International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 07, July 2026)

Digital Footprints in Cybercrime: A Comparative Analysis of Investigation Techniques Across Jurisdictions

Dr. Shivalingappa Angadi[1], Raveendra B Bhat[2]

[1]*Course Coordinator, Department of Criminology, Rashtriya Raksha University Shivamogga Campus, Karnataka, India*
[2]*Research Officer, Forensic psychology, Rashtriya Raksha University Shivamogga Campus, Karnataka, India*

***Abstract*--Financial fraud and phishing drive the largest share of cybercrime losses in the United States, the European Union, and India, yet each investigates through different institutional and evidentiary pathways (Federal Bureau of Investigation [FBI], 2025; Europol, 2024; National Crime Records Bureau [NCRB], 2026). Using secondary data from official reports and peer-reviewed literature (2019–2026), this paper compares live versus dead forensic acquisition, chain-of-custody protocol, AI/ML-assisted analysis, and legal admissibility across the FBI/DOJ, Europol, and India's I4C frameworks. Findings show technical convergence but legal divergence: the U.S. relies on Daubert-tested case law (Maryman & Associates, 2026), the EU on a new Production Order regime (White & Case, 2023), and India on statutory dual-certification under the Bharatiya Sakshya Adhiniyam (KSandK Legal, 2025). In every jurisdiction, AI-assisted evidence analysis is outpacing legal validation (Reliability and Admissibility of AI-Generated Evidence, n.d.), which this paper identifies as the central reform priority.**

***Keywords*-- digital forensics, cybercrime, chain of custody, financial fraud, phishing, admissibility, artificial intelligence**

I. Introduction

Phishing and financial fraud now generate the largest reported losses in cybercrime across all three jurisdictions (FBI, 2025; Europol, 2024; NCRB, 2026). The FBI's IC3 logged 859,532 complaints and US$16.6 billion in losses in 2024, a 33% year-over-year rise (FBI, 2025; LevelBlue, 2025). Europol's IOCTA ranks online fraud among the EU's three most threatening cybercrime types, with phishing evolving into smishing and quishing (Europol, 2024; Bergman, 2024). India's National Cybercrime Reporting Portal recorded 2.27 million complaints and ₹22,845.73 crore in losses in 2024, a 42% jump (The420.in, 2025; CyberPeace, 2026). Each jurisdiction has built structurally different responses: American Daubert jurisprudence (Maryman & Associates, 2026), the EU's coordinated Europol-IOCTA model with new Production Orders (European Commission, n.d.), and India's newly enacted Bharatiya Sakshya Adhiniyam (Naavi, n.d.). This paper compares four dimensions acquisition methodology, chain of custody, AI/ML tool use, and admissibility standards to identify where practice converges and where it does not.

II. Literature Review

In the United States alone, investment fraud accounted for the highest financial loss of all crimes, totaling $6.57 billion in costs related to "crypto pig butchering" schemes in 2025 (Abnormal Security, 2025). Business email compromise resulted in losses nearing $8.5 billion during 2022-2024 (Nacha, 2025). Meanwhile, the increasing number of phishing-as-a-service kits and use of AI-generated deepfakes by criminals indicates an uptick in sophisticated social engineering techniques (Europol's IOCTA, 2024; Bergman, 2024; NOTIONES, 2024).

India witnessed its first-time breach of one lakh (or 100 thousand) registered cases on cybercrime within a year, according to National Crime Records Bureau (NCRB) data released in 2026. A total of 17.9 percent increase was observed in cybercrime cases as compared to previous years since the beginning of this year, which included a significant surge in 'digital arrests' (IndiaSpend, 2025). From approximately

- *Dead (static) Acquisition* – examining the hard drive on a powered-off system.
- *Live Acquisition* – collecting volatile memory as well as encryption keys and current connections (Review of Live Forensic Analysis Techniques, n.d., University of Maryland Global Campus, n.d.)
- *Chain of Custody* - As mentioned earlier, maintaining chain of custody throughout an investigation means keeping documentation on those who have had access to evidence and when they accessed it. One way this can be done is by verifying the hash values of data for all three systems (Digital Evidence Chain of Custody, 2024, Corpotech Legal, 2024).
- *Evidentiary Risk* – Performing dead analysis has its own set of risks, such as tampering with data during transportation (Digital Forensics Investigation Jurisprudence, n.d.). When performing live analysis, there are also some risks involved, including changes that could occur if you unplug a live system, thereby changing the timestamps (Digital Forensics Investigation Jurisprudence, n.d.).

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 07, July 2026)

When dealing internationally, obtaining proper legal instruments is necessary prior to starting evidence collection (IOSR Journal of Electronics and Communication Engineering, n.d.).

The use of artificial intelligence ("AI") and machine learning ("ML") tools to triage fraud evidence at scale has become an increasing necessity for investigators (see A Comprehensive Analysis of AI and ML in Modern Digital Forensics, n.d.). However, their admissibility has been challenged across jurisdictions. Daubert-based admissibility challenges have questioned whether AI algorithms meet standards for sufficient explainability and independent validation (See Reliability and Admissibility of AI-Generated Evidence, n.d.). In 2024, a Washington Court ruled that AI enhanced video was "not scientific knowledge" under Frye's Rule and thus could be excluded as evidence (See Maryland State Bar Association [MSBA] 2024).

More recently, India passed the Bharatiya Sakshya Adhiniyam, which replaces section 65B of the Indian Evidence Act with requirements that digital evidence must be certified both by its device custodian and another technical expert (KSandK Legal 2025; Naavi n.d.). Meanwhile, the European Union issued Regulation 2023/1543 to expedite cross-border data sharing via "Production and Preservation Orders" (White & Case 2023; Sachoulidou 2024)

III. Methodology

This paper uses a secondary-data, multi-method comparative design, integrating descriptive, analytical, and empirical approaches. Sources include official statistical reports (FBI, 2025; Europol, 2024; NCRB, 2026), peer-reviewed and preprint forensic-science literature, and primary legal texts (the Bharatiya Sakshya Adhiniyam, 2023; EU Regulation 2023/1543; Daubert/Frye case law), predominantly dated 2023–2026 to reflect each jurisdiction's active legal transition.

IV. Analysis And Findings

Table 1 compares the four investigative dimensions. India's case volume and losses are growing fastest of the three (NCRB, 2026; The420.in, 2025), straining forensic laboratory capacity that officials describe as already short-staffed (NCRB's Crime in India 2024 Report, 2026). The U.S. Recovery Asset Team's Financial Fraud Kill Chain achieved a 66% success rate freezing US$561 million in 2024 through rapid, AI-assisted transaction triage (CertifID, 2026; TRM Labs, 2025). India's I4C deployed comparable tools: the Pratibimb mapping system aided over 16,000 arrests, and the Suspect Registry flagged nearly 2.5 million mule accounts (NPAV, 2025). Europol coordinates rather than investigates directly, leaving live/dead acquisition to national authorities while supporting cross-border operations such as Operation Morpheus (Industrial Cyber, 2024).

Table 1. Comparative investigative and legal architecture, United States, European Union, and India.

Dimension	United States	European Union	India
2024 volume / losses	859,532 complaints; US$16.6B (FBI, 2025)	Ranked top-3 EU threat; IOCTA synthesis, not centrally tallied (Europol, 2024)	2.27M complaints; ₹22,845 crore (NCRB, 2026)
Admissibility test	Daubert / Frye, FRE 702 (Justice Speakers Institute, 2026)	National law + Reg. 2023/1543 mutual-trust model (Sachoulidou, 2024)	Sec. 63, Bharatiya Sakshya Adhiniyam (KSandK Legal, 2025)
Cross-border evidence	MLATs, CLOUD Act (Cross-Border Data Forum, 2023)	Production/Preservation Orders, 10 days–8 hrs (White & Case, 2023)	BSA drops old jurisdictional limit (IJLSSS, n.d.)
AI/ML evidentiary gap	Tested case-by-case; Washington v. Puloka (MSBA, 2024)	No EU-wide AI standard (ScienceDirect, 2026)	No AI provision in BSA (KSandK Legal, 2025)

No jurisdiction has codified AI-specific admissibility standards (MSBA, 2024; ScienceDirect, 2026; KSandK Legal, 2025), even as all three depend operationally on AI/ML triage tools (CertifID, 2026; NOTIONES, 2024; NPAV, 2025).

V. Discussion

Across all three systems, forensic technique has converged while legal doctrine has not (Maryman & Associates, 2026; Sachoulidou, 2024; KSandK Legal, 2025). India's strict, no-discretion certification rule is deployed in the system with the least forensic capacity relative to caseload (NCRB's Crime in India 2024 Report, 2026), while the EU's fast cross-border pipeline (White & Case, 2023) has not yet produced an EU-wide AI evidentiary standard, and U.S. courts continue testing AI evidence case-by-case under a three-decade-old Daubert framework (MSBA, 2024). Policy priorities that follow include dedicated AI-evidence legislation, expanded forensic laboratory investment in India, and multilateral adoption of the EU's Production/Preservation Order model given the transnational origin of most fraud infrastructure documented across all three jurisdictions' own reporting (TRM Labs, 2025; CyberPeace, 2026).

VI. Conclusion

Financial fraud and phishing investigation shows technical convergence, comparable acquisition and chain-of-custody practice, alongside legal divergence across American case law, European regulation, and Indian statute (FBI, 2025; White & Case, 2023; KSandK Legal, 2025). The consistent finding across all three jurisdictions is that AI-assisted evidence analysis has outpaced legal validation (Reliability and Admissibility of AI-Generated Evidence, n.d.), making this gap the most urgent shared reform priority. Future research should examine case-level prosecutions testing these frameworks in practice as the EU's e-Evidence Regulation and India's Bharatiya Sakshya Adhiniyam mature (Eurojust, 2026; NCRB, 2026).

REFERENCES

[1] White & Case LLP. (2023). EU breaks down digital borders: New e-Evidence rules facilitate cross-border investigations. https://www.whitecase.com/

[2] University of Maryland Global Campus. (n.d.). Data acquisition. https://lti.umuc.edu/

[3] TRM Labs. (2025). A record-breaking year for cybercrime: Key findings from the FBI's 2024 IC3 report. https://www.trmlabs.com/

[4] The420.in. (2025). NCRP data shows rapid growth in cybercrime cases across India. https://the420.in/

[5] ScienceDirect. (2026). The evolution of scientific evidence between artificial intelligence and legal validity. https://www.sciencedirect.com/science/article/pii/S1344622326000805

[6] Sachoulidou, A. (2024). Cross-border access to electronic evidence in criminal matters. New Journal of European Criminal Law. https://journals.sagepub.com/doi/10.1177/20322844241258649

[7] Review of live forensic analysis techniques. (n.d.). International Journal of Hybrid Information Technology, 8(2).

[8] Reliability and admissibility of AI-generated forensic evidence. (n.d.). arXiv. https://arxiv.org/pdf/2601.06048

[9] NPAV. (2025). India's cybercrime explosion: 22.68 lakh cases in 2024. https://blogs.npav.net/

[10] NOTIONES. (2024). What the cybercrime landscape looks like: Overview from the IOCTA 2024 report. https://www.notiones.eu/

[11] National Crime Records Bureau. (2026). Crime in India 2024 report. https://www.drishtiias.com/daily-updates/

[12] Nacha. (2025). FBI's IC3 finds almost $8.5 billion lost to business email compromise. https://www.nacha.org/news/

[13] Naavi. (n.d.). Section 63 of Bharatiya Sakshya Adhiniyam. https://www.naavi.org/wp/

[14] Maryman & Associates. (2026). Daubert digital forensics explained for legal professionals. https://maryman.com/

[15] Maryland State Bar Association. (2024). Applying Daubert and Frye to AI evidence. https://www.msba.org/

[16] LevelBlue. (2025). FBI 2024 IC3 report: Phishing soars, ransomware batters critical infrastructure. https://www.levelblue.com/

[17] KSandK Legal. (2025). Section 63 BSA 2023: Admissibility of electronic evidence. https://ksandk.com/litigation/

[18] Justice Speakers Institute. (2026). AI evidence admissibility: Frye, Daubert & AI. https://justicespeakersinstitute.com/

[19] IOSR Journal of Electronics and Communication Engineering. (n.d.). Chain of custody in multi-jurisdictional digital forensic investigations.

[20] Industrial Cyber. (2024). IOCTA 2024 report: Law enforcement deals major blows against EU cybercrime. https://industrialcyber.co/

[21] India Spend. (2025). #Data Viz: How India's cyber crime incidence is rising. https://www.indiaspend.com/

[22] IJLSSS. (n.d.). The Bharatiya Sakshya Adhiniyam: A framework for admitting electronic evidence in India. https://ijlsss.com/

[23] Federal Bureau of Investigation. (2025). FBI releases annual Internet Crime Report. https://www.fbi.gov/news/press-releases/

[24] Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. https://www.europol.europa.eu/

[25] European Commission. (n.d.). E-evidence – cross-border access to electronic evidence. https://commission.europa.eu/

[26] Eurojust. (2026). Electronic evidence. https://www.eurojust.europa.eu/judicial-cooperation/instruments/electronic-evidence

[27] Digital Forensics Investigation Jurisprudence: Issues of admissibility of digital evidence. (n.d.). Herald Open Access.

[28] Digital evidence chain of custody: Navigating new realities of digital forensics. (2024). ResearchGate. https://www.researchgate.net/publication/386361522

[29] CyberPeace. (2026). The data behind India's digital fraud surge. https://cyberpeace.org/resources/blogs/

[30] Cross-Border Data Forum. (2023). Navigating toward an EU-U.S. agreement on electronic evidence. https://www.crossborderdataforum.org/

[31] Corpotech Legal. (2024). Admissibility of electronic evidence, certificate and hash value, S 63 BSA. https://corpotechlegal.com/

[32] CertifID. (2026). 2024 FBI IC3 cybercrime report: A breakdown. https://www.certifid.com/article/fbi-ic3-cybercrime-report

[33] Bergman, P. (2024). Summary of the Internet Organised Crime Threat Assessment (IOCTA) 2024. https://paulbergman.org/

[34] Abnormal Security. (2025). 2024 FBI IC3 report: Business email compromise remains a multi-billion dollar threat. https://abnormal.ai/blog/2024-fbi-ic3-report

[35] A comprehensive analysis of AI and ML in modern digital forensics and incident response. (n.d.). arXiv. https://arxiv.org/pdf/2309.07064