct events, identify attack methods, and determine the source of compromise.

---

[7] M. Abdullah, M. M. Nawaz, B. Saleem, M. Zahra, E. binte Ashfaq, and Z. Muhammad, "Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data," Analytics, pp. 1–44, 2025, doi: https://doi.org/10.3390/analytics4030025.

[8] M. A. O. A. Mhara, A. A. A. Abdulrahman, and A. A. S. Baroud, "Cyber Attacks And Threats: Study Of The Types Of Cyber Attacks: Hacking, Viruses, Targeted Attacks, And Electronic Espionage," Int. J. Electr. Eng. Sustain., vol. 2, no. 4, pp. 38–47, 2024, doi: 10.65998/ijees.v2i4.102.

v. Attribution: Identifying the responsible individual, group, or infrastructure involved in the attack.
vi. Reporting: Preparing comprehensive forensic reports that document findings and support legal proceedings.

D. Importance of Systematic Investigation Models

Systematic investigation models offer a cohesive and consistent method for gathering, preserving, analysing, and documenting digital evidence in a way that is legally sound for the purposes of cybercrime investigations. These types of models reduce the chances of evidence tampering, provide consistency for investigations, allow for synergy between forensic specialists and law enforcement, and bolster the validity of digital evidence in the court of law. Furthermore, structured investigation frameworks can help investigators efficiently address more complex cyber incidents and ensure the integrity, reliability, and reproducibility of the investigation.[9]

3 Digital Forensics and Digital Evidence Collection

Digital forensics is one of the core aspects of a cybercrime investigation, as it becomes a scientific process to identify, collect, preserve, examine and present digital evidence in a standard legal fashion. Cybercrimes are increasingly being committed with computer, mobile devices, cloud services, and interconnected networks; digital forensic techniques are used to reconstruct cybercrimes, identify perpetrators, and provide factual evidence for judicial proceedings. The forensic process is based on international standards to guarantee the authenticity, reliability and admissibility of digital evidence during an investigation. Thus, digital forensics starts filling this breach between technical analysis and legal requirement which allows us to tackle cyber offenders successfully.[10]

A. Role of Digital Forensics in Cybercrime Investigation

Digital forensics can help the investigation of cybercrime by reconstructing the attack's timeline, providing clues to malicious activity, identifying suspects, and recovering deleted or hidden data. It allows investigators to understand how a cyber attack took place, uncover compromised systems, track back through the series of events to understand unauthorized access, and

[9] C. Aprilia, R. A. Gebrewold, M. D. Bamiduro, N. Borisova, and A. Mengdigali, "The Evolution of Cybercrime and Its Impact on Various Sectors," Data Sci. J. Comput. Appl. Informatics, vol. 10, no. 01, pp. 11–35, 2026, doi: 10.32734/jocai.v10.i1-24471.

[10] H. Coupland, "Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them," York Law Rev., 2025, doi: https://doi.org/10.15124/yao-23h6-cf66.

understand the sequence of events. Additionally, it plays a crucial role in incident response, malware analysis, fraud investigations, IP theft, and cyber espionage cases, and is an essential component of contemporary digital investigations.[11]

B. Types of Digital Evidence

Digital evidence may originate from numerous electronic sources, including:

i. Computers and laptops: Documents, browser history, application data, deleted files, and system logs.
ii. Smartphones and tablets: Call records, messages, GPS locations, photographs, and mobile applications.
iii. Cloud storage and cloud services: Backups, shared files, virtual machines, and user activity records.
iv. Network logs: Firewall logs, router logs, intrusion detection system (IDS) records, and traffic captures.
v. Emails: Email headers, attachments, communication history, and metadata.
vi. Social media platforms: Posts, chats, multimedia content, timestamps, and user interaction records.

C. Evidence Acquisition and Preservation

The process of evidence acquisition is the process of making a forensically acceptable copy of the digital media without changing the original evidence. Write blockers and forensic imaging are often used to make an exact bit-by-bit copy of storage devices. Preservation involves securely storing the original evidence, documenting all forensic activities, and protecting digital evidence from accidental alteration, damage, or unauthorized use. Safeguarding provides the evidence to be reliable for further forensic evaluation and legal action.

D. Chain of Custody

Chain of custody is a documented record documenting the identification and collection of digital evidence through the processing of evidence for presentation in court. It documents who retrieved the evidence, the time and location of the evidence's retrieval, the method of transporting the evidence, and who stored the evidence, examined the evidence, and transferred it to another authorized person. Having a chain of custody that is intact can help bolster the legal

[11] Y. Huang, "Application of Digital Forensics in Cybercrime Investigations," in International Conference on Software Engineering and Machine Learning, 2025, pp. 69–74. doi: 10.54254/2755-2721/151/2025.22847.

validity of the evidence because it provides a clear record of how the evidence was handled and preserved throughout the investigation.

E. Common Forensic Tools

Digital investigations can be assisted by a variety of special tools. EnCase is an existing commercial forensic platform for disk imaging, file recovery and forensic analysis. Forensic Toolkit (FTK) offers effective indexing and email analysis, password recovery and evidence management. Autopsy is an open source forensic tool suite for file system analysis, keyword searching, timeline and deleted file recovery. Volatility is a memory (RAM) forensics tool which focuses on analysing running processes, malware, and volatile system artefacts. Wireshark is a network protocol analyzer, which is used to capture and analyse network traffic, with the purpose of discovering suspicious communications or network-based attacks.[12]

F. Maintaining Evidence Integrity and Admissibility

Evidence integrity is critical for the preservation of evidence that reflects the true nature of the information being preserved. Investigators use cryptographic hash functions (MD5 and/or SHA-256) to ensure that forensic images do not change during the investigation. By following standardized forensic procedures, detailed documentation, secure storage, and legal guidelines, digital evidence can be preserved in a way that meets judicial standards for authenticity, reliability, and admissibility.[13]

4 Modern Investigative Strategies for Hunting Cybercriminals

Cybercrime is increasingly becoming more complex, making it necessary to employ a more sophisticated approach to investigation than traditional digital forensic methods. Cyber investigation is becoming more complex with the use of encrypted communication, cloud platforms, cryptocurrencies, anonymous networks as new tools for modern cybercriminals. The number and variety of cyber attacks are growing rapidly in India due to the emergence of digital services, online banking, e-governance and the Digital India initiative. Law enforcement agencies like Indian Cyber Crime Coordination Centre (I4C), state cyber police departments and the Computer Emergency Response Team-India (CERT-In) have introduced intelligence-driven

[12] H. S. Khan, S. M. Atif, and A. Mustufa, "The Role of Digital Forensics in Cybercrime Investigations," NUML Int. J. Eng. Comput., 2025, doi: 10.52015/nijec.v3i2.85.

[13] I. Ismail and K. A. Z. Ariffin, "The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance," PLoS One, vol. 20, no. 9, pp. 1–26, 2025, doi: https://doi.org/10.1371/ journal.pone.0331683.

strategies and cutting-edge analytical tools to enhance the detection, attribution and prosecution of cybercrime.[14]

Open-Source Intelligence (OSINT): Open-Source Intelligence (OSINT) refers to the practice of gathering and analyzing information that is freely accessible from the internet, websites, social media, public databases, domain registration information, and online forums. OSINT can aid investigations in India in areas such as financial crimes, cyberstalking, fake social media accounts, and misinformation, as it allows investigators to trace digital footprints and connect suspects to crimes.

Network and Log Analysis: Network and log analysis involves analyzing firewall and server logs, intrusion detection system (IDS) alerts, authentication logs, and network traffic data to identify cyber incidents. Combining these data sources allows investigators to see if unauthorized access was made, map the path of attack, detect compromised systems and get a sense of the timeline of cyber intrusions.

Malware Analysis and Threat Intelligence: Malware Analysis refers to the analysis of malicious software to learn about the behavior, spread, persistence and communication of the software. When coupled with cyber threat intelligence, investigators can detect indicators of compromise (IoCs), determine which threat actor may be behind an attack, and craft effective mitigation steps in advance. CERT-In regularly issues threat advisories and vulnerability alerts to enhance the cyber incident response capabilities of India.

Dark Web Investigations: With the anonymity offered by the Dark Web, cybercriminals can sell and buy stolen credentials, malware, fake documents, and shady online services. It is difficult to access, but investigators use specialized forensic and intelligence tools to track down illegal markets, uncover criminal networks and collect evidence that is legally and ethically usable to aid in operations.

Artificial Intelligence and Machine Learning in Cyber Investigations: In recent years, AI and Machine Learning have been helping with cyber investigations in various ways, including automated anomaly detection, malware classification, phishing identification, and large log analysis. These technologies can greatly reduce investigative time, aid in pattern recognition,

[14] K. Rani, "Cybercrime and Legal Responses in the Indian Jurisdiction," Indian J. Law, vol. 1, no. 1, pp. 35–41, 2023.

and help with predictive threat detection, giving investigators the ability to respond more effectively to more sophisticated cyberattacks.[15]

Cross-border Collaboration among Law Enforcement Agencies and Cybersecurity Organizations: Cybercrimes are often transnational in nature, meaning international collaboration is crucial. Indian agencies work with other agencies like INTERPOL, International Telecommunication Union (ITU), other countries CERT and world cyber security groups to share threat information, investigate incidents, track international cybercriminals and assistance in sharing digital evidence. This partnership enhances India's ability to investigate intricate cybercrimes and aids in the global fight against new cyber threats.[16]

5 Challenges in Cybercrime Investigation

The advancement of cyber technologies over the years has made investigations of cybercrimes even more difficult, especially in countries like India where digitalization has gained momentum with the rise of online financial services and e-governance and increasing internet penetration. While investigators are now finding it easier to find specialized agencies like the Indian Cyber Crime Coordination Centre (I4C) and CERT-In, they still face technical, legal and operational difficulties in locating cybercriminals and obtaining admissible digital evidence.

One of the biggest obstacles is the prevalence of encryption and anonymous messaging, which makes it difficult for investigators to access the key data they need when communications are sent via secure messaging apps and encrypted channels. Furthermore, Virtual Private Networks (VPNs), the Tor network, cryptocurrencies, and anti-forensics tactics allow criminals to obscure and conceal their identities, block Internet Protocol (IP) addresses, clear digital footprints and transact money anonymously, making it harder to attach and retrieve evidence and making attribution more difficult.[17]

Cloud environments and Internet of Things (IoT) devices are also posing challenges as digital evidence can be stored on various cloud servers across countries and IoT devices might be of different types and also have limited forensic capabilities. Investigators also face jurisdictional

---

[15] T. Abdiukov, “Threat hunting in large-scale SOCs: A cyber threat intelligence-driven model using MITRE AT-TandCK and machine learning,” World J. Adv. Res. Rev., vol. 21, no. 03, pp. 2679–2689, 2024, doi: https://doi.org/10.30574/wjarr.2024.21.3.0830.

[16] A. K. A. T. Phani, “Jurisdictional Issues in Cross-Border Cybercrime,” Int. J. Creat. Open Res. Eng. Manag., vol. 02, no. 03, pp. 1–11, 2026, doi: https://doi.org/10.55041/ijcope.v2i3.019.

[17] W. Hartono, D. Muhardi, A. Akhiruddin, D. V. B. Purba, P. Asa, and H. M. Y. Dm, “CHALLENGES OF CRIM-INAL INVESTIGATION CYBER CRIME,” Awang Long Law Rev., vol. 7, no. 1, pp. 11–19, 2024.

and legal challenges because cybercrime often takes place across various countries and jurisdictions, with differing legal structures which can cause a delay in sharing evidence and case information.

One of the major challenges is the vast amounts of digital information created by computers, mobile devices, cloud solutions, social media, and network logs. The relevant evidence must be identified efficiently by using advanced forensic tools and skilled investigators. In addition, the cyber investigation needs to strike a balance between investigative needs and privacy and ethical issues, taking into account applicable laws like the Information Technology Act, 2000, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and the Digital Personal Data Protection Act, 2023. This balance is crucial for safeguarding individual rights and ensuring that digital evidence is admissible in court and that public confidence in cyber investigations is maintained.[18]

6 Conclusion

Cybercrime has evolved in sophistication, making cyber investigations a multi-disciplinary effort that requires digital forensics, intelligence collection, advanced analytical tools, and legal steps. New technologies, anonymity tools, and cross-border infrastructures are enabling new methods by which cybercriminals are exploiting these technologies, and investigators need systematic methodologies and specialized forensic techniques to identify offenders and legally admissible digital evidence. The review emphasizes the importance of structured investigation models, evidence collection, forensic tools, OSINT techniques, malware analysis, and international co-operation in the enhancement of cybercrime investigations. Efforts by agencies like the Indian Cyber Crime Coordination Centre (I4C) and CERT-In have contributed to strengthening India's preparedness for addressing emerging cyber threats. However, problems with encryption, cloud-based environments, jurisdictions, huge amounts of digital evidence and privacy laws remain challenges for investigations. Emerging forensic tools, training, legal frameworks, and international collaboration will be vital to the ongoing progression of cybercrime detection, attribution, prosecution, and cyber resilience.

[18] V. Kumar, “Investigation of Cyber Crimes in India: Procedural Challenges Under the Bharatiya Nagarik Suraksha Sanhita, 2023,” Int. J. Sci. Res., vol. 14, no. 12, pp. 2114–2116, 2025, doi: https://dx.doi.org/10.21275/SR251224150603.

7 Reference

[1] D. Herlisya, “The Evolution of Cybercrime in the Digital Era: Legal and Security Implications,” Tripeco J. Soc. Sci. Humanit., vol. 1, no. 1, pp. 39–47, 2025, doi: 10.54012/jssh.v1i1.632.

[2] A. Mahboubi et al., “Evolving techniques in cyber threat hunting: A systematic review,” J. ofNetwork Comput. Appl., vol. 232, p. 104004, 2024, doi: https://doi.org/10.1016/j.jnca.2024.104004.

[3] C. Horan and H. Saiedian, “Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions,” J. Cybersecurity Priv., pp. 580–596, 2021, doi: https://doi.org/10.3390/jcp1040029.

[4] G. K. Ayswariya and A. Rajan, “A Comparative Study on the Difference Between Conventional Crime and Cyber Crime,” Int. J. Pure Appl. Math., vol. 119, no. 17, pp. 1451–1464, 2018.

[5] A Kuzior, I. Tiutiunyk, A. Zielińska, and R. Kelemen, “Cybersecurity and cybercrime: Current trends and threats,” J. Int. Stud., vol. 17, no. 2, pp. 220–239, 2024, doi: 10.14254/2071-8330.2024/17-2/12.

[6] M. Abdullah, M. M. Nawaz, B. Saleem, M. Zahra, E. binte Ashfaq, and Z. Muhammad, “Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data,” Analytics, pp. 1–44, 2025, doi: https://doi.org/10.3390/analytics4030025.

[7] M. A. O. A. Mhara, A. A. A. Abdulrahman, and A. A. S. Baroud, “Cyber Attacks And Threats: Study Of The Types Of Cyber Attacks: Hacking, Viruses, Targeted Attacks, And Electronic Espionage,” Int. J. Electr. Eng. Sustain., vol. 2, no. 4, pp. 38–47, 2024, doi: 10.65998/ijees.v2i4.102.

[8] Aprilia, R. A. Gebrewold, M. D. Bamiduro, N. Borisova, and A. Mengdigali, “The Evolution of Cybercrime and Its Impact on Various Sectors,” Data Sci. J. Comput. Appl. Informatics, vol. 10, no. 01, pp. 11–35, 2026, doi: 10.32734/jocai.v10.i1-24471.

[9] Coupland, “Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them,” York Law Rev., 2025, doi: https://doi.org/10.15124/yao-23h6-cf66.

[10] Y. Huang, “Application of Digital Forensics in Cybercrime Investigations,” in International Conference on Software Engineering and Machine Learning, 2025, pp. 69–74. doi: 10.54254/2755-2721/151/2025.22847.

[11] S. Khan, S. M. Atif, and A. Mustufa, “The Role of Digital Forensics in Cybercrime Investigations,” NUML Int. J. Eng. Comput., 2025, doi: 10.52015/nijec.v3i2.85.

[12] Ismail and K. A. Z. Ariffin, “The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance,” PLoS One, vol. 20, no. 9, pp. 1–26, 2025, doi: https://doi.org/10.1371/ journal.pone.0331683.

[13] Rani, “Cybercrime and Legal Responses in the Indian Jurisdiction,” Indian J. Law, vol. 1, no. 1, pp. 35–41, 2023.

[14] T. Abdiukov, “Threat hunting in large-scale SOCs: A cyber threat intelligence-driven model using MITRE ATTandCK and machine learning,” World J. Adv. Res. Rev., vol. 21, no. 03, pp. 2679–2689, 2024, doi: https://doi.org/10.30574/wjarr.2024.21.3.0830.

[15] K. A. T. Phani, “Jurisdictional Issues in Cross-Border Cybercrime,” Int. J. Creat. Open Res. Eng. Manag., vol. 02, no. 03, pp. 1–11, 2026, doi: https://doi.org/10.55041/ijcope.v2i3.019.

[16] W. Hartono, D. Muhardi, A. Akhiruddin, D. V. B. Purba, P. Asa, and H. M. Y. Dm, “CHALLENGES OF CRIMINAL INVESTIGATION CYBER CRIME,” Awang Long Law Rev., vol. 7, no. 1, pp. 11–19, 2024.

[17] V. Kumar, “Investigation of Cyber Crimes in India: Procedural Challenges Under the Bharatiya Nagarik Suraksha Sanhita, 2023,” Int. J. Sci. Res., vol. 14, no. 12, pp. 2114–2116, 2025, doi: https://dx.doi.org/10.21275/SR251224150603.