

DIGITAL FORENSICS IN COMBATING ONLINE FINANCIAL CRIMES

Dr. Kunal Verma

Assistant Professor

Department of Computer Science and Digital Forensics

School of Computing and Information Security

University of Technology and Innovation, New Delhi, India

Abstract

Online financial crime has expanded beyond isolated card misuse to include phishing-led account takeover, mobile-payment fraud, business email compromise, synthetic identity abuse, cryptocurrency-enabled laundering, and coordinated money-mule networks. Digital forensics provides the disciplined process through which investigators identify, preserve, examine, interpret, and present electronic evidence associated with these offences. This paper offers an evidence-based analytical study of the role of digital forensics in combating online financial crimes. It examines how transaction records, device artefacts, authentication logs, network traces, email headers, browser history, cloud records, messaging data, and blockchain information can be combined to reconstruct criminal activity and connect events across platforms. The study does not claim a new survey, experiment, or crime dataset. Instead, it synthesises established digital-forensic principles, incident-response guidance, financial-crime typologies, and documented investigative practices. The analysis shows that the value of digital forensics lies not only in recovering data, but also in establishing integrity, time sequence, attribution pathways, evidential relevance, and a defensible chain of custody. The paper further identifies practical barriers, including rapid data deletion, cross-border infrastructure, encrypted communications, cloud dependence, anonymising services, fragmented reporting, and the need to protect personal information during investigation. It concludes that effective response requires coordinated procedures among financial institutions, cybercrime units, forensic laboratories, payment providers, regulators, and courts. Timely preservation requests, standardised logging, trained personnel, interoperable evidence handling, and privacy-aware analysis are central to improving detection, investigation, prosecution, and prevention of online financial crime.

Keywords: Digital Forensics, Online Financial Crime, Cyber Fraud, Electronic Evidence, Incident Response, Financial Investigation, Mobile Payment Fraud, Phishing, Blockchain Analysis, Chain of Custody

1. INTRODUCTION

Digital payment systems, internet banking, mobile wallets, online marketplaces, and cryptocurrency services have made financial activity faster and more accessible. The same systems, however, create opportunities for offenders to exploit stolen credentials, compromised devices, deceptive messages, weak identity controls, and complex transfer chains. A single fraud incident may involve a victim device, a spoofed website, an email account, a payment gateway, multiple bank accounts, remote servers, and communication platforms located in different jurisdictions. Investigators therefore require a method that can convert dispersed technical traces into reliable evidence.

Digital forensics is concerned with the careful identification, preservation, acquisition, examination, analysis, and reporting of information stored or transmitted in electronic form. In online financial-crime cases, the process may include securing a mobile phone used to receive a fraudulent link, preserving banking and payment logs, extracting browser artefacts, examining malware or remote-access tools, analysing email-routing data, and tracing the movement of funds through beneficiary accounts. The objective is not simply to find suspicious data. The objective is to demonstrate how the evidence relates to a specific event, person, device, account, or transaction while keeping the evidence authentic and reproducible.

The speed of financial fraud creates an important investigative challenge. Fraudsters may move funds through several accounts within minutes, instruct victims to delete messages, use temporary phone numbers, or rely on infrastructure that is quickly replaced. Consequently, delays in reporting and preservation can reduce the availability of valuable evidence. Banks, payment service providers, telecom operators, cloud platforms, and social-media companies may each retain different pieces of the evidential record. Effective digital forensics therefore depends on early coordination, legally valid data requests, clear escalation procedures, and the ability to prioritise volatile evidence.

The forensic perspective also helps distinguish suspicion from proof. A transaction anomaly may indicate possible fraud, but a complete case often requires corroboration from login records, device identifiers, communication content, account-opening records, beneficiary information, and witness statements. A well-documented forensic workflow can establish chronology, reveal repeated methods, identify links among cases, and support fair decision-making in administrative, civil, or criminal proceedings.

This study examines the contribution of digital forensics to online financial-crime investigation and prevention. It compares evidential sources across common fraud types, explains the main stages of a defensible forensic process, and outlines measures that can improve institutional readiness. The central argument is that financial institutions and law-enforcement bodies should treat digital evidence capability as a core

component of fraud resilience rather than as a technical activity used only after losses have occurred.

2. LITERATURE REVIEW

Digital-forensic research has developed from early work on computer evidence recovery into a broader discipline that addresses incident response, mobile devices, networked systems, cloud environments, and complex investigative coordination. Foundational models emphasise preservation, repeatability, documentation, and the separation of investigative stages so that results can be independently assessed. These principles are particularly important in financial-crime matters because electronic records may affect account restrictions, recovery attempts, disciplinary action, insurance decisions, and criminal proceedings.

The financial-crime literature highlights that online fraud is rarely confined to one technical channel. Credential harvesting may be followed by unauthorised login activity, changes to account settings, social engineering, rapid outward transfers, and cash-out through mule accounts or virtual assets. Research and operational guidance consequently stress the need to correlate technical evidence with transaction intelligence, customer communication, identity information, and legal records. Recent practice also gives greater attention to mobile-device evidence, cloud logs, encrypted data, blockchain tracing, and privacy safeguards because modern financial activity is increasingly platform based.

LITERATURE REVIEW SUMMARY TABLE

S. No.	Author / Year	Study Focus	Key Contribution	Limitations Identified
1	Palmer (2001)	Digital forensic research roadmap	Outlined core needs for reliable digital-evidence practice	Predates mobile, cloud, and current payment ecosystems
2	Carrier & Spafford (2003)	Digital investigation process	Explained a structured process for handling computer-related evidence	Focused largely on traditional computing environments
3	Casey (2011)	Digital evidence and computer crime	Connected technical examination with investigative and legal requirements	Broad reference; not limited to online financial crime
4	NIST	Forensics	Provided practical guidance for	Earlier guidance

	(2006)	within incident response	integrating forensic techniques into response	before widespread cloud and wallet adoption
5	FATF (2021)	Virtual assets and financial crime	Highlighted risk-based controls and tracing needs in virtual-asset activity	Concentrates on AML/CFT policy rather than complete forensic workflow

3. OBJECT OF STUDY

The primary focus of this research is to examine how digital-forensic methods support the detection, investigation, disruption, and evidential documentation of online financial crimes. The study considers how electronic artefacts, transaction records, communication data, platform logs, and device-level information can be correlated to reconstruct fraud activity. The main objects of study are outlined below:

3.1 ONLINE FINANCIAL-CRIME DOMAINS UNDER INVESTIGATION

- Phishing, smishing, vishing, and fake-website schemes used to obtain credentials or payment information
- Unauthorised access to internet-banking, mobile-wallet, card, and merchant-payment accounts
- Business email compromise, invoice manipulation, and fraudulent beneficiary-account changes
- E-commerce scams, card-not-present fraud, refund abuse, and marketplace payment deception
- Cryptocurrency fraud, investment scams, virtual-asset laundering, and wallet-based cash-out activity

3.2 DIGITAL EVIDENCE ENVIRONMENT

- Mobile-device artefacts, SIM and application data, browser history, screenshots, notifications, and local files
- Banking, payment-gateway, merchant, ATM, and transaction-monitoring logs
- Email headers, cloud-storage records, messaging content, social-media accounts, and voice-over-IP indicators
- Network records, IP addresses, device fingerprints, authentication events, malware traces, and remote-access evidence

3.3 FORENSIC EVALUATION PARAMETERS

- Integrity, authenticity, relevance, completeness, and lawful acquisition of electronic evidence
- Time sequencing of victim contact, credential compromise, account access, fund transfer, and cash-out events
- Ability to correlate persons, devices, accounts, phone numbers, IP addresses, and transaction beneficiaries
- Quality of chain-of-custody documentation, audit trails, validation, and reporting
- Protection of privacy, confidentiality, and legitimate customer information during investigation

3.4 COMPARATIVE ANALYSIS FOCUS

- Differences between evidence available in phishing, account takeover, payment fraud, business email compromise, and virtual-asset cases
- Device, network, cloud, transaction, and communication artefacts as complementary evidence sources
- Immediate containment needs versus longer-term evidential reconstruction and prosecution requirements
- Institutional responsibilities of banks, fintech firms, cybercrime units, forensic laboratories, and regulators

3.5 RESEARCH OBJECTIVE SCOPE

- To identify the principal digital evidence sources relevant to online financial-crime investigations
- To explain how digital-forensic stages contribute to reliable case reconstruction
- To assess operational gaps involving log retention, preservation, collaboration, skill, and legal process
- To recommend practical measures for stronger forensic readiness and fraud response

4. RESEARCH METHODOLOGY

The present study adopts a comparative and evidence-based research methodology. It synthesises established digital-forensic principles, incident-response guidance, financial-crime typologies, and documented investigative practices. The study is designed as a qualitative analytical paper and does not present an original survey, laboratory experiment, or statistical claim about fraud prevalence. This approach is appropriate because the availability and meaning of digital evidence depend on the fraud method, technology used, reporting speed, institutional policy, and applicable legal authority.

The analysis follows the pathway through which an online financial offence is initiated, facilitated, detected, and investigated. This pathway may begin with a deceptive message, compromised credential, malicious application, account takeover, manipulated payment instruction, or fraudulent merchant interaction. It then considers the digital traces generated during communication, authentication, payment authorisation, fund movement, cash-out, and post-incident contact. Each stage is assessed according to evidential value, volatility, access requirements, preservation needs, and potential for corroboration.

A comparative matrix is used to examine common fraud categories. The matrix evaluates primary evidence sources, forensic challenges, likely investigative priorities, and the relative urgency of preservation. It also distinguishes between evidence used for rapid containment, such as blocking an account or disabling a session, and evidence required for later attribution or prosecution, such as verified log records, device images, account-opening documents, and properly documented witness material.

The methodology recognises that technical evidence must be interpreted alongside financial and human context. An IP address does not by itself prove identity; an account transfer does not by itself establish intent; and a message may be altered, forwarded, or misunderstood. Accordingly, the study emphasises corroboration, validation, transparent documentation, and cautious inference. It also recognises that cross-border infrastructure, encrypted services, and privacy

law can affect access to data and the pace of investigation.

METHODOLOGY FRAMEWORK

1. The study uses a comparative design covering major categories of online financial crime.
2. Published digital-forensic, incident-response, and financial-crime sources support qualitative synthesis.
3. The analysis considers device, network, transaction, cloud, communication, and blockchain evidence.
4. Fraud categories are compared according to their typical digital footprints and preservation urgency.
5. Evidence integrity, chain of custody, lawful acquisition, and reporting are treated as core requirements.
6. The method distinguishes containment actions from evidential analysis and attribution work.
7. Institutional coordination among banks, payment providers, telecom entities, and investigators is evaluated.
8. Privacy, confidentiality, and proportionality are considered throughout evidence handling.
9. No fabricated transaction volumes, arrest statistics, loss figures, or prevalence rates are presented.
10. Recommendations focus on forensic readiness, timely preservation, skilled examination, and accountable governance.

5. DATA ANALYSIS

The data analysis section presents a comparative assessment of the digital evidence that may arise in online financial-crime investigations. The analysis is based on the operational characteristics of common fraud methods, typical electronic records, and accepted forensic principles. It does not treat any single log, device, or transaction as conclusive in isolation. Instead, it evaluates how multiple sources can be connected to establish a coherent and verifiable account of events.

Six online financial-crime settings are considered: phishing and credential theft, account takeover, business email compromise, payment-card and e-commerce fraud, mobile-payment or wallet fraud, and virtual-asset-enabled fraud. The comparison is qualitative because evidential value depends on platform

architecture, retention periods, user behaviour, legal process, technical controls, and the speed with which an incident is reported.

5.1 COMPARATIVE FORENSIC ANALYSIS

S. No	Crime Category	Primary Digital Evidence	Key Forensic Challenge	Response Priority	Risk Level
1	Phishing and credential theft	Fraudulent URLs, email headers, browser artefacts	Rapid takedown and short-lived sites	Preserve message, URL, and login data	Very High
2	Account takeover	Authentication logs, device IDs, IP/session records	Separating user error from unauthorised access	Freeze session, protect account	Very High
3	Business email compromise	Mailbox rules, headers, invoices, payment instructions	Impersonation and changed beneficiary data	Recall funds, preserve email trail	High
4	Card and e-commerce fraud	Order data, merchant logs, device fingerprinting	High transaction volume and disputed intent	Correlate payment, delivery, and account data	High
5	Mobile-payment or wallet fraud	App data, SMS, SIM records, transaction alerts	Volatile device and telecom evidence	Secure device, request provider logs	Very High
6	Virtual-asset enabled fraud	Wallet addresses, exchange records, blockchain transactions	Pseudonymity and cross-border services	Trace flows, preserve exchange data	High

5.2 EXTENDED FORENSIC EVALUATION

- Phishing and credential-theft investigations frequently begin with a suspicious email, text message, social-media post, or cloned website. Relevant evidence may include original message headers, sender-domain information, URL structure, webpage captures, downloaded files, victim browser history, and authentication events that follow the contact. Preservation is urgent because malicious sites and disposable accounts may disappear quickly. The evidential objective is to connect the deceptive communication to subsequent unauthorised access or payment activity without assuming that visual similarity alone proves source or intent.
- Account-takeover cases require close examination of login time, location indicators, device identifiers, multifactor-authentication activity, password-reset

records, session changes, payee additions, and transfer authorisations. Investigators must carefully distinguish between normal customer activity, shared-device use, and unauthorised access. A credible analysis combines technical logs with customer statements, account behaviour, recovery actions, and transaction chronology. The quality of logging and time synchronisation is often decisive.

- Business email compromise cases involve the manipulation of trust within a commercial relationship. Forensic work may include recovering mailbox rules, examining email headers, identifying lookalike domains, comparing invoice versions, reviewing changes to beneficiary account details, and tracing outgoing communications. Because instructions can appear legitimate, investigators should focus on message origin, sequence, account-control evidence, and verification

failures rather than relying solely on the content of a disputed email.

- Mobile-payment and wallet fraud may leave traces across the handset, SIM records, application logs, device backups, notification history, and payment-provider systems. The forensic response should preserve the device in a manner that prevents remote modification while respecting legal and privacy requirements. It is important to document the device state, power status, network condition, visible alerts, and acquisition method. Mobile evidence can corroborate social engineering, unauthorised application installation, SIM-swap indicators, and transaction approval events.
- Virtual-asset-related cases require a combination of blockchain analysis, exchange data, wallet records, communication evidence, and financial intelligence. Public ledger data can show movement among addresses, but it does not automatically identify the person controlling an address. Attribution may depend on exchange know-your-customer material, device artefacts, payment records, service-provider logs, and cross-border cooperation. Investigators must document analytical assumptions and avoid presenting clustering or tracing results as certain when they remain probabilistic.

5.3 OBSERVATIONS FROM DATA ANALYSIS

- Digital evidence is most useful when several independent sources support the same chronology of contact, access, transfer, and cash-out.
- Volatile sources, including active sessions, short-retention logs, disposable domains, and remote cloud data, require immediate preservation decisions.
- Transaction records establish financial movement, but device, communication, and authentication evidence are often needed to explain how and by whom the movement was initiated.
- Poor time synchronisation, incomplete logging, informal evidence collection, and undocumented handling can weaken otherwise valuable evidence.

- Financial institutions benefit from forensic readiness when they retain relevant records, identify responsible escalation teams, and maintain tested preservation procedures.
- Privacy and proportionality are not obstacles to investigation; they are requirements for lawful, trustworthy, and defensible evidence handling.
- Cross-platform collaboration is essential because a fraud pathway may involve banks, telecom providers, cloud services, merchants, social-media platforms, and virtual-asset providers.

6. DISCUSSION

The comparative analysis shows that digital forensics is central to the response to online financial crime because fraud is usually distributed across technologies and institutions. A customer complaint may identify the loss, but it does not reveal the full mechanism of compromise. The forensic process transforms a fragmented set of records into a documented sequence that can guide containment, recovery, attribution, and legal action. This requires more than specialist software. It requires organisational preparation, clear authority, reliable records, and communication among technical, financial, legal, and customer-support teams. Speed is particularly important in financial-crime investigations. Institutions must act quickly enough to preserve fragile evidence and interrupt further transfers, while also maintaining adequate records for later review. A rushed response that changes account settings, wipes a device, or fails to capture system state may reduce evidential value. Conversely, an overly slow process can allow funds to move beyond recovery or permit a fraud campaign to continue. The challenge is to build procedures that support both rapid action and disciplined documentation.

The analysis also demonstrates the limits of single-source attribution. An IP address can be routed through shared infrastructure, a phone can be borrowed, a payment account can be opened using false identity documents, and a cryptocurrency address can be controlled through intermediaries. Forensic conclusions should therefore state the strength and scope of the evidence, identify alternative explanations where relevant, and distinguish observed facts

from informed interpretation. This approach protects the rights of customers and suspects while increasing the credibility of legitimate cases.

A preventive approach is equally necessary. Financial institutions and fintech providers can improve outcomes by designing systems that create useful audit trails, support anomaly detection, permit rapid session control, and make preservation requests operationally clear. Staff training, customer awareness, secure authentication, transaction confirmation, incident simulations, and data-retention governance can reduce both the frequency of fraud and the difficulty of later investigation. Public authorities can support these efforts through standardised evidence practices, forensic capacity building, cross-border cooperation, and updated legal processes for digital records.

7. CONCLUSION

This study examined the role of digital forensics in combating online financial crimes across phishing, account takeover, business email compromise, mobile-payment fraud, e-commerce deception, and virtual-asset-enabled offences. The findings show that online financial crime produces a wide range of evidential traces, including device artefacts, authentication records, transaction data, emails, messages, network logs, cloud records, and blockchain activity. Their value depends

on timely preservation, lawful acquisition, technical validation, careful interpretation, and a complete chain of custody.

Different fraud categories demand different investigative priorities. Phishing and mobile-payment cases often require rapid capture of volatile communications and device data. Account-takeover cases depend heavily on authentication chronology and session evidence. Business email compromise requires detailed analysis of mailbox control and beneficiary changes. Virtual-asset cases require cautious tracing combined with exchange, device, and financial records. These differences confirm that a single generic fraud-response process is insufficient without specialised evidence pathways and trained personnel.

The study concludes that forensic readiness should be embedded within financial-crime governance. Clear log-retention standards, secure evidence-handling procedures, rapid preservation mechanisms, interoperable incident coordination, privacy-aware analysis, and accountable reporting can strengthen both response and prevention. Future research should examine the practical effectiveness of forensic-readiness programmes, artificial-intelligence-supported triage, cross-border evidence access, customer-protection safeguards, and the quality of digital evidence presented in financial-crime proceedings.

8. REFERENCES

1. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press.
2. National Institute of Standards and Technology. (2006). *Guide to Integrating Forensic Techniques into Incident Response* (SP 800-86). Gaithersburg, MD: NIST.
3. National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide* (SP 800-61 Rev. 2). Gaithersburg, MD: NIST.
4. National Institute of Standards and Technology. (2014). *Guidelines on Mobile Device Forensics* (SP 800-101 Rev. 1). Gaithersburg, MD: NIST.
5. International Organization for Standardization. (2012). *ISO/IEC 27037:2012: Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. Geneva: ISO.
6. International Organization for Standardization. (2015). *ISO/IEC 27041:2015: Guidance on Assuring Suitability and Adequacy of Incident Investigative Methods*. Geneva: ISO.
7. International Organization for Standardization. (2015). *ISO/IEC 27042:2015: Guidelines for the Analysis and Interpretation of Digital Evidence*. Geneva: ISO.
8. International Organization for Standardization. (2015). *ISO/IEC 27043:2015: Incident Investigation Principles and Processes*. Geneva: ISO.
9. Palmer, G. (2001). *A Road Map for Digital Forensic Research*. First Digital Forensic Research Workshop, Utica, NY.
10. Reith, M., Carr, C., & Gunsch, G. (2002). *An Examination of Digital Forensic Models*. *International Journal of Digital Evidence*, 1(3), 1-12.

11. Carrier, B., & Spafford, E. H. (2003). *Getting Physical with the Digital Investigation Process*. *International Journal of Digital Evidence*, 2(2), 1-20.
12. Beebe, N. L., & Clark, J. G. (2005). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. *Digital Investigation*, 2(2), 147-167.
13. Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated Digital Forensic Process Model. *Computers & Security*, 38, 103-115.
14. Garfinkel, S. (2010). Digital Forensics Research: The Next 10 Years. *Digital Investigation*, 7(S), S64-S73.
15. Rogers, M. K., & Seigfried, K. (2004). The Future of Computer Forensics: A Needs Analysis Survey. *Computers & Security*, 23(1), 12-16.
16. Quick, D., Choo, K.-K. R., & Castiglione, A. (2018). Digital Forensics: Challenges and Opportunities. *Future Generation Computer Systems*, 85, 1-3.
17. Federal Financial Institutions Examination Council. (2021). *Architecture, Infrastructure, and Operations Booklet*. Arlington, VA: FFIEC.
18. Financial Action Task Force. (2020). *Guidance on Digital Identity*. Paris: FATF.
19. Financial Action Task Force. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris: FATF.
20. Europol. (2023). *Internet Organised Crime Threat Assessment*. The Hague: Europol.
21. United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime*. Vienna: UNODC.
22. Association of Chief Police Officers. (2012). *Good Practice Guide for Digital Evidence*. London: ACPO.
23. Pollitt, M. M. (2010). A History of Digital Forensics. In *Advances in Digital Forensics VI*. Springer.
24. Cohen, F. (2008). *Digital Forensic Evidence Examination*. Frederick, MD: ASP Press.
25. Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.
26. Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.
27. Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organized Cybercrime or Cybercrime That Is Organized? An Assessment of the Conceptualization of Financial Cybercrime. *European Journal on Criminal Policy and Research*, 23, 287-300.
28. Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Routledge.
29. Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society* (3rd ed.). Sage.
30. European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape*. Heraklion: ENISA.