REVIEW PAPER

Digital Forensics in the Era of Cybercrime: A Systematic Review of Evidence on Integrity, Validation, Quality Assurance and Practice, 2016 to 2026

Running title: Digital forensics in the era of cybercrime: a systematic review

Authors: Dr. Anandita Singh, Dr. Abhishek Sheoran, Dr. Akshay Kumar, Dr. Kanika Kohli, Dr. K. K. Aggarwal

Dr. Anandita Singh, Junior Resident, Maharishi Markandeshwar Institute of Medical Science & Research, Mullana, Ambala, Haryana, India. Email: sherrysinghvns@gmail.com; Phone: +91 9651898916

Dr. Abhishek Sheoran, Junior Resident, MMIMSR, Mullana, Ambala, Haryana, India. Email: abhisheoran11@gmail.com; Phone: +91 9557777434

Dr. Akshay Kumar, Senior Resident, UPUMS, Saifai, Etawah, Uttar Pradesh, India. Email: akshayksaini339@gmail.com; Phone: +91 8630003176

Dr. Kanika Kohli, Professor, MMIMSR, Mullana, Ambala, Haryana, India. Email: kohlikanika1986@gmail.com; Phone: +91 9728405109

Dr. K. K. Aggarwal, Professor & Head of Department, MMIMSR, Mullana, Ambala, Haryana, India. Email: drkkaggarwal57@gmail.com; Phone: +91 9814195527

Keywords (MeSH): Forensic Sciences; Computer Security; Crime; Systematic Review; Evidence, Digital; Artificial Intelligence

Abstract

Background: Cybercrime is rising, and courts increasingly depend on digital evidence. It is unclear how reliable the evidence base for digital forensic practice is.

Objective: To synthesise empirical and structured evidence from 2016 to 2026 on the integrity, validation, quality assurance, practice and workforce conditions of digital forensics in cybercrime investigation.

Methods: This review followed PRISMA 2020 and was not registered. PubMed was searched for English language records from 2016 to 2026 and all 399 records were screened by title and abstract. Studies were extracted and appraised with a five item abstract based checklist, and findings were synthesised narratively.

Results: Twenty eight studies were included: 8 laboratory validations, 4 surveys, 4 qualitative studies, 3 document analyses, 1 Delphi study and 8 evidence syntheses. Sixteen were published in 2025 or 2026. Mean appraisal score was 3.84 of 5. Full file system extraction altered system files and logs between acquisitions, and file system anti forensic attacks went undetected by most of four tools tested. Peer review was mostly limited to reports. Seventeen percent of 94 examiners met criteria for post traumatic stress disorder. A language model pipeline reached an F1 score of 1.000 for wallet addresses in 273 fraud complaints.

Conclusions: Evidence supports hash documentation, tool validation, structured peer review and human supervised automation, but it is small, heterogeneous and rarely from India. Prospective multi centre validation is needed.

How to cite this article: Authors: Singh A, Sheoran A, Kumar A, Kohli K, Aggarwal KK. Digital Forensics in the Era of Cybercrime: A Systematic Review of Evidence on Integrity, Validation, Quality Assurance and Practice, 2016 to 2026. Int J Drug Deliv Technol. 2026;16(89s):356-368. DOI: 10.25258/ijddt.16.89s.37.

Introduction

Cybercrime is going up faster than the police can investigate it. In India, 86,420 cybercrime cases were registered in 2023, up 31% from 65,983 in 2022, and fraud made up 68.9% of them [1]. The FBI Internet Crime Complaint Center took in more than one million complaints in 2025, with reported losses near USD 20.9 billion [2]. Every one of these cases

has a victim, whether of cyberviolence or of a coercive scam such as the so called digital arrest [3,4], and nearly every one leaves digital traces that someone must turn into evidence a court will accept [5].

The legal side has also changed in India. Section 63(4) of the Bharatiya Sakshya Adhiniyam (BSA) 2023 asks for a certificate that gives the hash value of an electronic record and is signed by an expert, and in May 2026 the Supreme Court held that this requirement is valid [6]. The hash is therefore no longer a technical detail, because a certificate can fail on it. Whether the hash means what the certificate says depends on how the data were acquired and analysed, and that is a question for evidence, not opinion.

Modern phones make this harder. Manufacturers now use file based encryption, so the older ways of copying data no longer work and examiners have moved to full file system extraction. The phone has to be booted and its user data partition decrypted, and then files are read one at a time. While this goes on, apps keep running and the phone may connect to a network, so files can change under the examiner's hands [7]. A hash is a short fingerprint of a file, computed so that any later change shows up. If two acquisitions of the same phone give different hashes, a court can fairly ask which one to trust, and the examiner needs a ready answer.

Earlier reviews of digital forensics are mostly narrative, and they seldom say how the papers were found or chosen. We therefore did a systematic review to ask what the empirical and structured evidence from 2016 to 2026 tells us about the reliability, quality assurance, practice and workforce of digital forensics in cybercrime work, and where the gaps are. We also looked at what this means for India.

Methods

Protocol and reporting

We followed the PRISMA 2020 statement. The review was not registered in PROSPERO or anywhere else, and no protocol was published. Table 1 shows the eligibility criteria, and we applied them to every record.

Table 1. Eligibility criteria.

Element	Included	Excluded
Population or setting	Digital forensic practice, evidence or workforce in cybercrime or criminal investigation	Studies not about digital forensics
Design	Laboratory validation, survey, qualitative study, document analysis, Delphi study, or systematic or structured evidence synthesis	Narrative reviews, commentaries, overviews, conceptual frameworks without evaluation
Outcomes	Reliability, integrity, validity, quality assurance, practice, legal use, wellbeing, or accuracy of automation	Algorithm, dataset or single artefact papers without an evidentiary reliability outcome
Limits	English, 2016 to 2026, indexed in PubMed	Other languages or dates

Information sources and search

We searched PubMed in October 2026 for English language records from 2016 to 2026. PubMed was chosen because the main forensic science journals are indexed there and abstracts can be exported in one step. The search concepts were digital forensics, digital evidence, cyber and mobile forensics, anti-forensics, forensic tool validation, and artificial intelligence in digital investigation, joined with Boolean operators. This gave 399 unique records, all retrieved with their abstracts. Separately, we collected three official or legal sources (cybercrime statistics and the BSA ruling) for context only.

Study selection

One reviewer read the title and abstract of every record. Anything not about digital forensics was dropped first. The remaining abstracts were checked against Table 1 and excluded for one of three reasons: a narrative review, commentary or institutional overview; a conceptual framework with no empirical test; or a technical method, dataset or single artefact study with no result on evidentiary reliability. We did not retrieve full texts, so every decision rests on the abstract. A review was kept only if it used a systematic, structured or mapping method. We did not remove overlap between included syntheses and primary studies, because the syntheses cover far more literature than PubMed holds, and no primary study was counted twice in our numbers.

Data extraction and quality appraisal

From each included study we took the year, design, sample or data source and main findings, and placed it under one of five themes: integrity and tool validation; quality assurance and reporting; investigative, legal and organisational practice; workforce, wellbeing and education; and emerging technology. When a study fitted two themes we used the one closest to its main outcome. No validated appraisal tool fits such mixed designs, so we made a five item checklist: clear objective, suitable design, stated sample or data source, a reference standard or independent check, and stated limitations. Each item scored 1, 0.5 or 0, so totals run from 0 to 5. A total of 4.5 or more was called high, 3.5 to 4.0 moderate and below 3.5 lower. The items target the usual weak points in this field: vague aims, designs that cannot answer the question, undisclosed sample size, no comparison with a known truth or a second rater, and no mention of limits. Scores came from abstracts only, are indicative, and were not used to exclude anything.

Synthesis

The studies were too different for a meta-analysis. We summarised the findings in words, theme by theme, and drew a graph only where one study reported several comparable values.

Results

Study selection

The search found 399 records and no duplicates. Screening removed 130 that were not about digital forensics. Of 269 abstracts assessed, 241 were excluded: 49 narrative reviews, commentaries or overviews, 27 conceptual frameworks without an empirical test, and 165 technical method, dataset or single artefact studies. That left 28 studies (Figure 1). The 165 technical papers were mostly new detection algorithms for tampered images, audio and video, catalogues of artefacts from one app or device, or released datasets. They are useful engineering work, but they do not tell us whether evidence is reliable. The 49 narrative items were institutional reviews and commentaries, and the 27 frameworks proposed models for cloud, drone and Internet of Things settings that were never tested on casework or reference data.

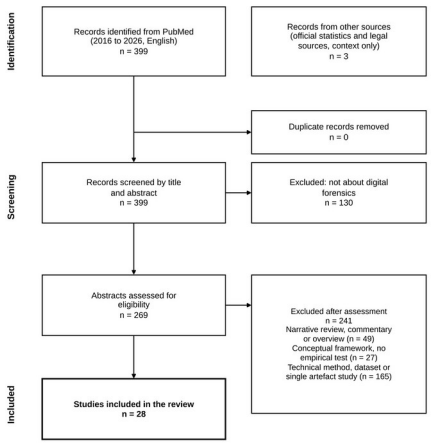


Figure 1. PRISMA 2020 flow diagram of record identification, screening and inclusion. Source: Search and screening record compiled for this review (PubMed, October 2026).

Characteristics of included studies

There were 8 laboratory validations, 4 surveys, 4 qualitative studies, 3 document analyses, 1 Delphi study and 8 evidence syntheses (Table 2). Sixteen of the 28 (57%) came out in 2025 or 2026, so the evidence is new and still thin. Integrity and tool validation was the biggest theme (8 studies), followed by practice and legal use (6), quality assurance and reporting (5), emerging technology (5) and workforce (4). Sample sizes varied a great deal, from a single trial case to 154 papers in the largest synthesis. The qualitative studies had 7 to 15 participants or units, the Delphi panel had 21 experts, and the surveys had 50 to 113 respondents. Only one abstract mentioned India, as one of four countries compared [8].

Table 2. Characteristics of the 28 included studies.

Study	Year	Design	Sample or data	Principal finding
Bhat [9]	2020	Experimental tool testing	4 tools, 11 anti-forensic attacks	Few attacks were detected by all tools; most went unnoticed
Yoo [7]	2026	Experimental, repeated acquisitions	Android smartphones, full file system extraction	System files and logs changed between acquisitions; user content largely retained integrity
Cuomo [10]	2022	Laboratory and field methodology	Mobile extractions from real court cases	Several hashes changed in extractions made minutes apart; repeatable and non repeatable procedures defined
Nash [11]	2025	Quasi experimental	60 images, 3 iPhones	Stream hashes matched in 100%; container hashes changed in the Photos app (100%) but not in the Files folder (0%)
Wales [12]	2025	Quantitative laboratory study	100 recordings, 11 iPhones, 5 models	Median presignal padding 2070.5 samples, above the 1024 expected; background noise reduced it
Sinaga [13]	2026	Comparative tool evaluation	3 tools, 4 smartphones	Artefact counts differed by tool and device; usability scores 71.0, 69.2 and 59.7
Ismail [14]	2025	Experimental, triplicate runs	4 tools (2 commercial, 2 open source), 3 scenarios	Open source tools gave reliable, repeatable results comparable to commercial tools
Sicbaldi [15]	2026	Systematic review and meta-analysis	Smartwatch validation studies, 4 brands	Heart rate most studied and most accurate; validation evidence heterogeneous

Study	Year	Design	Sample or data	Principal finding
Sunde [16]	2021	Content analysis of reports	40 reports from a quasi experiment	Conclusions were categorical or strength of support; reporting deficiencies and varied certainty wording
Bauge [17]	2025	Cross sectional survey	113 practitioners and managers, Norway and the UK	Peer review mostly limited to reports rather than verification of results and methods
Sunde [18]	2025	Mixed methods implement ation study	Norwegian police digital forensic units	Cognitive participation and reflexive monitoring strengthened; collective action stayed underdeveloped
Shin [19]	2023	Standards crosswalk and Delphi	21 experts, 3 rounds	40 laboratory components in seven areas derived
OliveiraJ r [20]	2022	Systematic mapping study	107 primary studies	Experiments often omitted hypotheses, variables, datasets and statistics
Zhang [21]	2022	Court document analysis	Sentencing documents, 2013 to 2018	Phone evidence in 3.3% of proceedings; messaging share rose from 1% (2015) to 25% (2018); mostly subsidiary evidence
Miller [22]	2022	Survey	50 US prosecutors, 51 investigator s	Training, specialist prosecutors and prosecutor and investigator relationships were crucial
Ng [23]	2025	Qualitative interviews	13 police officers, England and Wales	Digital evidence seen as objective yet fragile; officers carry interpretive burden
Bérubé [24]	2025	Qualitative case study	One terrorism related trial	Operational, technical and management constraints hindered accurate processing of traces
Saulen [8]	2026	Comparati ve doctrinal analysis	4 jurisdictions including India	Legal effect of digital records depends on the offence; documentation of source, authority and integrity needed
Casey [25]	2020	Interviews and requiremen ts analysis	15 Swiss digital forensic units	Prioritised requirements for inter regional knowledge management
Stricklan d [26]	2023	Interpretati ve phenomen ological analysis	7 UK analysts	Compassion fatigue, secondary traumatic stress and burnout symptoms reported
Tyagi [27]	2025	Cross sectional survey	94 examiners	36% sought counselling; 17% (n = 16) met PTSD criteria
Shortlan d [28]	2024	Rapid evidence assessment	34 articles	Exposure linked to burnout, secondary traumatic stress and turnover intentions
OliveiraJ r [29]	2025	Systematic mapping study	49 primary studies	Uneven landscape; professional training underexplored; few standard curricula
Ko [30]	2026	Validation study	273 complaints, 3 language models	F1 1.000 for wallets, 0.911 to 0.918 for URLs, 0.865 to 0.904 for loss; 31.1% sent to human review

Study	Year	Design	Sample or data	Principal finding
Zaheen [31]	2025	Systematic review	100 of about 1000 articles	AI improved accuracy and workflow; datasets small, external validation limited
Silva [32]	2024	Systematic literature review	29 ontologies	Ontology methods, types and evaluation approaches mapped to investigation phases
Kim [33]	2023	Literature review and survey	154 papers, 2015 to 2022	Cyber forensics research for smart cities limited compared with cybersecurity
Sonowal [34]	2026	Survey with multicriteria analysis	Deduplication methods, 6 adversarial threats	File level and fixed block methods scored highest (4.35 and 4.30); lossy methods below 3.0

Quality appraisal

The mean score was 3.84 out of 5. 6 studies were rated high, 20 moderate and 2 lower (Table 3), with totals from 2.0 to 5.0. Limitations were the weakest item: 13 of 28 abstracts mentioned none. Figure 2 gives the mean by theme. The high scorers were the file integrity tests with controls [11,9], the smartwatch meta-analysis [15], the Delphi study of laboratory standards [19], the language model validation [30] and the artificial intelligence review [31]. The two lower scores went to a field methodology report that gave no sample details [10] and a court document analysis whose abstract did not state the number of cases [21]. Since we scored abstracts, a missing item may only mean a short abstract.

Table 3. Quality appraisal of included studies (1 = yes, 0.5 = partly, 0 = no).

Study	Objective	Design	Sample	Reference check	Limits	Total	Rating
Bhat [9]	1	1	1	1	0.5	4.5	High
Yoo [7]	1	1	0.5	1	0	3.5	Moderate
Cuomo [10]	1	0.5	0	0.5	0	2	Lower
Nash [11]	1	1	1	1	1	5	High
Wales [12]	1	1	1	1	0	4	Moderate
Sinaga [13]	1	1	1	0.5	0	3.5	Moderate
Ismail [14]	1	1	1	1	0	4	Moderate
Sicbaldi [15]	1	1	0.5	1	1	4.5	High
Sunde [16]	1	1	1	1	0	4	Moderate
Bauge [17]	1	1	1	0.5	0.5	4	Moderate
Sunde [18]	1	1	0.5	1	0	3.5	Moderate
Shin [19]	1	1	1	1	0.5	4.5	High
OliveiraJr [20]	1	1	1	0.5	0.5	4	Moderate
Zhang [21]	1	1	0.5	0.5	0	3	Lower
Miller [22]	1	1	1	0	0.5	3.5	Moderate
Ng [23]	1	1	1	0.5	0	3.5	Moderate
Bérubé [24]	1	1	0.5	0.5	0.5	3.5	Moderate
Saulen [8]	1	1	1	0.5	0	3.5	Moderate
Casey [25]	1	1	1	0.5	0.5	4	Moderate
Strickland [26]	1	1	1	0.5	0	3.5	Moderate
Tyagi [27]	1	1	1	0.5	0	3.5	Moderate
Shortland [28]	1	1	1	0.5	0	3.5	Moderate
OliveiraJr [29]	1	1	1	0.5	0.5	4	Moderate
Ko [30]	1	1	1	1	0.5	4.5	High
Zaheen [31]	1	1	1	0.5	1	4.5	High
Silva [32]	1	1	1	0.5	0.5	4	Moderate
Kim [33]	1	1	1	0.5	0.5	4	Moderate
Sonowal [34]	1	1	0.5	1	0.5	4	Moderate

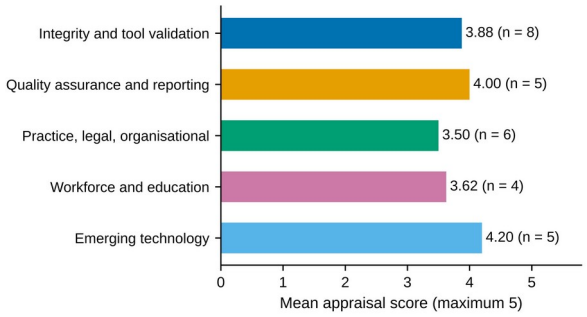


Figure 2. Mean appraisal score of included studies by theme.

Source: Calculated in this review from Table 3; scores are indicative and abstract based.

Evidence integrity and tool validation

Eight studies asked whether acquisition and tools keep evidence intact or expose its flaws. One team tested four forensic tools against eleven file system anti-forensic attacks, which hide data using ordinary file system features. Only a few attacks were picked up by all four tools, and most were missed [9]. In Android phones, full file system extraction changed system files and logs from one acquisition to the next, while user created content mostly stayed the same [7]. A methods paper built on real court cases found that several hashes changed between extractions made only minutes apart, and it separated repeatable from non repeatable procedures [10].

Some failures are quieter. When 60 images were downloaded from Dropbox to iPhones, the stream hash matched in all of them, but the container hash changed in every image saved through the Photos app and in none saved to the Files folder [11]. In 100 recordings from 11 iPhones, the zero padding at the start of encoded audio had a median of 2070.5 samples, well above the expected 1024, and it was smaller when background noise was higher [12]. Three widely used tools pulled very different artefact counts from the same phones (Figure 3). On an iPhone 11 Pro the first tool got 8,539 artefacts against 6,542 and 4,220. On an iPhone 13 Mini the third tool got 355,671 against 135,024 and 173,140. On a Xiaomi Android phone the counts were close (285, 280 and 329). The authors put much of the gap down to how artefacts are classified and where they come from, so a bigger count does not mean better evidence. Usability scores were 71.0, 69.2 and 59.7 [13].

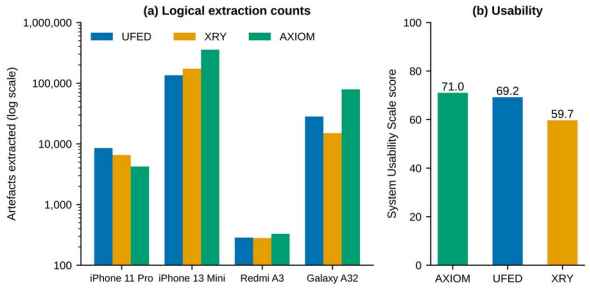


Figure 3. Tool comparison from one study: (a) artefacts extracted by three tools from four phones; (b) usability scores.

Source: Values reported in [13]; logical extraction, one device per model.

Two open source tools (Autopsy and ProDiscover Basic) were compared with two commercial ones (FTK and Forensic MagiCube) in triplicate runs of data preservation, recovery of deleted files by carving and targeted artefact search. The open source tools gave reliable, repeatable results comparable to the commercial ones [14]. A meta-analysis of smartwatch validation studies found heart rate the most studied and most accurate measure, but the evidence overall was uneven and most validation was done in healthy people in a laboratory [15]. Going back to the full file system study, the authors sorted files into five classes of forensic relevance and proposed two fixes: restore altered files from an initial reference image, or document every change made during acquisition [7].

Quality assurance and reporting

Reporting and review looked weaker than the technical work. Forty reports from a quasi experiment used either categorical conclusions or strength of support statements, the wording of certainty varied widely, and many content gaps matched those seen in other forensic disciplines [16]. In a survey of 113 practitioners and managers in Norway and the UK, peer review mostly meant checking the report, not the results or methods behind it [17]. The authors used a peer review hierarchy and found that the commonest reviews were the ones least likely to catch serious errors. A checklist based review trial in Norwegian police units improved cognitive participation and reflexive monitoring, but collective action stayed weak [18]. A Delphi panel of 21 experts, over three rounds, compared ISO/IEC 17025 and 27001 with Interpol and Council of Europe guidance and settled on 40 laboratory components in seven areas [19]. A mapping of 107 experiments found that hypotheses, variables, datasets and statistics were often not reported [20].

Investigative, legal and organisational practice

Digital evidence was used a lot, but often in a supporting role. In Chinese sentencing documents from 2013 to 2018, phone evidence appeared in 3.3% of proceedings, messaging apps grew from 1% to 25% of phone evidence between 2015 and 2018, and most phone data had little effect on the verdict [21]. A survey of 50 prosecutors and 51 investigators in the United States named training, prosecutors who specialise in digital evidence, and good working ties between prosecutors and investigators as the key factors [22]. Police officers in England and Wales described digital evidence as seemingly objective yet fragile, and they had to do the interpreting themselves [23]. In one terrorism trial, operational, technical and management constraints got in the way of processing digital traces correctly [24]. A comparison of four countries, India among them, showed that the legal weight of a digital record depends on the offence, and that source, authority and integrity checks need to be documented [8]. Interviews with 15 Swiss digital forensic units produced a ranked list of needs for sharing knowledge between regions [25].

Workforce, wellbeing and education

Seven UK analysts who work with child sexual abuse material described compassion fatigue, secondary traumatic stress and burnout. One of their themes was that once you know, you cannot unknow [26]. Among 94 digital and multimedia examiners, 36% had sought counselling and 17% (n = 16) met criteria for post traumatic stress disorder. Image analysts reported more distress and more barriers to asking for help, and examiners with the disorder described fears about their promotion [27]. A rapid evidence assessment of 34 articles linked exposure to traumatic material with burnout, secondary traumatic stress and intention to quit [28]. A mapping of 49 education studies found uneven coverage, little work on professional training and few standard curricula [29].

Emerging technology and artificial intelligence

A pipeline supervised by humans used three language models on 273 cryptocurrency fraud complaints. F1 scores were 1.000 for wallet addresses, 0.911 to 0.918 for web addresses and 0.865 to 0.904 for loss amounts, against 0.381 or lower for rule based baselines on loss (Figure 4). Of the actionable cases, 31.1% were sent to human review [30]. Two raters agreed closely (kappa 0.969 to 0.988), 96.7% of complaints held traceable identifiers, and

processing took 74 minutes at about USD 15, although sending complaints to commercial cloud services raises data sovereignty concerns. A systematic review of artificial intelligence in forensic medicine reported better accuracy and workflow but small datasets and limited external validation [31]. Other reviews mapped 29 ontologies for digital forensics [32], found little cyber forensics research for smart cities compared with cybersecurity across 154 papers [33], and ranked file level and fixed block deduplication highest on a reliability index (4.35 and 4.30) [34].

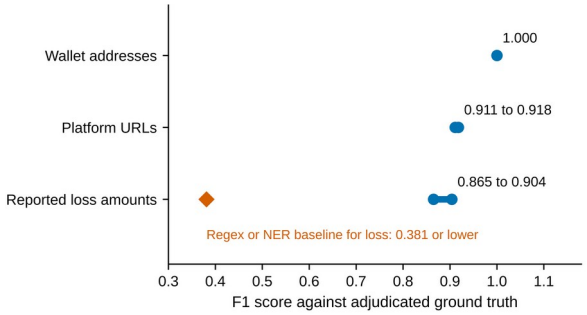


Figure 4. F1 scores of language model extraction from cryptocurrency fraud complaints.

Source: Values reported in [30].

Discussion

Principal findings

Technical integrity depends on conditions. Hashes of user created content held steady, but system files, containers and encoded streams changed, and most tools missed anti-forensic attacks. The human side lags behind the technical side: review was shallow, reports differed in how they stated certainty, and examiners carried a real psychological load. Automation helped when a person supervised it and when it was measured against ground truth.

A changed hash does not prove tampering, since operating systems and apps rewrite files all the time. Police and courts may not know this. Officers saw digital evidence as objective [23], and a trial case showed how constraints led to misreading [24]. The answer in both settings is explanation backed by documentation.

Figure 5 sets out how the threats and the controls connect. The controls are modest and can be tested: record every hash change, validate tools on reference data, review the results and not only the report, and state conclusions with explicit strength of support.

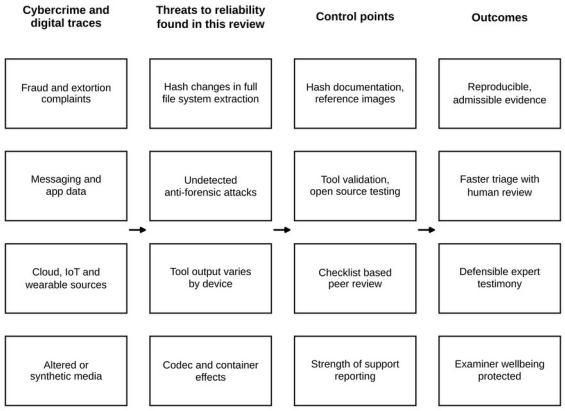


Figure 5. Mechanism diagram: how digital traces are threatened and which control points protect evidence.

Source: Original schematic synthesised from the included studies [9,7,11,12,17,18].

Implications for India

Section 63(4) BSA puts the hash at the centre of admissibility [6]. Going by these studies, a certificate should say which files may vary legitimately in full file system extraction, and laboratories should keep reference images and repeat acquisitions [7,10]. Open source tools look workable where money is short, as long as they are validated [14]. Tools should be picked for provenance and usability, not artefact count [13]. Fraud complaints can be triaged with language models if a human review queue is kept [30]. Checklist peer

review, standard laboratory components and support for examiners cost little [18,19,27]. Figure 6 puts these steps into one workflow. It is our own synthesis and has not been validated.

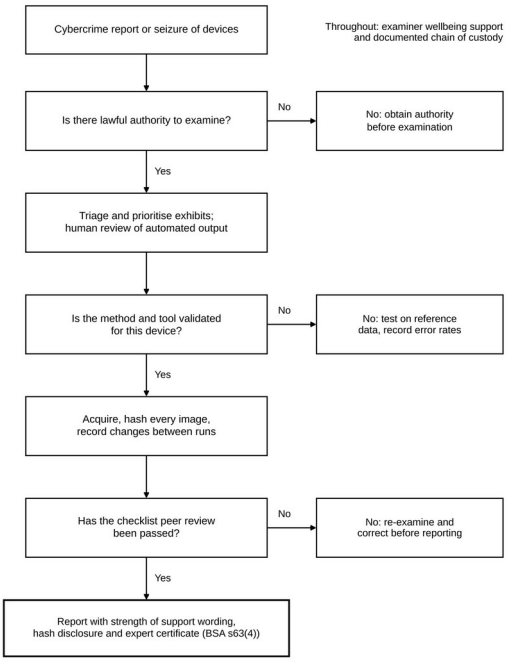


Figure 6. Evidence handling workflow for a cybercrime investigation.

Source: Authors' synthesis from [7,13,18,16,30,27]; not a validated protocol.

Limitations

The strengths are that every stage is counted, technical and human themes are covered together, and each study has an appraisal. The limits are real, though. We searched PubMed only, so computer science databases, where much technical work appears, were missed. Only one person screened, working from abstracts, with no second reviewer and no agreement statistic, so some records may be misclassified, particularly among the 165 technical studies we excluded. The checklist is not validated and rests on abstracts. The studies were too different to pool. Failed validations are rarely published, so publication bias is likely. The three official sources were news or legal commentary, not primary reports.

Future research

Several things are needed next: validation of acquisition tools against reference data in Indian multi centre settings, prospective evaluation of checklist review and accreditation, trials of wellbeing programmes for examiners, independent external validation of language model triage, and registered reviews that add computer science databases.

Conclusion

Hash documentation, validated tools, structured peer review and supervised automation have the best support so far. The evidence is small, varied and rarely Indian. Coordinated validation research and laboratory standards are needed before courts lean heavily on digital evidence.

Declarations

Conflict of interest: None

Funding: None

Ethics statement: Not applicable, as this review used published literature and public sources only

Registration: Not registered.

References

1. Press Trust of India. Cyber crimes show staggering jump of 31 pc in 2023 as compared to 2022: NCRB [Internet]. The Week; 2025 Sep 30 [cited 2026 Oct 19]. Report of National Crime Records Bureau, Crime in India 2023. No DOI or PMID (official statistics reported by news agency). Available from: https://www.theweek.in/wire-updates/national/2025/09/30/del87-ncrb-cyber-crime.html
2. CyberScoop. FBI Internet Crime Complaint Center annual cybercrime report [Internet]. Summary of the FBI IC3 2025 Internet Crime Report [cited 2026 Oct 19]. No DOI or PMID (official report summarised by news outlet). Available from: https://cyberscoop.com/fbi-

internet-crime-complaint-center-annual-cybercrime-report/

3. Nair AS, Anand N, Sharma MK. Lived experiences of individuals with cyberviolence: Understanding the nature of the dark side of social media use. Ind Psychiatry J. 2025;34(3):456-462. doi: https://doi.org/10.4103/ipj.ipj_67_25. PMID: https://pubmed.ncbi.nlm.nih.gov/41180056/
4. Robert SJ, Singh V, Pandey RP, Bhuyan B. Digital arrest in the cyber age: a psychological perspective on fear, authority, and consciousness. Front Psychol. 2026;17:1726740. doi: https://doi.org/10.3389/fpsyg.2026.1726740. PMID: https://pubmed.ncbi.nlm.nih.gov/41858474/
5. Klasén L, Fock N, Forchheimer R. The invisible evidence: Digital forensics as key to solving crimes in the digital age. Forensic Sci Int. 2024;362:112133. doi: https://doi.org/10.1016/j.forsciint.2024.112133. PMID: https://pubmed.ncbi.nlm.nih.gov/39089208/
6. SCC Online Blog. Hash value is an electronic fingerprint; Section 63(4) BSA certificate requirement is valid: Supreme Court [Internet]. 2026 Jul 8 [cited 2026 Oct 19]. Reports Pune Bar Association v Union of India, 2026 SCC OnLine SC 1297. No DOI or PMID (legal commentary). Available from: https://www.scconline.com/blog/post/2026/07/08/sc-upholds-admissibility-of-electronic-evidence-under-section-63-4-bsa/
7. Yoo S, Park Y, Jeong D. Preserving evidence integrity in full file system extractions: Assessing hash inconsistencies and potential solutions. J Forensic Sci. 2026;71(5):2070-2087. doi: https://doi.org/10.1111/1556-4029.70362. PMID: https://pubmed.ncbi.nlm.nih.gov/42124431/
8. Saulen N, Kanatov AK, Kozhantayeva ZK, Tlepbergenov O, Osmanova D. From cyberbullying to criminal liability: Digital forensic markers in cases of suspected abetment to suicide. Forensic Sci Int Synerg. 2026;13:100729. doi: https://doi.org/10.1016/j.fsisyn.2026.100729. PMID: https://pubmed.ncbi.nlm.nih.gov/42730233/
9. Bhat WA, AlZahrani A, Wani MA. Can computer forensic tools be trusted in digital investigations?. Sci Justice. 2020;61(2):198-203. doi: https://doi.org/10.1016/j.scijus.2020.10.002. PMID: https://pubmed.ncbi.nlm.nih.gov/33736854/
10. Cuomo R, D'Agostino D, Ianulardo M. Mobile Forensics: Repeatable and Non-Repeatable Technical Assessments. Sensors (Basel). 2022;22(18):7096. doi: https://doi.org/10.3390/s22187096. PMID: https://pubmed.ncbi.nlm.nih.gov/36146443/
11. Nash AE, Moe T, Wales GS. Exploring Dropbox image downloads to iPhone via safari: File system versus camera roll validation study. J Forensic Sci. 2025;71(1):405-412. doi: https://doi.org/10.1111/1556-4029.70173. PMID: https://pubmed.ncbi.nlm.nih.gov/40890941/
12. Wales GS. Quantitative study of zero-amplitude sample padding in iOS AAC encoding: Consistency across devices and the impact of background noise. J Forensic Sci. 2025;70(6):2309-2323. doi: https://doi.org/10.1111/1556-4029.70157. PMID: https://pubmed.ncbi.nlm.nih.gov/40830816/
13. Sinaga SJ, Asykar MA, Manurung H, Wibowo WC, Yazid S, Edwardo TO. Comparative evaluation of artifact extraction performance and usability in digital forensic tools: A study of Cellebrite UFED, MSAB XRY, and Magnet AXIOM. J Forensic Sci. 2026;71(4):1652-1661. doi: https://doi.org/10.1111/1556-4029.70320. PMID: https://pubmed.ncbi.nlm.nih.gov/41834190/
14. Ismail I, Akram Zainol Ariffin K. The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. PLoS One. 2025;20(9):e0331683. doi: https://doi.org/10.1371/journal.pone.0331683. PMID: https://pubmed.ncbi.nlm.nih.gov/40938950/
15. Sicbaldi M, Bartoli L, Albites-Sanabria J, D'Ascanio I, Silvani A, Chiari L, et al. Is my smartwatch a valid witness? A systematic review and meta-analysis. Forensic Sci Int.

2026;384:112901. doi: https://doi.org/10.1016/j.forsciint.2026.112901. PMID: https://pubmed.ncbi.nlm.nih.gov/41819643/

16. Sunde N. What does a digital forensics opinion look like? A comparative study of digital forensics and forensic science reporting practices. Sci Justice. 2021;61(5):586-596. doi: https://doi.org/10.1016/j.scijus.2021.06.010. PMID: https://pubmed.ncbi.nlm.nih.gov/34482939/
17. Bauge RK, Ryser E, Sunde N, Horsman G. Evaluating the scope of peer review in digital Forensics: Insights from Norway and the U.K. Sci Justice. 2025;65(2):139-148. doi: https://doi.org/10.1016/j.scijus.2025.01.005. PMID: https://pubmed.ncbi.nlm.nih.gov/40082060/
18. Sunde N, Dahl O. From intuitive to structured quality control: implementing checklist-based peer reviews of reports in Norwegian digital forensic units. Sci Justice. 2025;65(5):101298. doi: https://doi.org/10.1016/j.scijus.2025.101298. PMID: https://pubmed.ncbi.nlm.nih.gov/40930681/
19. Shin SM, Hong JW, Kim GB. Study on the standard components of digital forensics laboratory. J Forensic Sci. 2023;68(3):839-855. doi: https://doi.org/10.1111/1556-4029.15254. PMID: https://pubmed.ncbi.nlm.nih.gov/37078656/
20. OliveiraJr E, Silva TJ, Zorzo AF, Neu CV. Digital Forensics Experimentation: Analysis and Recommendations. Forensic Sci Rev. 2022;34(1):21-41. DOI not available. PMID: https://pubmed.ncbi.nlm.nih.gov/35105534/
21. Zhang A, Bradford B, Morgan RM, Nakhaeizadeh S. Investigating the uses of mobile phone evidence in China criminal proceedings. Sci Justice. 2022;62(3):385-398. doi: https://doi.org/10.1016/j.scijus.2022.03.011. PMID: https://pubmed.ncbi.nlm.nih.gov/35598931/
22. Miller CM. A survey of prosecutors and investigators using digital evidence: A starting point. Forensic Sci Int Synerg. 2022;6:100296. doi: https://doi.org/10.1016/j.fsisyn.2022.100296. PMID: https://pubmed.ncbi.nlm.nih.gov/37398922/
23. Ng M, Medhurst R, Dando CJ, Bull R. "A Ronin Without a Master": Exploring Police Perspectives on Digital Evidence in England and Wales. Behav Sci (Basel). 2025;15(10). doi: https://doi.org/10.3390/bs15101416. PMID: https://pubmed.ncbi.nlm.nih.gov/41153206/
24. Bérubé M, Beaulieu LA, Allard S, Denault V. From digital trace to evidence: Challenges and insights from a trial case study. Sci Justice. 2025;65(5):101306. doi: https://doi.org/10.1016/j.scijus.2025.101306. PMID: https://pubmed.ncbi.nlm.nih.gov/40930686/
25. Casey E, Zehnder A. Inter-regional digital forensic knowledge management: needs, challenges, and solutions. J Forensic Sci. 2020;66(2):619-629. doi: https://doi.org/10.1111/1556-4029.14613. PMID: https://pubmed.ncbi.nlm.nih.gov/33156519/
26. Strickland C, Kloess JA, Larkin M. An exploration of the personal experiences of digital forensics analysts who work with child sexual abuse material on a daily basis: "you cannot unsee the darker side of life". Front Psychol. 2023;14:1142106. doi: https://doi.org/10.3389/fpsyg.2023.1142106. PMID: https://pubmed.ncbi.nlm.nih.gov/37377701/
27. Tyagi S, Seigfried-Spellar KC. A behavioral health needs assessment and general psychological well-being of digital and multimedia forensic examiners. J Forensic Sci. 2025;71(1):72-89. doi: https://doi.org/10.1111/1556-4029.70207. PMID: https://pubmed.ncbi.nlm.nih.gov/41174856/
28. Shortland N, Crayne MP, Mezzapelle JL. Vicarious Trauma via the Observation of Extremist Atrocities: A Rapid Evidence Assessment. Trauma Violence Abuse. 2024;26(5):1097-1108. doi: https://doi.org/10.1177/15248380241305359. PMID: https://pubmed.ncbi.nlm.nih.gov/39717959/
29. OliveiraJr E, Zorzo AF. Review and agenda of Digital Forensics education and training. Forensic Sci Int. 2025;378:112655. doi:

https://doi.org/10.1016/j.forsciint.2025.112655 . PMID: https://pubmed.ncbi.nlm.nih.gov/41076964/

30. Ko S, Kim J, Jang JY, Kim G. Human-supervised LLM triage of pig butchering complaints: A validation study of multi-model identifier extraction. J Forensic Sci. 2026. doi: https://doi.org/10.1111/1556-4029.70411. PMID: https://pubmed.ncbi.nlm.nih.gov/42483775/
31. Zaheen U, Rakha A, Hassan Q, Khan MF, Akhtar S, Munawar A. A systematic review about the evolving role of artificial intelligence in various fields of forensic medicine. J Forensic Leg Med. 2025;117:103043. doi: https://doi.org/10.1016/j.jflm.2025.103043. PMID: https://pubmed.ncbi.nlm.nih.gov/41314025/
32. Silva TJ, OliveiraJr E, Zorzo AF. How Ontologies Have Supported Digital Forensics: Review and Recommendations. Forensic Sci Rev. 2024;36(2):99-125. DOI not available. PMID: https://pubmed.ncbi.nlm.nih.gov/39153741/
33. Kim K, Alshenaifi IM, Ramachandran S, Kim J, Zia T, Almorjan A. Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey. Sensors (Basel). 2023;23(7):3681. doi: https://doi.org/10.3390/s23073681. PMID: https://pubmed.ncbi.nlm.nih.gov/37050740/
34. Sonowal G, Rughani P, Gogia G. Forensic data deduplication: A comprehensive survey of methods and challenges for digital investigation. J Forensic Sci. 2026. doi: https://doi.org/10.1111/1556-4029.70480. PMID: https://pubmed.ncbi.nlm.nih.gov/42798236/