CYBERSTALKING, DIGITAL FORENSICS

The Role of Digital Forensics in Identifying Cyberstalkers

Oghenetega Avwokuruaye, Iloka Chike Betram, Hope Uzoamaka Anyaragbu, Okorie Emeka Anthony, Omeye Emmanuel Chizoba, Okeke Ogochukwu Clementina

Admiralty University of Nigeria, Ibusa, Delta State, Nigeria

Published October 2026

Abstract

Cyberstalking often involves repeated unwanted contact, monitoring, threats, impersonation, or the distribution of personal information through digital platforms. Identifying the person responsible can be difficult because offenders may use pseudonyms, temporary accounts, spoofed identifiers, virtual private networks, shared devices, or services that retain limited records. This article examines the role of digital forensics in identifying cyberstalkers and assessing the reliability of evidence used to attribute online activity. Drawing on literature concerning cyberstalking investigations, social-networking application artefacts, mobile-device forensics, and digital-evidence validation, it synthesises a practical investigative workflow. The workflow covers case scoping, lawful evidence acquisition, preservation and integrity checking, examination of devices and platform records, cross-source correlation, timeline reconstruction, attribution assessment, and reporting. The article distinguishes technical linkage to an account or device from identification of the human actor, and explains why behavioural patterns should be treated as corroborative rather than conclusive evidence. It also considers encryption, ephemeral messaging, cloud dependence, jurisdictional barriers, privacy, and the risk of misattribution. The article is conceptual and does not report new experimental findings. It concludes that digital forensics can strengthen cyberstalking investigations when methods are validated, alternative explanations are tested, and conclusions are expressed in proportion to the evidence.

Keywords: cyberstalking; digital evidence; digital forensics; evidence validation; mobile device forensics; offender attribution; social media

1 Introduction and literature review

1.1 Introduction

Digital communication enables people to maintain relationships, exchange information, and participate in public life. The same platforms can be misused to monitor, intimidate, threaten, impersonate, or repeatedly contact another person. Cyberstalking is generally associated with a pattern of unwanted conduct that causes distress or concern for safety, rather than a single unpleasant message in isolation. Legal definitions vary across jurisdictions, so investigators must relate observed conduct to the applicable law.

Identifying a cyberstalker presents both a technical and an evidential problem. An account name may be fabricated, a phone number may be spoofed, an account may be compromised, and an internet connection may be shared. A screenshot can document threatening content but may not independently establish who created it, whether the exchange is complete, or whether the displayed

timestamp is accurate. Investigators therefore need a structured process for preserving traces, testing their reliability, and determining whether independent sources support the same explanation.

Digital forensics provides methods for acquiring, preserving, examining, interpreting, and reporting information stored or transmitted by digital systems. Mobile-device guidance treats preservation, acquisition, examination, analysis, validation, and reporting as connected activities (Kim and Lee, 2020; Menahil et al., 2021). In cyberstalking cases, relevant sources may include a complainant's phone, a lawfully acquired suspect device, messaging and social-media artefacts, email records, cloud records, telecommunications information, and network logs.

1.2 Cyberstalking and digital evidence

Cyberstalking may include persistent unwanted messages, repeated attempts to contact a victim across platforms, surveillance of online activity, impersonation, threats, doxxing, or the use of technology to facilitate offline harassment. Conduct can migrate between services: a person blocked on one platform may contact the victim through another account, email, SMS, or a third party. A case file limited to one application can therefore omit context and make connected events appear unrelated.

Kaur et al. (2021) conducted a systematic literature review of cyberstalking research, identifying themes in prior work and directions for future research. Their review is relevant to understanding cyberstalking as a pattern of online conduct, but it is not a case study of a specific police investigation. Behavioural interpretation can guide investigative hypotheses, but it is not a substitute for technical evidence and cannot independently prove authorship. Research on social-networking forensics has demonstrated the value of examining application remnants on mobile devices, while showing that available artefacts vary across applications and platforms (Menahil et al., 2021; Arshad et al., 2025).

1.3 The attribution problem

Attribution is the assessment of whether evidence links an event to an account, device, network connection, or person. These are different levels of inference. A message may be linked to an account without proving that the account holder sent it. A device may contain an application but be shared or remotely accessed. An IP address may identify a connection used by a household, workplace, public network, or VPN endpoint rather than a specific individual. The investigator must state precisely what each source supports and what it cannot establish.

Research on anonymous and spoofed SMS resources highlights the difficulty of determining the origin of communications when services obscure or alter identifying information (Kaur et al., 2021; Santos et al., 2023). Such cases require careful correlation of device artefacts, service-provider records, timing, account-access information, and alternative explanations.

1.4 Aim and guiding questions

This article explains the contribution of digital forensics to identifying cyberstalkers and proposes a structured process for evaluating evidence. It asks: what sources can support a cyberstalking investigation; how should artefacts be acquired and validated; how can evidence be correlated to assess attribution; and what limitations prevent a digital trace from being treated as conclusive proof of identity?

2 Methodology and proposed forensic workflow

2.1 Article approach

This article uses a narrative, literature-informed approach drawing on research concerning cyber-stalking case analysis, social-networking artefacts, mobile-device forensic practice, and digital-evidence reliability, alongside technical guidance. It synthesises implications for an investigative workflow; it is not a systematic review and does not report new experimental results. The proposed workflow should be adapted to the law, capabilities, and procedures of the jurisdiction in which a case is investigated.

2.2 Proposed workflow

The workflow has seven iterative stages: (1) case scoping and hypothesis formation; (2) lawful collection and preservation; (3) acquisition and integrity verification; (4) examination of relevant artefacts; (5) cross-source correlation and timeline reconstruction; (6) attribution assessment and testing of alternatives; and (7) reporting and review (Table 1). New findings at one stage may justify returning to an earlier stage—for example, a timeline discrepancy may require further provider records or a review of the acquisition method.

Table 1. Proposed stages of a digital forensic investigation.

Stage	Main activities	Expected output
1. Scope	Document conduct, dates, platforms, identifiers, risks, and legal authority	Case plan and investigative questions
2. Preserve	Secure relevant devices and records; document condition, authority, and transfers	Evidence register and chain-of-custody record
3. Acquire and verify	Use suitable methods; record tool versions/settings; calculate and verify hashes	Acquisition files and integrity records
4. Examine	Review messages, account identifiers, databases, notifications, media, browser artefacts, and logs	Artefact inventory with provenance and limitations
5. Correlate	Normalise timestamps, compare sources, build an event timeline, and document conflicts	Correlated timeline and relationship map
6. Assess attribution	Evaluate account, device, network, and person-level links; test alternatives	Attribution assessment with uncertainty
7. Report and review	Explain methods, findings, exclusions, limitations, and reproducibility	Report suitable for investigative and legal scrutiny

2.3 Case scoping and hypothesis formation

Investigators should translate a complaint into testable questions: whether repeated messages came from the same account, whether multiple accounts share relevant access indicators, whether an account was active at the alleged times, and whether separate incidents form a connected sequence. Alternative hypotheses should be recorded early. An account may have been compromised; a device may be shared; a sender identifier may be spoofed; or two events may be coincidental. This reduces the risk of interpreting ambiguous artefacts only in ways that support an initial suspicion.

2.4 Lawful collection and preservation

Collection should be proportionate and supported by appropriate consent, warrant, statutory authority, or another lawful basis. The scope should identify the devices, accounts, time ranges, and data categories sought. Investigators should document the condition of each item, who supplied it, and every transfer or action that may affect the evidence. Screenshots can preserve visible content quickly, but they are not necessarily a substitute for underlying message data, metadata, or a forensic acquisition where those sources are lawfully available.

Mobile devices can change state through notifications, background synchronisation, clock updates, or remote commands. Isolation or powering down may preserve some evidence but may also cause loss of volatile data or prevent access to encrypted content. Decisions should be case-specific and documented, consistent with recognised mobile-forensic guidance (Menahil et al., 2021).

2.5 Acquisition, integrity, and chain of custody

Acquisition methods should suit the device, operating system, application, and legal authority. Investigators should record the tool and version, configuration, date and time, operator, errors, and limitations. Cryptographic hashes help demonstrate that a particular acquired file or image has not changed since the hash was calculated. A matching hash does not prove that the original information was truthful, complete, or authored by a particular person; it supports integrity of the hashed item during subsequent handling.

Chain-of-custody documentation should identify who collected, transferred, stored, accessed, examined, and returned or disposed of each item, with dates, times, purposes, and relevant signatures or system logs. Brunty (2023) and Stoykova and Franke (2023) advocate explicit reliability validation across technology, method, and application levels, supporting the need to document how a result was produced rather than only recording the final output.

2.6 Examination of digital artefacts

Potential sources include the victim's device, a lawfully acquired suspect device, application databases, browser history and caches, notification records, email headers, SMS and call records, cloud backups, account login alerts, platform preservation responses, and network or telecommunications records. Not every source will be available or relevant. Investigators should distinguish data collected directly from a device from information supplied by a provider or copied into a screenshot, and document the provenance of each artefact.

Applications differ in how they store messages, attachments, account identifiers, timestamps, and deletion states. Some information may remain in local databases or caches; other information may only be available from a provider or may no longer exist. Encryption, updates, retention policies, and remote deletion can limit recovery. Findings from one application version should not be assumed to apply to every version or operating system. Studies of disappearing-message applications also show that retention and recovery depend on application behaviour and acquisition conditions (Vasilaras et al., 2022).

2.7 Correlation and timeline reconstruction

A message on the victim's device may be compared with a notification record, a corresponding conversation database on another device, platform records, and relevant account-access information. Investigators should assess whether sources are genuinely independent. Two screenshots of the

same conversation are not independent confirmation, and several records generated by one application may share the same underlying clock or database.

Timeline reconstruction requires attention to time zones, daylight-saving settings, device clock drift, server timestamps, and the distinction between creation, delivery, receipt, display, and export times. The report should state its time basis and preserve original timestamps alongside normalised values. Missing events should be treated as gaps rather than silently inferred. Conflicting records should be described and investigated rather than resolved by selecting the time that best fits a preferred account.

2.8 Attribution assessment

Attribution should be expressed in layers. First, determine whether an artefact is associated with an account or service. Second, assess whether it is linked to a device or network session. Third, evaluate whether evidence supports the conclusion that a particular person controlled the account or device at the relevant time. The final step may require evidence beyond digital artefacts, including access-control records, admissions, witness evidence, contextual knowledge, or other independently obtained information.

Repeated phrases, knowledge of non-public information, timing patterns, and sequences of accounts may be relevant contextual indicators. However, such characteristics can be imitated, shared, or explained by common sources. Behavioural evidence should be presented as supporting context, not as a unique forensic signature that identifies a person.

2.9 Reporting and review

A defensible report distinguishes observations, interpretations, and conclusions. It states what was examined, what was unavailable, which tools and methods were used, how integrity was assessed, what supports or weakens each hypothesis, and what uncertainty remains. Conclusions should not be categorical where evidence establishes only a weaker association. Independent review of critical steps can help detect errors in tool outputs, timestamp conversions, and attribution reasoning.

3 Evidence sources and their investigative value

The value of a source depends on the question asked and the reliability of the records obtained. No single source is universally decisive. The main sources and their limitations are summarized in Table 2.

Table 2. Common sources of evidence in cyberstalking investigations.

Source	Potential value	Key caution
Victim's device	Messages, calls, notifications, media, account identifiers, local databases, browser artefacts	Receipt or display does not independently prove who authored the content
Suspect device (lawfully acquired)	Local conversations, account sessions, cached data, attachments, drafts, and application traces	Presence on a device does not prove who used it at the relevant time
Platform/provider records	Account details, session data, login records, reported content, and retained message metadata	Retention, encryption, jurisdiction, and registration accuracy limit interpretation

Source	Potential value	Key caution
Email, SMS, telecom records	Routing information, timestamps, identifiers, and subscriber or call records	Spoofing, number reassignment, shared subscriptions, and intermediary services complicate attribution
Network and access logs	Connection times, IP addresses, authentication events, and access patterns	VPNs, public Wi-Fi, shared networks, NAT, and clock differences impede person-level attribution
Cloud backups	Additional message copies, attachments, synchronised records, and records absent locally	Backups may be incomplete, stale, or reflect a different device state
Screenshots and exports	Rapid documentation of visible content and contextual details	May be edited, cropped, misdated, or lack underlying metadata

3.1 Social media and messaging artefacts

Relevant artefacts may include user IDs, profile URLs, message IDs, conversation participants, attachment hashes, post identifiers, edit or deletion indicators, and account-access events. Stable identifiers are useful because display names and profile photographs can change. Where providers offer formal preservation or legal-request processes, requests should specify accounts, time ranges, record types, and the legal basis. Recent work on social-media forensic methods likewise emphasises systematic collection and analysis of platform-specific artefacts (Arshad et al., 2025).

The absence of a message on one device does not prove that it was never sent. It may have been deleted, synchronisation may have failed, the application may store only a subset of records locally, or the data may exist elsewhere. Conversely, a recovered fragment should not automatically be represented as a complete conversation. Reports should distinguish complete messages, partial bodies, metadata-only artefacts, and reconstructions based on multiple sources.

3.2 Network, IP, and subscriber information

Network evidence may narrow the possible connections used to access an account, but an IP address is not a person identifier. It may be shared through network address translation, dynamically assigned, associated with a VPN endpoint, or used by a public access point. Attribution requires time-aligned records and an understanding of how the service, ISP, and local network allocate addresses. A subscriber record identifies a subscriber, not necessarily the individual who performed a specific action.

3.3 Behavioural evidence and context

Context helps investigators assess whether events form a pattern of persistent conduct. The sequence of contact attempts, escalation, references to offline events, use of multiple channels, and relationship to reported incidents may be relevant. Kaur et al. (2021) describe BEA as an aid to interpretation and reconstruction, but such analysis is vulnerable to hindsight bias if similarities are interpreted as confirmation after a suspect has already been selected. Competing explanations and disconfirming evidence must remain visible.

4 Discussion

4.1 Strengthening the evidential chain

The contribution of digital forensics is not simply to retrieve more data; it is to provide a transparent chain of reasoning from collection to conclusion. Acquisition preserves a defensible copy, examination identifies artefacts and their provenance, correlation tests whether sources support the same event sequence, and validation evaluates the reliability of tools, methods, and interpretations. This layered approach is consistent with mobile-device guidance and research advocating structured reliability validation (Stoykova and Franke, 2023).

4.2 Interpreting evidence at the correct level

A frequent analytical error is moving directly from technical association to human identity. Evidence may show that an account sent a message, that a device contained a session for the account, or that a network connection accessed a service. Each proposition is different. Person-level conclusions generally require additional evidence connecting the account or device to the individual at the relevant time. The strength of a conclusion should reflect the quality, independence, and consistency of supporting sources and the plausibility of alternatives.

4.3 Tool reliability and reproducibility

Forensic software can parse databases, extract files, recover artefacts, and generate timelines, but its output is not self-authenticating. Investigators should understand tool limitations, test tools against known data where feasible, retain logs, and verify critical findings through independent methods when possible. Reliability validation should consider technology, method, and application; a tool may perform differently across devices, operating systems, or application versions (Stoykova and Franke, 2023). A structured validation process is therefore necessary before relying on tool output in a consequential investigation (Brunty, 2023).

4.4 Practical, legal, and ethical constraints

Investigations may be constrained by end-to-end encryption, disappearing messages, remote deletion, device lock states, cloud retention limits, platform policies, and cross-border legal process. Evidence should be preserved promptly, but collection must remain within legal authority and avoid unnecessary intrusion into unrelated personal information. Devices may contain sensitive material about family members, colleagues, and other third parties; access should be restricted and collection proportionate.

A case may involve hundreds of messages across several services. Search, clustering, and timeline tools can assist triage, but output must be checked for false matches, lost context, and errors involving slang, images, or common phrases. Automated risk scores should not be treated as proof of identity or intent. Investigators should also actively consider exculpatory information, such as shared access or evidence that an account was compromised. Research into NLP-based digital-forensic analysis of online social networks illustrates the potential role of automated analysis, while its output still requires contextual evaluation (Shahbazi and Byun, 2022).

4.5 Implications for investigators

Investigators should prioritise preservation, maintain a clear chain of custody, use methods suitable for the relevant platform, preserve original values and metadata, and separate observation from

inference. They should seek corroboration from genuinely independent sources and explain what each source can and cannot prove. This discipline supports both the prosecution of genuine offenders and the exclusion of wrongly suspected individuals.

5 Limitations, future research, and conclusion

5.1 Limitations

This article is a narrative synthesis and proposed workflow, not a systematic review or empirical evaluation. It does not measure artefact recovery rates, compare commercial tools, or estimate attribution accuracy. The sources discussed are not exhaustive, and application behaviour changes across operating systems, versions, and service configurations. The workflow is therefore a conceptual model that requires adaptation and evaluation in specific investigative settings.

5.2 Future research

Future work could evaluate the workflow using controlled cyberstalking scenarios with known ground truth, including spoofed SMS, multiple accounts, shared devices, deleted messages, VPN use, and cross-platform contact. Possible metrics include artefact recovery rate, precision and recall of event extraction, timeline accuracy, source-correlation accuracy, false-attribution rate, processing time, and inter-examiner agreement. Studies should document devices, application versions, acquisition methods, and ground-truth events to support replication.

Further research should examine how uncertainty is communicated to courts and non-technical decision-makers. A useful reporting model could distinguish account linkage, device linkage, network linkage, and person attribution, identifying the evidence required to move between levels. Additional work is needed on privacy-preserving triage, analysis of encrypted or ephemeral messaging, and cooperation between investigators, service providers, and telecommunications operators.

5.3 Conclusion

Digital forensics plays an important role in identifying cyberstalkers by enabling investigators to preserve and analyse traces of communication, account access, device use, and online behaviour. Its strongest contribution emerges when evidence from several sources is acquired lawfully, preserved with documented integrity, examined using suitable methods, and correlated in a transparent timeline. Social media artefacts and behavioural context can help reconstruct events, but neither should be used in isolation to make a definitive claim about a person's identity.

Identification should be treated as a graduated evidential process, not a simple match between a username, IP address, phone number, or device and a suspect. A reliable investigation validates its methods, tests alternative explanations, records uncertainty, and distinguishes what the evidence demonstrates from what remains inference. These principles can strengthen cyberstalking investigations while reducing the risk of unreliable conclusions and wrongful attribution.

References

[1] Arshad M, Ahmad AA, Choo CW, Sam EA (2025). Investigating methods for forensic analysis of social media data to support criminal investigations. *Frontiers in Computer Science*, 7, 1566513. https://doi.org/10.3389/fcomp.2025.1566513

[2] Brunty J (2023). Validation of forensic tools and methods: a primer for the digital forensics examiner. *WIREs Forensic Science*, 5(2), e1474. https://doi.org/10.1002/wfs2.1474

[3] Casino F, Dasaklis TK, Spathoulas GP, Anagnostopoulos M, Ghosal A, Borocz I, Solanas A, Conti M, Patsakis C (2022). Research trends, challenges, and emerging topics in digital forensics: a review of reviews. *IEEE Access*, 10, 25464–25493. https://doi.org/10.1109/ACCESS.2022.3154059

[4] Heath H, MacDermott Á, Akinbi A (2023). Forensic analysis of ephemeral messaging applications: disappearing messages or evidential data? *Forensic Science International: Digital Investigation*, 46, 301585. https://doi.org/10.1016/j.fsidi.2023.301585

[5] Hyder MF, Arshad S, Fatima T (2024). Toward social media forensics through development of iOS analyzers for evidence collection and analysis. *Concurrency and Computation: Practice and Experience*. https://doi.org/10.1002/cpe.8074

[6] Kaur P, Dhir A, Tandon A, Alzeiby EA, Abohassan AA (2021). A systematic literature review on cyberstalking: an analysis of past achievements and future promises. *Technological Forecasting and Social Change*, 163, 120426. https://doi.org/10.1016/j.techfore.2020.120426

[7] Kim D, Lee S (2020). Study of identifying and managing the potential evidence for effective Android forensics. *Forensic Science International: Digital Investigation*, 33, 200897. https://doi.org/10.1016/j.fsidi.2019.200897

[8] Menahil A, Iqbal W, Iftikhar M, Shahid WB, Mansoor K, Rubab S (2021). Forensic analysis of social networking applications on an Android smartphone. *Wireless Communications and Mobile Computing*, 2021, 5567592. https://doi.org/10.1155/2021/5567592

[9] Santos ILS, Pimentel CE, Mariano TE (2023). Cyberstalking scale: development and relations with gender, FOMO and social media engagement. *Current Psychology*, 42, 4802–4810. https://doi.org/10.1007/s12144-021-01823-3

[10] Shahbazi Z, Byun YC (2022). NLP-based digital forensic analysis for online social network based on system security. *International Journal of Environmental Research and Public Health*, 19(12), 7027. https://doi.org/10.3390/ijerph19127027

[11] Stoykova R, Franke K (2023). Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International: Digital Investigation*, 45, 301554. https://doi.org/10.1016/j.fsidi.2023.301554

[12] Vasilaras A, Dosis D, Kotsis M, Rizomiliotis P (2022). Retrieving deleted records from Telegram. *Forensic Science International: Digital Investigation*, 43, 301447. https://doi.org/10.1016/j.fsidi.2022.301447

[13] Wijnberg D, Le-Khac NA (2021). Identifying interception possibilities for WhatsApp communication. *Forensic Science International: Digital Investigation*, 38, 301132. https://doi.org/10.1016/j.fsidi.2021.301132