 DOI: 10.5281/zenodo.19145864

A COMPREHENSIVE ANALYSIS OF DIGITAL EVIDENCE AND CYBER FORENSICS IN HACKING CASES

By Hershika A. S[1] & Sujith Kumar R G[2]

ABSTRACT

The exponential proliferation of information and communication technologies has fundamentally transformed the landscape of criminal activity, giving rise to a sophisticated category of offences collectively termed cybercrime, of which hacking represents one of the most prevalent and technically complex manifestations. as hacking incidents increasingly target critical infrastructure, financial institutions, governmental systems, and individual users, the imperatives of digital evidence collection and cyber forensic investigation have assumed paramount significance within the administration of criminal justice. A significant dimension of this study concerns the legal architecture governing digital evidence across jurisdictions, with particular reference to the information technology act, 2000 (as amended in 2008), the Indian Evidence Act, 1872, the Bharatiya Sakshya Adhiniyam, 2023, and analogous international instruments including the budapest convention on cybercrime, 2001. The study analyses landmark judicial pronouncements that have shaped the admissibility and evidentiary weight accorded to electronically generated records, examining the evolving judicial approach toward section 65b certificates, hash value integrity, chain of custody requirements, and expert testimony in cyber forensic matters.

The study further identifies critical lacunae in existing legislative frameworks, including jurisdictional ambiguities in transborder hacking incidents, the fragility of attribution in cases involving anonymisation technologies, The volatility of

[1] The author (I) is a law student at School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University.
[2] The author (II) is an Assistant professor at School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University.

digital evidence, and the absence of standardised forensic protocols. it engages with the tension between effective law enforcement and the constitutional guarantees of privacy, due process, and the right against self-incrimination in the context of compelled decryption and device seizure.

Keywords: Digital evidence, Cyber forensics, Hacking, Cybercrime, Information Technology act, Admissibility, Chain of custody, Attribution, Section 65B, Budapest convention, Cyber jurisdiction, Electronic records.

CHAPTER 1: INTRODUCTION

- **Introduction**

The rapid proliferation of digital technology has fundamentally transformed both the commission and investigation of criminal offences. Hacking — broadly defined as unauthorised intrusion into computer systems — has evolved from the domain of individual hobbyists into a sophisticated, transnational criminal enterprise. With each passing year, the scale, complexity, and frequency of hacking incidents escalates, demanding a commensurate evolution in the legal and forensic frameworks that govern their prosecution.[3]

Digital evidence defined under the Information Technology Act, 2000 as 'electronic record' — has assumed central importance in the adjudication of cyber offences. Yet, its peculiar characteristics, namely volatility, susceptibility to alteration, and cross-jurisdictional origin, pose formidable challenges to investigators, prosecutors, and courts alike. Cyber forensics, as the scientific discipline dedicated to the recovery, preservation, and analysis of digital evidence, thus occupies a critical intersection between technology and law.[42]

Despite legal provisions and technological tools, several challenges persist in investigating hacking cases, including jurisdictional issues, encryption, anonymity, and rapid technological changes. This study examines the legal framework governing digital evidence, the role of cyber

[3] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023, European Union Agency for Law Enforcement Cooperation (2023).

[4] Section 2(1)(t), Information Technology Act, 2000 (Act 21 of 2000), Government of India

forensics in hacking investigations, and the challenges faced in ensuring the admissibility of digital evidence in courts. In India, the primary legislative instruments governing this field are the Information Technology Act, 2000 (as amended by the Information Technology (Amendment) Act, 2008), the Indian Evidence Act, 1872 (as amended, and now succeeded by the Bharatiya Sakshya Adhiniyam, 2023), and the Indian Penal Code, 1860 (succeeded by the Bharatiya Nyaya Sanhita, 2023)[5][3]. Despite these legislative measures, significant lacunae persist in evidentiary standards, chain-of-custody protocols, and admissibility criteria, often frustrating legitimate prosecutorial efforts.

- **Scope of Study**

The present study is confined to an analytical examination of digital evidence and cyber forensic practices specifically in the context of hacking offences under Indian law, with comparative reference to international frameworks including the Budapest Convention on Cybercrime, 2001, the United States Computer Fraud and Abuse Act (CFAA), 1986, and the United Kingdom's Computer Misuse Act, 1990. The study encompasses:[64]

- The statutory definitions of hacking, unauthorised access, and related offences under Indian law.
- The legal standards governing the collection, preservation, and admissibility of digital evidence.
- Judicial pronouncements from Indian and foreign courts on digital forensic evidence.
- Emerging challenges include encryption, anonymisation, cloud computing, and dark web forensics.
- Policy recommendations for legislative and procedural reform.

The study does not extend to matters of cybersecurity policy unrelated to criminal prosecution, financial cyber crimes (such as online fraud or cryptocurrency offences), or issues of corporate data protection, except insofar as they intersect with hacking offences.

- **Review of Literature**

[5] Information Technology (Amendment) Act, 2008 (Act 10 of 2009); Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023);Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[6] Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185, Budapest, 23 November 2001.

The existing literature on digital evidence and cyber forensics may be surveyed across four broad categories:[7]

- **Foundational Texts**

Casey's seminal work, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd ed., 2011), remains the authoritative reference on the technical and legal dimensions of digital forensics. Similarly, Carrier's File System Forensic Analysis (2005) provides the foundational framework for file- level forensic examination. In the Indian context, Pawan Duggal's Cyberlaw: The Indian Perspective offers the most comprehensive treatment of the Information Technology Act and its forensic implications.[8]

- **Statutory and Regulatory Analysis**

Numerous scholars have examined the adequacy of the Information Technology Act, 2000 in addressing contemporary hacking offences. Naavi Vijaykumar's work on the ITA-2008 amendments critically evaluates the enhanced penal provisions under Sections 43, 66, and 66B–66F. The Law Commission of India's Report No. 221 (2012) on 'Need for Legislation to Regulate Electronic Evidence' highlighted persistent evidentiary lacunae, many of which remain unremedied.[9]

- **Comparative Jurisprudence**

Scholars such as Susan Brenner (Cybercrime: Criminal Threats from Cyberspace, 2010) and Orin Kerr (Computer Crime Law, 4th ed., 2018) have extensively analysed the American legal landscape. The UK Parliament's Joint Committee on the Draft Communications Data Bill (2012) similarly provides crucial insights into legislative approaches to cyber investigation. The Council of Europe's explanatory reports on the Budapest Convention remain indispensable for understanding international legal standards.[10]

---

[7] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd ed., Academic Press, 2011), p. 5.

[8] B. Carrier, File System Forensic Analysis (Addison-Wesley, 2005); Pawan Duggal, Cyberlaw: The Indian Perspective (Saakshar Law Publications, 2014).

[9] Law Commission of India, Report No. 221, 'Need for Legislation to Regulate Electronic Evidence' (2012), Chapter III.

[10] S.W. Brenner, Cybercrime: Criminal Threats from Cyberspace (Praeger, 2010); O.S. Kerr, Computer Crime Law (4th ed., West Academic, 2018).

- **Judicial Literature**

Indian jurisprudence on digital evidence, though nascent, has been shaped by decisions such as State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru (2005) 11 SCC 600, Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473, and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1, which have progressively refined the standards for certification and admissibility of electronic records.[11]

- **Hypothesis**

The present study proceeds upon the following hypotheses:[12]

- The existing statutory framework under the Information Technology Act, 2000 and the Bharatiya Sakshya Adhiniyam, 2023 is inadequate to address the evidentiary requirements of contemporary hacking prosecutions, particularly in relation to cloud-stored and encrypted data.
- The absence of standardised, legally codified cyber forensic protocols in India leads to inconsistency in the collection and preservation of digital evidence, jeopardising prosecutorial outcomes.
- Judicial understanding of digital forensic evidence in India remains insufficiently developed to effectively evaluate technical evidence in complexhacking cases, necessitating structural reforms including specialised cyber courts and expert adjudicators.

- **Research Methodology**

The present study employs a doctrinal research methodology, primarily involving the analysis of primary legal sources statutes, subsidiary legislation, rules, and judicial decisions — supplemented by secondary sources including academic commentaries, law commission reports, and expert treatises.[13]

---

[11] State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru (2005) 11 SCC 600; Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

[12] The hypothesis is formulated in the normative tradition of legal research as described in S.N. Jain, 'Doctrinal and Non- Doctrinal Legal Research' (1975) 17 Journal of the Indian Law Institute 549.

[13] P. Hutchinson & N. Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17 Deakin Law Review 83.

The study further employs a comparative methodology, juxtaposing Indian legal standards with those prevailing in the United States, United Kingdom, European Union, and under the Budapest Convention on Cybercrime. This comparative lens enables identification of best practices and legislative gaps.

Case law analysis is drawn from the Supreme Court of India, various High Courts, and Cyber Appellate Tribunals, complemented by landmark decisions from the US Supreme Court, UK courts, and the European Court of Human Rights where instructive. All primary sources have been accessed through authorised legal databases including SCC Online, Manupatra, Westlaw India, and official government repositories.

The study does not employ empirical or quantitative research methods. However, governmental statistical data from CERT-In Annual Reports, NCRB Crime in India Reports, and international cybercrime statistics (Europol, FBI IC3) are cited to contextualise the findings.

- **Research Gap**

The review of existing literature reveals several significant research gaps:[14]

- Most Indian scholarship on cybercrime law fails to engage adequately with the forensic-technical dimensions of evidence collection and analysis, treating these as matters outside the proper domain of legal inquiry.
- Conversely, technical cyber forensics literature rarely engages with the legal admissibility standards that govern the use of forensic findings in Indian courts.
- There is a notable absence of updated scholarship examining the implications of the Bharatiya Nyaya Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023 for cyber forensic practice, given their recent enactment.
- Literature addressing the specific forensic challenges of hacking cases — as distinguished from general cybercrime — remains sparse in the Indian context.

The present study seeks to bridge this interdisciplinary gap by conducting an integrated doctrinal and comparative analysis of both the legal and forensic dimensions of digital evidence in hacking cases.

[14] CERT-In, Annual Report 2022–23, Ministry of Electronics and Information Technology, Government of India (2023).

- **Research Problem**

The central research problem may be articulated as follows: Does the existing Indian legal framework, in conjunction with established cyber forensic practices, provide a sufficiently robust, coherent, and practically effective system for the collection, preservation, and admissibility of digital evidence in hacking prosecutions, and if not, what reforms are necessary?

This overarching problem subsumes the following sub-problems:

- What is the scope and adequacy of statutory definitions of hacking and related offences under the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023?
- What are the legal standards governing the admissibility of electronic records and digital forensic reports in Indian courts?
- What forensic challenges are specific to hacking investigations, and how have courts addressed technical evidence in such cases?
- What legislative and procedural reforms would best address the identified deficiencies?

CHAPTER 2: STATUTORY FRAMEWORK — DEFINITIONS, PROVISIONS, AND HISTORICAL DEVELOPMENT

- **Historical Development of Cybercrime Legislation**

- **Pre-Information Technology Act Era (Pre-2000)**

Prior to the enactment of the Information Technology Act, 2000, there was no dedicated legislative framework governing computer-related offences in India. Cyber offences were prosecuted, with considerable difficulty, under the provisions of the Indian Penal Code, 1860 (IPC) — particularly Sections 378 (theft), 403 (dishonest misappropriation), 425 (mischief), and 463 (forgery) — and the Indian Evidence Act, 1872. The absence of specific provisions created significant jurisdictional and definitional ambiguities, and few prosecutions were successfully concluded.[15]

[15] P. Duggal, Textbook on Cyber Law (Universal Law Publishing, 2014), pp. 23–27.

The landmark case of Ratan Tata v. MTNL (1990) highlighted the inadequacy of existing law in addressing computer intrusion, while the Pune Citibank Mphasis Fraud Case (2005) demonstrated the practical impossibility of effective prosecution under pre-ITA provisions.

- **The Information Technology Act, 2000**

The Information Technology Act, 2000 (Act 21 of 2000) was enacted on 17 October 2000, based on the UNCITRAL Model Law on Electronic Commerce (1996) and the UN Resolution A/RES/51/162. It represented India's first comprehensive legislative attempt to regulate electronic commerce and cybercrime, though its original formulation was widely criticised as inadequate to address the full range of emerging cyber threats.

- **The Amendment Act of 2008**

The Information Technology (Amendment) Act, 2008 (Act 10 of 2009), which came into force on 27 October 2009, introduced far-reaching reforms, including the insertion of new Sections 43A, 66A through 66F, 67A, 67B, 69, 69A, 69B, 70, 70A, 70B, 71A, 72, and 72A. These provisions substantially expanded the scope of both civil liability and criminal punishment for a wide range of cyber offences including hacking, data theft, identity fraud, and cyber terrorism.

- **The New Criminal Laws: BNS and BSA (2023)**

The Bharatiya Nyaya Sanhita, 2023 (BNS) replaced the Indian Penal Code, 1860 with effect from 1 July 2024. Chapter XI of the BNS consolidates offences relating to documents and property marks, and Section 316 thereof specifically addresses forgery in electronic records. The Bharatiya Sakshya Adhiniyam, 2023 (BSA) replaced the Indian Evidence Act, 1872 and consolidates provisions relating to the admissibility of electronic evidence under Sections 61–65, significantly refining the certification requirements for electronic records first laid down in Section 65B of the Indian Evidence Act.[16]

- **Key Definitions Under the Information Technology Act, 2000**
- **'Computer' — Section 2(1)(i)**

[16] Information Technology (Amendment) Act, 2008 (Act 10 of 2009), Statement of Objects and Reasons

Section 2(1)(i) defines 'computer' as any electronic, magnetic, optical, or other high-speed data processing device or system that performs logical, arithmetic, and memory functions by manipulating electronic, magnetic, or optical impulses, and includes all input, output, processing, storage, software, or communication facilities that are connected or related to such device or system. This definition is notably broad and technology-neutral, extending to mobile devices, servers, embedded systems, and networked devices.

- **'Computer System' — Section 2(1)(l)**

A 'computer system' is defined under Section 2(1)(l) as a device or collection of devices, including input and output support devices, but excluding calculators that are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control, and other functions.

- **'Computer Network' — Section 2(1)(j)**

'Computer network' is defined under Section 2(1)(j) as the interconnection of one or more computers or computer systems or communication devices through the use of satellite, microwave, terrestrial line, wire, wireless, or other communication media; and terminals or a complex consisting of two or more interconnected computers or communication devices, whether or not the interconnection is continuously maintained.

- **'Electronic Record' — Section 2(1)(t)**

Section 2(1)(t) defines 'electronic record' as data, record, or data generated, image, or sound stored, received, or sent in an electronic form or microfilm or computer-generated microfiche. This definition is foundational to the admissibility of digital evidence in Indian courts and underpins the entire evidentiary framework of the ITA.

- **'Hacking' — Section 66, ITA (as amended in 2008)**

Section 66 of the ITA, 2000 (substituted by the 2008 Amendment) provides: 'If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment of either description for a term which may extend to three years or with fine which

may extend to five lakh rupees or with both.' Section 43 identifies the predicate acts including unauthorised access, downloading, introduction of viruses/malware, denial of service, and disruption of computer systems. The mental element — 'dishonestly or fraudulently' — distinguishes criminal hacking from the civil liability under Section 43.

- **Sections 66A–66F: Specific Cyber Offences**

The 2008 Amendment inserted Sections 66A through 66F, creating specific offences relating to:[23]

- Section 66B: Punishment for dishonestly receiving stolen computer resource or communication device (up to 3 years / Rs. 1 lakh fine).
- Section 66C: Punishment for identity theft — fraudulent/dishonest use of any person's electronic signature, password, or unique identification feature (up to 3 years and Rs. 1 lakh fine).
- Section 66D: Cheating by personation using computer resources or communication devices (up to 3 years and Rs. 1 lakh fine).
- Section 66E: Punishment for violation of privacy — intentional capturing, publishing, or transmitting an image of private area without consent (up to 3 years / Rs. 2 lakh fine).
- Section 66F: Cyber terrorism — acts intended to threaten unity, integrity, security, or sovereignty of India or to strike terror (up to life imprisonment).

- **Sections 69, 69A, 69B: Power to Intercept and Monitor**

Section 69 empowers the Central and State Governments to issue directions for interception, monitoring, or decryption of information in the interest of sovereignty, security, or public order. Section 69A provides the power to issue directions for blocking public access to information. Section 69B empowers the Government to authorise agencies to monitor and collect traffic data. These provisions are subject to procedural safeguards under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

- **Provisions Under the Bharatiya Sakshya Adhiniyam, 2023**
- **Admissibility of Electronic Records — Sections 61–65, BSA**

The Bharatiya Sakshya Adhiniyam, 2023 replaces the evidentiary provisions of the Indian Evidence Act, 1872, including the provisions that governed electronic evidence. Section 63 BSA (corresponding to the former Section 65B IEA) provides for the admissibility of electronic records produced by a computer. The certificate requirement — confirming the functioning of the computer, accuracy of the output, and proper activity at the material time — remains central. Sections 64 and 65 BSA address primary and secondary evidence in digital contexts, adapting the traditional framework to electronic realities.

- **International Legal Framework**

- **Budapest Convention on Cybercrime, 2001**

The Council of Europe's Convention on Cybercrime (Budapest Convention), opened for signature on 23 November 2001, is the only binding international treaty on cybercrime. Article 2 defines 'illegal access', Article 3 covers 'illegal interception', Articles 4 and 5 address 'data interference' and 'system interference', and Article 6 prohibits misuse of devices. Articles 16–21 set out procedural measures for evidence preservation and collection, including expedited preservation of stored computer data (Article 16), production orders (Article 18), and real-time collection of traffic data (Article 20). India is not a signatory but has been invited to accede.[17]

- **Computer Fraud and Abuse Act (CFAA), USA, 1986**

The United States' primary cybercrime statute, 18 U.S.C. § 1030, prohibits unauthorised access to protected computers and access with intent to defraud. Its provisions have been extensively litigated, particularly regarding the scope of 'authorisation' a question addressed most recently in Van Buren v. United States, 593 U.S. 374 (2021), in which the Supreme Court adopted a narrower, 'gates-up- or-gates-down' interpretation of unauthorised access.[18]

- **Computer Misuse Act, 1990 (UK)**

The UK's Computer Misuse Act, 1990 (CMA), as amended by the Police and Justice Act 2006 and the Serious Crime Act 2015, creates three core offences: unauthorised access to computer

[17] Council of Europe, Convention on Cybercrime and Explanatory Report, ETS No. 185 (Budapest, 2001), Art. 2–6, 16

[18] Van Buren v. United States, 593 U.S. 374 (2021); 18 U.S.C. § 1030 (Computer Fraud and Abuse Act, 1986).

material (Section 1), unauthorised access with intent to commit or facilitate further offences (Section 2), and unauthorised acts with intent to impair[19], or with recklessness as to impairing, the operation of a computer (Section 3). Section 3ZA (inserted in 2015) creates the additional offence of unauthorised acts causing, or creating a significant risk of, serious damage.

CHAPTER 3: DIGITAL EVIDENCE AND CYBER FORENSICS IN HACKING CASES — ISSUES, METHODOLOGIES, AND JUDICIAL TRENDzs

- **Nature and Characteristics of Digital Evidence**
- Digital evidence possesses several distinctive characteristics that differentiate it from traditional physical evidence and generate unique legal challenges. These characteristics include:
- Volatility: Certain digital evidence (RAM contents, network traffic, running processes) may be lost permanently upon system shutdown, necessitating immediate forensic acquisition.
- Mutability: Digital data can be altered without visible trace, raising persistent concerns about integrity and authenticity.
- Duplicability: Perfect copies of digital evidence can be created, and forensic examination is typically conducted on verified copies (forensic images) rather than original media.
- Cross-jurisdictionality: Digital evidence in hacking cases is frequently distributed across multiple jurisdictions and stored on remote servers, complicating both acquisition and legal process.
- **Cyber Forensic Methodology**

- **The ACPO Principles**

The Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence (5th ed., 2012) established four foundational principles that remain internationally influential: (1) no action taken should change data held on a digital device; (2) persons accessing original data must be competent to do so and explain their actions; (3) an audit trail of all processes must be created and preserved; and (4) the officer in charge bears overall responsibility for

[19] Computer Misuse Act, 1990 (c. 18) (UK), as amended by Serious Crime Act 2015, s. 41–44.

compliance with these principles. While not legally binding in India, these principles have been endorsed by Indian courts and CERT-In guidelines as best practice.[20]

- **Stages of Cyber Forensic Investigation**

A forensically sound investigation in a hacking case typically proceeds through the following stages:

- Identification: Recognising and categorising potential sources of digital evidence (seized devices, server logs, network traffic captures, cloud repositories).
- Preservation: Creating forensic images (bit-stream copies) of storage media using write-blockers; capturing volatile data from live systems using validated tools such as FTK Imager, Autopsy, or dd; computing cryptographic hash values (MD5, SHA-256) to verify integrity.
- Collection: Physical seizure and documentation of hardware; logical extraction of files, metadata, and logs under proper chain-of-custody procedures.
- Examination: Analysis of forensic images using validated tools; recovery of deleted files, log analysis, malware reverse engineering, network traffic analysis (PCAP analysis), and intrusion detection artefact examination.
- Analysis: Attribution of attacks through IP address tracing, user account correlation, geolocation data, browser artefacts, and malware signature analysis.
- Documentation and Reporting: Preparation of a forensic report satisfying the certification requirements under the Bharatiya Sakshya Adhiniyam, 2023.

- **Chain of Custody in Digital Evidence**

Chain of custody refers to the documented, chronological record of the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence. In digital evidence, the chain of custody must account for every person who handled the digital media, every copy made, every tool used for analysis, and the cryptographic verification of integrity at each stage.[21][19]

---

[20] Section 69, Information Technology Act, 2000; Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

[21] NIST, Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86 (2006), §3.1–3.6.

In Syed Asifuddin v. State of Andhra Pradesh (2005) Cri LJ 4314, the Andhra Pradesh High Court emphasised that where chain of custody of electronic evidence was not properly established, such evidence could not be relied upon without independent corroboration. The Punjab & Haryana High Court in Dharambir v. CBI (2008) similarly insisted on strict documentary proof of custody before electronic records could be accepted.[22]

- **Admissibility of Digital Evidence**
- **The Section 65B Certification Requirement (Indian Evidence Act / BSA)**

The most litigated question in Indian digital evidence law has been the requirement for certification under the erstwhile Section 65B of the Indian Evidence Act (now Section 63, Bharatiya Sakshya Adhiniyam, 2023). The evolution of the law in this area has passed through three distinct phases:

- **Phase 1 — Navjot Sandhu (2005):** The Supreme Court held that a Section 65B certificate was not mandatory where oral evidence of the computer's functioning was available. This was widely criticised as allowing a lower standard of proof.
- **Phase 2 — Anvar P.V. (2014):** A three-judge Bench overruled Navjot Sandhu and held that a Section 65B certificate was a mandatory pre- condition for admissibility of electronic records — the certificate being the only permissible mode of secondary evidence.
- **Phase 3 — Arjun Panditrao (2020):** A five-judge Constitution Bench of the Supreme Court confirmed Anvar P.V., but crucially held that the certificate need not be filed at the time of production; it could be submitted subsequently, and the court retained residual discretion to take evidence at a later stage. It further clarified who is a 'responsible official' competent to give the certificate.

- **Reliability and Authenticity of Digital Evidence**

Beyond certification, courts must assess the authenticity and reliability of digital evidence. The Supreme Court in Tomaso Bruno v. State of Uttar Pradesh (2015) 7 SCC 178 emphasised that CCTV footage should be accompanied by evidence about the integrity of the recording system

[22] NIST, Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86 (2006), §3.1–3.6.

and the unbroken custody of the recording media. These principles apply with equal force to all forms of digital evidence in hacking cases.[23]

- **Forensic Challenges Specific to Hacking Cases**
- **Attribution and IP Address Evidence**

Establishing attribution identifying the human being responsible for a specific hacking act is the most persistent challenge in cyber forensics. IP addresses, while foundational to attribution, present multiple legal and technical complexities: dynamic IP assignment, Network Address Translation (NAT), use of proxy servers, VPNs, and the Tor network can all sever the link between IP address and individual user.[24]

In the US Supreme Court's landmark decision in Carpenter v. United States, 585

U.S. 296 (2018), the Court held that government acquisition of historical cell-site location records without a warrant violated the Fourth Amendment's protections against unreasonable searches. While addressed to location data rather than hacking, this decision's reasoning — that digital data can reveal intimate details of personal life even when held by third parties — has significant implications for IP address and network log evidence acquisition.

- **Malware Analysis and Reverse Engineering**

Malware forensics — the systematic analysis of malicious software to establish how an intrusion was conducted, what data was accessed or exfiltrated, and whether the malware is attributable to a known threat actor — is central to many hacking prosecutions. Forensic malware analysis employs both static analysis (examining code without execution) and dynamic analysis (executing malware in a controlled sandbox environment). Indian courts have accepted malware forensic expert reports as admissible evidence, subject to the certification requirements of the BSA.

- **Log File Analysis**

---

[23] Carpenter v. United States, 585 U.S. 296 (2018), per Roberts CJ.

[24] ACPO, Good Practice Guide for Digital Evidence (5th ed., 2012), Principles 1–4; CERT-In, Guidelines for Collection and Preservation of Digital Evidence (2014).

System logs, access logs, authentication logs, firewall logs, and intrusion detection system (IDS) logs are among the most valuable categories of evidence in hacking cases. However, their forensic value depends critically upon log integrity (logs must not have been altered or selectively deleted), log completeness (many systems do not log all relevant activity by default), and accurate time-stamping (time zone discrepancies and clock drift can create ambiguities in event reconstruction).[25]

- **Encryption and Its Forensic Implications**

  The widespread adoption of strong encryption — end-to-end encryption in messaging applications, full-disk encryption on devices, encrypted communication channels, and the use of anonymising networks such as Tor — represents perhaps the greatest contemporary challenge to cyber forensic investigation.[26]

  Section 69(3) of the ITA, 2000 provides that where decryption of any information is necessary for national security or public order, the subscriber or intermediary must extend all facilities and assistance to the authorised Government agency and failure to comply is punishable with imprisonment up to seven years. However, this provision does not assist where the suspect is unknown, where keys are held by foreign entities, or where end-to-end encrypted services technically preclude service-provider-level decryption.[27]

  The privilege against self-incrimination under Article 20(3) of the Constitution of India further complicates compelled decryption. In the seminal case of Ritesh Sinha v. State of Uttar Pradesh (2019) 8 SCC 1, the Supreme Court held that a voice sample could be compelled without violating Article 20(3). However, the question of whether decryption of an encrypted device constitutes testimonial compulsion — and is thus protected by Article 20(3) — remains unresolved by the Supreme Court.[28]

- **Cloud Computing and Hacking Evidence**

---

[25] SANS Institute, 'Windows Forensic Analysis', SANS Reading Room (2019

[26] UK Home Office, 'The Investigatory Powers Act 2016: Encryption and Exceptional Access' (2020).

[27] Section 69(3) read with Rule 13, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

[28] Ritesh Sinha v. State of Uttar Pradesh (2019) 8 SCC 1; see also Selvi v. State of Karnataka (2010) 7 SCC 263 (narco- analysis).

The migration of data storage and processing to cloud computing environments introduces profound complications for cyber forensic investigation. Cloud-based evidence raises the following specific issues:[29]

- Multi-tenancy: Cloud infrastructure is shared among multiple customers; forensic acquisition must be designed to avoid contaminating co-tenants' data, while also ensuring the completeness of the target's data.
- Data volatility and ephemeral resources: Containerised applications, serverless functions, and auto-scaling infrastructure may result in evidence existing only momentarily and in no persistent form.
- Jurisdictional fragmentation: A single cloud deployment may distribute data across servers located in multiple countries, requiring mutual legal assistance (MLAT) or letters rogatory for lawful access, which can take months or years.

  The CLOUD Act (Clarifying Lawful Overseas Use of Data Act), enacted in the United States in 2018, permits American law enforcement to compel US cloud service providers to produce data stored abroad. India lacks a comparable bilateral or multilateral mechanism, though negotiations for India's accession to the Budapest Convention are ongoing.[30]

- **Dark Web Forensics**

  The dark web — portions of the internet not indexed by conventional search engines and accessible only through anonymising networks such as Tor — is a primary marketplace for hacking tools, exploits, stolen credentials, and ransomware-as-a-service offerings. Forensic investigation of dark web hacking activities presents distinctive challenges:[31]

- Tor network anonymity: While Tor nodes can be correlated through global traffic analysis, individual node de-anonymisation requires either technical exploitation or physical access to exit node logs.
- Cryptocurrency evidence: Dark web transactions typically employ cryptocurrencies (Bitcoin, Monero). Blockchain forensics — tracing cryptocurrency flows through techniques such as

[29] NIST, Guidelines on Security and Privacy in Public Cloud Computing, Special Publication 800-144 (2011).
[30] Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018).
[31] D. Moore & T. Rid, 'Cryptopolitik and the Darknet' (2016) 58 Survival: Global Politics and Strategy 7.

transaction graph analysis and exchange KYC data — has become a specialised forensic discipline.

- Undercover operations: Law enforcement agencies have increasingly employed covert infiltration of dark web marketplaces — methods whose legality under Indian law (absent specific authorisation) remains contested.
- **Cross-Border Cyber Jurisdiction and Mutual Legal Assistance**

  Hacking offences are inherently transnational — the perpetrator, victim, and server infrastructure frequently exist in different countries. **Section 75** of the Information Technology Act, 2000 provides for extra-territorial application of the Act where offences involve a computer, computer system, or computer network located in India, regardless of the nationality of the offender.

  The primary mechanism for cross-border evidence gathering remains Mutual Legal Assistance Treaties (MLATs). India has executed MLATs with approximately 44 countries as of 2024. However, MLAT requests are notoriously slow, with average response times measured in years rather than months — plainly inadequate for the preservation of volatile digital evidence.
- **Significant Case Law Analysis**
- **Indian Cases**

  State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru (2005) 11 SCC 600: The Supreme Court upheld the admission of computer-generated call records from mobile service providers, holding that Section 65B certification was not an absolute pre-condition where secondary evidence of the computer's functioning was available through oral testimony. Subsequently overruled by Anvar P.V.[3230]

  Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473: A three-judge bench overruled Navjot Sandhu and held unequivocally that electronic records can only be proved by a certificate under Section 65B. The Court distinguished between primary evidence (original storage device) and secondary evidence (printout or copy), holding that the former is admissible without certification under Section 65, but the latter requires certification.[33]

  Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1:

---

[32] State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru (2005) 11 SCC 600, per P.V. Reddi J.

[33] Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473, per Kurian Joseph J.

A five-judge Constitution Bench affirmed Anvar P.V. and additionally clarified:

(a) the person competent to give the certificate is a 'responsible official' who has custody of the computer and can speak to its proper functioning; (b) the certificate can be filed later if not available at the time of production; and (c) courts should not take a hyper-technical view of certification requirements in civil proceedings.[34]

Shreya Singhal v. Union of India (2015) 5 SCC 1[35]: The Supreme Court struck down Section 66A of the ITA, 2000 (as amended), which had criminalised the sending of 'offensive' electronic messages, on the ground that it violated Article 19(1)(a) (freedom of speech) and was neither a reasonable restriction under Article 19(2) nor defined with sufficient precision to be enforceable. While not directly a hacking case, this decision significantly shaped the constitutional limits of cyber offence provisions.

Manohar Lal Sharma v. Principal Secretary (2014) 2 SCC 532 ('Coalgate' Case): The Supreme Court's acceptance of forensic examination of electronic records in the coal block allocation investigation case established important precedent regarding court-supervised digital forensic investigation and the integrity of seized electronic evidence.[36]

Kotak Mahindra Bank v. D.L. Rawal & Ors. (Bombay High Court, 2012): The Bombay High Court accepted server logs and email records as admissible electronic evidence in a banking fraud/hacking case, setting important precedent for the admissibility of commercial server-generated records.

CBI v. Arif Azim (Sony Sambandh Network Case, 2008): This case, decided by the Additional Sessions Judge, New Delhi, involved unauthorised access to Sony's computer network and fraudulent use of credit card data. It was one of India's first successful hacking prosecutions under the ITA, 2000, resulting in conviction under Section 66 and Sections 419/420 IPC.

SWATCHTA PLATFORM HACK:

- In September 2022, Cyble Research & Intelligence Labs investigated the Swachh City data leak that compromised the Personally Identifiable Information (PII) of over 16 million Indian

[34] Shreya Singhal v. Union of India (2015) 5 SCC 1, per J. Chelameswar J.

[35] Shreya Singhal v. Union of India (2015) 5 SCC 1

[36] Manohar Lal Sharma v. Principal Secretary (2014) 2 SCC 532.

nationals. On September 23, 2022, researchers discovered the leaked database through Cyble's Threat Intelligence platform. The leak was shared by threat actor (TA) LeakBase, active on the cybercrime forum Breach Forums.

- The Swachhata Platform (Swachh.city) is a Swachh Bharat Mission initiative governed by the Ministry of Housing and Urban Affairs (MoHUA), Government of India. The platform is used to submit and follow up on municipal complaints.
- The threat actor identifies themselves as LeakBase, Chucky, Sqlrip, and Chuckies on various underground forums. LeakBase often operates for financial gain and conducts sales on its marketplace forum, leakbase.cc.
- The TA Leak Base had been active on Breach Forums since March 29, 2022, and is also a moderator on LeakBase.cc. They had previously compromised several prominent financial institutions in India prior to this leak.
- Leaked details include usernames, email addresses, password hashes, mobile numbers, one-time passwords (OTPs), last logged-in times, and IP addresses, among others.
- More specifically, the database comprises 101,718 unique email addresses and 15,835,111 unique mobile numbers.
- A total of 6 GB of compromised data from the Swachhata Platform was shared via a popular file-hosting platform.
- Not only were the details of web users of Swachh City compromised, but even the database of users who downloaded the Swachhata-MoHUA app on iOS and Android were victims of the data breach.
- The SQL header revealed that the impacted infrastructure was running on outdated versions of phpMyAdmin and the Ubuntu 16.04.1 host operating system.
- Cyble's Threat Intelligence Platform captured compromised administrator and non-administrator accounts' login information for the phpPgAdmin web portal in multiple instances of stealer malware logs from April 11, 2022 indicating the initial compromise may have preceded the public disclosure by months. Research largely indicates that the credentials were possibly compromised from developer accounts, which could have been the primary indicators of the TA's initial access. However, the TA also disclosed that their primary tactic was a custom brute-forcing method.

- CloudSEK's CEO Rahul Sasi noted it was also likely that a web-based security vulnerability or API-based vulnerability was exploited.
- The breach poses a significant threat as the compromised data can be exploited for phishing attacks, fake breach notice emails, social engineering to obtain more sensitive information, ransomware attacks, data exfiltration, and the sale of leads on cybercrime forums.
- The breach puts users at risk of phishing, smishing, social engineering, and identity theft.

Key Technical Vulnerabilities Exposed

- Outdated infrastructure — Ubuntu 16.04.1 (end-of-life) and outdated phpMyAdmin were running in production.
- Weak credential security — Admin credentials were compromised via stealer malware and possibly brute-force.
- Lack of intrusion detection — The attacker had access for months (April– May 2022) before public disclosure in September 2022.
- OTP data storage — Storing transmitted OTP tokens in a database is a serious security design flaw.
- No timely patching — Running government platforms on end-of-life software violates basic security hygiene.

This breach became one of the most significant Indian government data breaches of 2022, highlighting the vulnerability of public-sector digital infrastructure to cybercriminal actors.

Stealer Malware Log Forensics

Cyble's Threat Intelligence Platform captured compromised administrator and non-administrator accounts' login information for the phpPgAdmin web portal of the impacted infrastructure in multiple instances of stealer malware logs from April 11, 2022.

What stealer malware logs reveal forensically:

Stealer malware (also called "info-stealers") are trojans that harvest credentials, browser cookies, autofill data, and session tokens from infected machines. Key forensic observations here:

- The fact that stealer logs appeared on April 11, 2022, means a developer or admin's endpoint was infected prior to the breach
- The logs captured phpPgAdmin credentials — the PostgreSQL web admin interface — confirming attackers had database-level access
- **International Cases**

  United States v. Morris, 928 F.2d 504 (2d Cir. 1991): The first federal conviction under the CFAA arising from the Morris Worm — the first major computer worm released on the internet. The Second Circuit affirmed that 'intentional access' under 18 U.S.C. § 1030(a)(5) did not require intent to cause damage, only intent to access.[37][35]

  R v. Gold & Schifreen [1988] 2 WLR 984 (UK House of Lords): Defendants who gained unauthorised access to BT's Prestel network (including the Duke of Edinburgh's email account) were acquitted because the existing Forgery and Counterfeiting Act, 1981 could not be stretched to cover computer access credentials. This case directly precipitated the Computer Misuse Act, 1990.[38][36]

  Van Buren v. United States, 593 U.S. 374 (2021): The US Supreme Court adopted a narrow 'gates-up-or-gates-down' interpretation of unauthorised access under the CFAA, holding that an individual who has authorisation to access a computer system does not exceed that authorisation under Section 1030(a)(2) merely by using his access for an improper purpose — a significant limitation on the scope of federal hacking liability.[39]

  United States v. Mitnick (Kevin Mitnick Case, C.D. Cal., 1999): The prosecution of the world's most notorious hacker resulted in his guilty plea to computer fraud and wire fraud charges involving the penetration of dozens of corporate networks. The case established important prosecutorial precedents for the use of packet capture logs and network forensic evidence.[40]

---

[37] United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

[38] R v. Gold & Schifreen [1988] 2 WLR 984 (HL).

[39] Van Buren v. United States, 593 U.S. 374 (2021), per Barrett J.

[40] United States v. Mitnick, Case No. CR-99-0818-DT (C.D. Cal., 1999).

Cybersecurity and Infrastructure Security Agency (CISA) v. Texas (5th Cir., 2022): This case addressed the evidentiary standards for attribution of nation-state hacking operations, examining the admissibility of threat intelligence reports and TTPS (Tactics, Techniques, and Procedures) evidence compiled by cybersecurity firms as expert opinion evidence.[41]

- **Expert Testimony in Cyber Forensic Cases**

The admissibility and weight of expert opinion evidence in cyber forensic cases is governed in India by **Sections 45–51** of the **Bharatiya Sakshya Adhiniyam, 2023** (corresponding to Sections 45–51 of the former Indian Evidence Act, 1872). Expert witnesses in hacking cases typically include certified forensic examiners (CFCE, EnCE), network security specialists, and malware analysts.

In the United States, the admissibility of expert scientific testimony is governed by **the Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993)** standard, requiring that methodology be scientifically valid, applied in a manner consonant with accepted scientific technique, and relevant to the facts in issue. Indian courts have drawn upon Daubert-like reasoning in assessing cyber forensic
expert evidence, though no formal adoption of the Daubert standard has occurred.[42][40]

The United Nations Convention against Cybercrime was adopted by the General Assembly of the United Nations on 24 December 2024 in New York by resolution 79/243. The Convention is the first comprehensive global treaty on this matter, which provides States with a range of measures to be undertaken to prevent and combat cybercrime. It also aims to strengthen international cooperation in sharing electronic evidence for serious crimes.

Status of the Convention, from adoption to the Conference of the States Parties

After years of work, the Convention was adopted by the General Assembly on 24 December 2024, opened for signature on 25 October 2025 at a signing ceremony held in Hanoi, Viet Nam, and will remain open for signature at United Nations Headquarters in New York until 31

[41] CISA v. Texas, No. 22-50789 (5th Cir. 2022).

[42] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), per Blackmun J.

December 2026. The Convention will enter into force after 40 States become Parties, with its implementation reviewed by the Conference of the States Parties.

For an overview of the signature and ratification processes of the UN Convention against Cybercrime, including model instruments

Key events:

- **Adoption by the General Assembly** (24 December 2024): The United Nations Convention against Cybercrime was adopted by consensus through General Assembly resolution 79/243 of 24 December 2024.
- **Signing Ceremony** (25 and 26 October 2025): The Convention opened for signature in Hanoi at the High-Level Conference and Signing Ceremony hosted by the Government of Viet Nam. The ceremony concluded with 72 signatories .Further information about the ceremony can be found at hanoiconvention.org.
- **Ratification and Accession by States**: Following signature, States will complete their internal domestic processes to implement the Convention and, once concluded, deposit an instrument of ratification, acceptance, or approval with the Secretary-General to formally become States Parties to the Convention. States that did not sign the Convention may also become Parties by depositing an instrument of accession.
- **Entry into Force**: The Convention will enter into force 90 days after the 40th instrument of ratification, acceptance, approval or accession is deposited.
- **Conference of the States Parties**: After entry into force, a Conference of the States Parties will convene periodically to improve the capacity of and cooperation among States Parties to achieve the objectives of the Convention and to promote and review.

Chapters of the Convention

The Convention's nine chapters provide a comprehensive approach to prevent and combat the global problem of cybercrime while including human rights safeguards. The Convention resolves technical and legal challenges by adjusting traditional means and methods of criminal

investigations to the information and communication technology environment and by strengthening international cooperation.

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

The General Assembly established the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, which approved a draft convention in August 2024. The Ad Hoc Committee is further mandated by the General Assembly to hold sessions to prepare the draft rules of procedure for the Conference of the States Parties, and to negotiate a draft protocol supplementary to the Convention, addressing, inter alia, additional criminal offences as appropriate

CHAPTER 4: CONCLUSION AND SUGGESTIONS

- **CONCLUSIONS AND SUGGESTIONS**

- **Adequacy of the Statutory Framework**

The review of statutory provisions and judicial decisions leads to the conclusion that the Indian legal framework for digital evidence and cyber forensics in hacking cases, while substantially improved since the original enactment of the Information Technology Act, 2000, remains materially deficient in several critical respects.

First, the statutory definitions of hacking-related offences under Section 66 ITA and corresponding provisions of the Bharatiya Nyaya Sanhita, 2023 lack the precision and granularity necessary to accommodate the full spectrum of contemporary attack methodologies, including supply-chain attacks, zero-day exploitation, firmware manipulation, and AI-assisted attacks.

Second, the evidentiary certification framework under the Bharatiya Sakshya Adhiniyam, 2023, while judicially refined through the Anvar P.V. and Arjun Panditrao line of authority, continues to generate practical difficulties — particularly in relation to the qualification of the 'responsible official', the handling of server-side cloud evidence, and the certification of real-time network captures.

- **Assessment of Hypotheses**

The first hypothesis is confirmed: the existing framework is inadequate for cloud and encrypted evidence. The second hypothesis is confirmed: the absence of standardised forensic protocols leads to inconsistency and evidential weakness. The third hypothesis is substantially confirmed: while the Supreme Court has made significant strides in rationalising electronic evidence law, judicial understanding of the technical dimensions of cyber forensics at trial court level remains uneven, and the infrastructure of specialised cyber courts is nascent.

- **The Evolving Challenge**

Artificial intelligence-assisted cyber attacks, quantum computing's prospective impact on cryptographic infrastructure, Internet-of-Things (IoT) device forensics, and the growing sophistication of anonymisation technologies collectively ensure that the gap between legal frameworks and technical reality will persist — and potentially widen — absent proactive and sustained legislative and institutional response.

- **Suggestions**

- **Legislative Reform**

Enactment of a Dedicated Digital Evidence Act: India should enact a comprehensive Digital Evidence Act, consolidating and updating the scattered provisions currently found in the ITA, BSA, and Code of Criminal Procedure. This Act should incorporate standards for the collection, preservation, analysis, and presentation of digital evidence, drawing upon internationally recognised frameworks such as ISO/IEC 27037:2012 (Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence).

Amendment of the ITA to Expand Hacking Offences: Section 66 and Section 43 of the ITA should be amended to expressly incorporate: (a) supply- chain attacks; (b) ransomware deployment; (c) unauthorised access to IoT and critical infrastructure systems; (d) AI-assisted automated attack tools. Penalties should be graduated according to the severity of the attack and the nature of the victim institution (e.g., critical infrastructure operators should attract enhanced penalties).

Statutory Codification of Forensic Standards: The law should mandate that all digital evidence in criminal proceedings be collected, preserved, and analysed in accordance with

CERT-In prescribed standards (or a new statutory body's standards), with chain-of-custody documentation a statutory
requirement. Courts should be empowered to exclude evidence where these standards have not been complied with, absent a satisfactory explanation.

Accession to the Budapest Convention: India should complete its accession to the Budapest Convention on Cybercrime, which would provide an immediate and comprehensive framework for cross-border digital evidence acquisition, expedited preservation requests, and real-time data collection replacing the slow and inadequate MLAT mechanism for cybercrime cases.

Encryption and Decryption Framework: Parliament should enact a clear and constitutionally balanced framework governing compelled decryption, expressly addressing the interaction with Article 20(3) of the Constitution. This framework should provide for judicial oversight of decryption orders, time-limited preservation orders directed at encrypted cloud data, and procedural safeguards against fishing expeditions.

- **Judicial and Institutional Reforms**

Establishment of Dedicated Cyber Courts: The Cyber Appellate Tribunal established under the ITA lacks criminal jurisdiction. Dedicated Cyber Courts with criminal jurisdiction, staffed by judges with specialised training in digital evidence and cyber forensics, should be established in each High Court jurisdiction. Special Public Prosecutors with cyber law expertise should be appointed in each such court.

Judicial Education: The National Judicial Academy should introduce mandatory modules on digital evidence law, cyber forensics, and technical evaluation of expert evidence in its training curricula for judges at all levels. The Supreme Court's e-committee should develop supplementary online resources for judicial reference.

Strengthening CERT-In and Forensic Infrastructure: CERT-In's forensic capacity should be significantly expanded, with the establishment of regional cyber forensic laboratories with standardised, validated equipment and personnel certified to internationally recognised standards (ISO/IEC 17025 accreditation). State police cyber cells should be funded and equipped to conduct initial forensic triage in hacking cases without dependence on central government resources.

Court-Appointed Digital Forensic Experts: The Supreme Court and High Courts should develop panels of court-appointed digital forensic experts available to assist courts in evaluating

technical evidence modelled on the court-appointed scientific advisor systems in the UK and France. This would address the asymmetry in technical expertise between prosecution and defence, and reduce the risk of courts misappraising forensic evidence.

- **International Cooperation**

Bilateral MLAT Reform: Existing MLAT agreements should be renegotiated to include specific provisions for expedited preservation of digital evidence (on the model of Budapest Convention Article 16) with a maximum response time of 24–48 hours for preservation requests and a clearly specified timeline for substantive provision of evidence.

Data Localisation as a Forensic Tool: The Digital Personal Data Protection Act, 2023's data localisation provisions should be leveraged to ensure that forensically relevant data pertaining to Indian users and Indian-origin attacks is stored within India's territorial jurisdiction, facilitating domestic legal process and reducing dependence on foreign judicial assistance.

- **Concluding Observations**

The integrity of cyber forensic evidence is the bedrock upon which all hacking prosecutions ultimately rest. Without technically sound evidence collection, legally robust admissibility standards, and forensically competent courts, the criminal justice system will remain structurally ill-equipped to bring sophisticated cyber attackers to account. The reform agenda identified in this study is neither radical nor unprecedented many of its components reflect international best practice and are entirely consistent with India's constitutional and legal tradition.

The rapid pace of technological change in the cyber threat landscape militates against legislative delay. Every year that the identified lacunae persist is a year in which cyber criminals, both domestic and foreign, exploit the gaps between India's legal framework and the technical realities of their operations. The window for comprehensive reform is open; it should not be allowed to close by default.

REFERENCES

- **Primary Sources**

- **Statutes and Legislation**

- Information Technology Act, 2000 (Act 21 of 2000), Government of India.
- Information Technology (Amendment) Act, 2008 (Act 10 of 2009), Government of India.
- Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), Government of India.
- Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), Government of India.
- Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), Government of India.
- Indian Evidence Act, 1872 (Act 1 of 1872) [repealed].
- Indian Penal Code, 1860 (Act 45 of 1860) [repealed].
- Digital Personal Data Protection Act, 2023 (Act 22 of 2023), Government of India.
- Computer Fraud and Abuse Act, 1986, 18 U.S.C. § 1030 (USA).
- Computer Misuse Act, 1990 (c. 18) (UK), as amended.
- Council of Europe Convention on Cybercrime (Budapest Convention), ETS No. 185 (2001).
- Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115- 141 (USA, 2018).
- Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

- **Case Law**

- Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473.
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1.
- Carpenter v. United States, 585 U.S. 296 (2018) (USA).
- CBI v. Arif Azim (Additional Sessions Judge, New Delhi, 2008) [unreported].
- Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993) (USA).
- Dharambir v. CBI (2008) (P&H) [unreported].
- Kotak Mahindra Bank v. D.L. Rawal (Bombay HC, 2012) [unreported].
- Manohar Lal Sharma v. Principal Secretary (2014) 2 SCC 532.
- R v. Gold & Schifreen [1988] 2 WLR 984 (UK HL).
- Ritesh Sinha v. State of Uttar Pradesh (2019) 8 SCC 1.
- Selvi v. State of Karnataka (2010) 7 SCC 263.
- Shreya Singhal v. Union of India (2015) 5 SCC 1.
- State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru (2005) 11 SCC 600.
- Syed Asifuddin v. State of Andhra Pradesh (2005) Cri LJ 4314.
- Tomaso Bruno v. State of Uttar Pradesh (2015) 7 SCC 178.
- United States v. Mitnick, Case No. CR-99-0818-DT (C.D. Cal., 1999).
- United States v. Morris, 928 F.2d 504 (2d Cir. 1991).
- Van Buren v. United States, 593 U.S. 374 (2021).

- **Secondary Sources**

- **Books and Treatises**

- Brenner, S.W., Cybercrime: Criminal Threats from Cyberspace (Praeger, 2010).
- Carrier, B., File System Forensic Analysis (Addison-Wesley, 2005).
- Casey, E., Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd ed., Academic Press, 2011).
- Duggal, P., Cyberlaw: The Indian Perspective (Saakshar Law Publications, 2014).
- Duggal, P., Textbook on Cyber Law (Universal Law Publishing, 2014).
- Kerr, O.S., Computer Crime Law (4th ed., West Academic, 2018).
- Mason, S. (ed.), Electronic Evidence (4th ed., Institute of Advanced Legal Studies, 2017).
- Schneier, B., Secrets and Lies: Digital Security in a Networked World (Wiley, 2000).
- Sikorski, M. & Honig, A., Practical Malware Analysis (No Starch Press, 2012).

- **B. Journal Articles**

- Goyal, K., 'Admissibility of Electronic Evidence in India: A Critical Analysis' (2021) 63 Journal of the Indian Law Institute 45.
- Hutchinson, P. & Duncan, N., 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17 Deakin Law Review 83.

- Jain, S.N., 'Doctrinal and Non-Doctrinal Legal Research' (1975) 17 Journal of the Indian Law Institute 549.
- Moore, D. & Rid, T., 'Cryptopolitik and the Darknet' (2016) 58 Survival: Global Politics and Strategy 7.

C. Official Reports

- ACPO, Good Practice Guide for Digital Evidence (5th ed., 2012).
- CERT-In, Annual Report 2022–23, Ministry of Electronics and Information Technology, Government of India (2023).
- Council of Europe, Explanatory Report to the Budapest Convention on Cybercrime, ETS No. 185 (2001).
- Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023 (Europol, 2023).
- ISO/IEC 27037:2012, Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence (ISO, 2012).
- Law Commission of India, Report No. 221, 'Need for Legislation to Regulate Electronic Evidence' (2012).
- Law Commission of India, Report No. 248, 'Obsolete Laws: Warranting Immediate Repeal' (2014).
- NCRB, Crime in India 2022: Statistics, National Crime Records Bureau (Ministry of Home Affairs, 2023).
- NIST, Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86 (2006).

- NIST, Guidelines on Security and Privacy in Public Cloud Computing, Special Publication 800-144 (2011).
- UNODC, Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime, Vienna, 2013).