Quantum Security in Forensic Investigation for the Analysis of Chatbot-Linked Crimes on Social Media: A Framework for Post-Quantum Digital Evidence Preservation

Dr. Heena Goswami

Assistant Professor of Science and Technology, Gujarat National Law University, Gandhinagar, Gujarat-INDIA
Email: hgoswami@gnlu.ac.in & goswamiheena@gmail.com

Abstract
The growth of social media crime has changed digital forensic practice by increasing the volume, velocity, and volatility of evidence associated with chatbot-mediated offenses. Chatbots are now implicated in phishing, impersonation, fraud, grooming, coordinated disinformation, and automated social engineering campaigns that often cross multiple platforms. At the same time, the emerging quantum computing era introduces new security risks to digital evidence, particularly for systems that rely on conventional public-key cryptography for storage, transfer, and verification. This paper examines the role of quantum security in forensic investigation, focusing on the analysis of chatbot-linked crimes on social media and the need to preserve evidential integrity in a post-quantum environment. Drawing on recent work in social media forensics, digital evidence governance, and quantum forensics, the paper proposes a conceptual framework combining post-quantum cryptography, immutable logging, federated evidence processing, and AI-assisted chatbot trace analysis. The paper argues that future forensic practice must address both the forensic challenges posed by chatbot-enabled crime and the cryptographic threats posed by quantum computing if courts are to receive trustworthy, admissible digital evidence.

Keywords- Chatbots, Social media, Forensic Investigation, Linked-crimes

Introduction

Social media platforms have become major spaces for criminal communication, social engineering, fraud, harassment, and coordinated manipulation. These environments are especially significant in cases involving chatbots, because automated conversational systems can be used to imitate users, amplify harmful messaging, collect personal information, or facilitate phishing and impersonation at scale. In forensic practice, such cases are difficult because social media evidence is highly volatile and often distributed across multiple jurisdictions, platforms, and device types.

The forensic response to this challenge has traditionally relied on digital evidence preservation, chain of custody, and structured investigative procedures. However, modern platforms create evidence that may disappear quickly, be altered by users, or be stored on systems beyond the immediate control of investigators. Recent social media forensics research therefore emphasizes automation, blockchain-based preservation, and federated learning to protect integrity while enabling large-scale evidence analysis. At the same time, quantum computing creates a new layer of risk because standard cryptographic systems may eventually be vulnerable to quantum attacks, creating long-term concerns for evidence confidentiality and authenticity.

This paper argues that forensic investigation of chatbot-linked crimes on social media should be designed as a post-quantum digital forensic process. Such a process must preserve evidence securely, analyze chatbot behavior across platforms, and ensure that stored artifacts remain trustworthy even in a future where quantum adversaries may be capable of breaking current cryptographic protections.

Quantum Security Context

Quantum security refers to security mechanisms designed to resist or leverage quantum computational capabilities. In forensic investigation, the most important concern is not that investigators need quantum computers themselves, but that evidence systems must remain secure against future quantum-enabled attacks on encryption, authentication, and digital signatures. Research in quantum forensics and post-quantum security highlights the need to adapt digital forensic frameworks to quantum-era threats by using quantum-resistant algorithms and updated investigative methodologies.

Forensic Investigations rely on three key things: keeping information secret, making sure it's accurate, and verifying its source. But quantum computers can compromise all of these if the systems used to protect evidence aren't secure against quantum attacks. This is a big deal, especially when it comes to social media investigations. Think about all the digital evidence that's collected - logs, messages, screenshots, and metadata. This information is often stored in cloud systems or saved for long periods of time before it's presented in court. If the encryption used to protect this evidence becomes outdated, it can call into question the entire chain of evidence. When it comes to dealing with post-quantum cryptography, a sensible approach is to view it as a way to preserve and control data, rather than just a minor technical tweak. This means that systems used to investigate crimes should be designed to keep evidence safe and secure throughout the entire process.

It's especially important for crimes that involve chatbots, because investigators need to be able to connect the dots between the content generated by these automated systems and other clues like account logs, device artifacts, and network traces. By doing so, they can ensure that evidence remains trustworthy, timestamped, and protected from tampering. This way, even if quantum computers become powerful enough to break current encryption methods, the evidence will still be reliable and admissible in court. In essence, treating post-quantum cryptography as a preservation control helps to future-proof forensic systems and ensures that justice can be served, no matter what advances in technology may bring. .

Chatbot-Linked Crimes

Chatbot-linked crimes on social media can take several forms. These include phishing through conversational scripts, impersonation of legitimate individuals or customer service accounts, grooming and coercive manipulation, scam automation, misinformation propagation, and fraudulent user engagement. Recent work on social media forensics notes that social platforms are now a major source of evidence in crimes such as cyberbullying, defamation, fake news, and hostile manipulation. Also, AI-assisted harassment can be analyzed as a **linked-crime model** because it treats abusive conduct as a sequence of connected offenses rather than a single isolated act. In this framework, the same digital actor or small group may use automated scripts, chatbot prompts, fake profiles, synthetic images, and reposting networks to commit cyberbullying, doxxing, stalking, intimidation, and defamation across multiple platforms. The legal significance lies in the fact that each act is not merely repetitive; it may perform a different functional role in the wider criminal scheme, such as identifying the victim, amplifying abuse, concealing identity, or increasing psychological harm. This approach is consistent with case-based discussions of AI-assisted harassment, which describe bots, AI-generated content, and cross-platform messaging as mechanisms for scaling abusive behaviour. The table 1 shows various types of chatbot-linked crimes.

Chatbot-linked crime type	How the chatbot is used	Typical harm or legal issue
Phishing and social engineering	Drafts convincing scam emails, messages, or impersonation scripts	Identity theft, fraud, unauthorized access
Cybercrime support	Generates malicious code or helps automate attack steps	Malware creation, intrusion, extortion
Fraud and scams	Produces persuasive text for fake offers, fake support chats, or investment scams	Financial loss, deceptive practices
Disinformation and propaganda	Creates large volumes of false or manipulative content	Public deception, political manipulation, incitement
Violence facilitation	Assists users with planning harmful acts or testing violent scenarios	Threats to life, criminal conspiracy, incitement
Self-harm contribution	Reinforces harmful thinking or fails to interrupt dangerous exchanges	Wrongful death claims, negligence allegations, safeguarding failures
Data misuse and privacy violations	Reveals or helps recover sensitive personal or business data from conversations	Privacy breach, unlawful disclosure, evidence issues
Extortion and blackmail	Helps draft ransom notes or pressure messages	Extortion, coercion, cyber-enabled blackmail

Table 1- Adapted from Europol and U.S. law-enforcement warnings on generative AI misuse, recent reporting on AI-assisted cybercrime and chatbot-related harm, and Indian reports on AI-enabled scams, voice cloning, deepfakes, and chatbot-facilitated data leakage.

Chatbots are making it harder to determine who's behind a message because they can have conversations that seem like they're with a real person, hide the identity of the person controlling them, and send lots of messages from different accounts all at once. This makes it tough to articulate if a person is sending harmful messages or if it's a computer program doing it automatically. To solve this problem, investigators need to look at more than just the message itself - they need to examine the way the words are used, the hidden information about the message, the history of the account sending it, the records from the platform it was sent on, and other clues from outside the platform. When it comes to using chatbot-generated content as evidence in a courtroom, there's a big issue to consider. Investigators have to be able to show exactly how they collected, preserved, and validated the content, and prove that it's connected to a specific suspect, device, or operator.

The problem isn't just about whether the content is harmful or not - it's about making sure that the evidence hasn't been tampered with and that the investigator can clearly explain how the chatbot conversation took place. This is known as the chain of custody, and it's crucial in building a strong case. If the chain of custody is broken, the evidence may not be admissible in court, which could have serious consequences for the investigation. So, it's not just about the content itself, but about being able to track its entire trail and verify its authenticity.

Forensic Challenges

The main forensic problems in chatbot-linked social media crime are volatility, scale, attribution, and evidentiary integrity. Social media evidence can be deleted quickly or altered by account owners, while platform policies and privacy restrictions may limit direct access to logs. The key investigation on social media forensics emphasizes

that collecting, storing, and validating evidence remains difficult because these environments are heterogeneous and dynamic.

Attribution is also difficult because chatbots blur the boundary between human and machine action. A malicious campaign may involve prompt engineering, automation tools, account farms, or a single operator controlling many profiles. This requires investigators to combine natural language analysis with infrastructure-based evidence, such as IP logs, authentication records, message timestamps, browser artifacts, and device traces. Recent digital evidence reviews also stress the need for forensic maturity, collaboration with practitioners, and attention to how evidence will be interpreted in court.

Another issue is evidential admissibility. Courts require that digital evidence be shown to be authentic, reliable, and collected according to defensible procedures. If data are stored in conventional systems without strong tamper resistance, or if preservation relies on weak cryptographic methods, defense counsel may challenge the evidence's integrity. This is one reason why blockchain-enabled preservation and secure logging have become important in social media forensics research.

Applying Boyd's Cycle

Boyd's cycle can be applied to chatbot investigations as a structured framework for identifying, analyzing, and responding to suspicious conversational behavior on social media. The OODA loop—Observe, Orient, Decide, Act—was developed as a decision-making model and is widely used in security and law enforcement contexts because it emphasizes speed, adaptability, and continuous feedback. In chatbot investigations, the cycle helps analysts move from raw platform data to actionable forensic conclusions.

1. Observe

The first stage is **Observe**, which involves collecting all relevant social media evidence. Investigators should capture chatbot messages, timestamps, account metadata, username changes, profile images, response frequency, and interaction patterns across platforms. This stage also includes identifying suspicious indicators such as repetitive phrases, unnatural response delays, identical message templates, or links to phishing pages. In digital investigations, the quality of observation matters more than the quantity of data, because investigators need accessible and reliable information to support later analysis.

2. Orient

The second stage is **Orient**, where investigators interpret the evidence in context. This means comparing chatbot activity with known fraud tactics, scam scripts, grooming patterns, or automated propaganda behaviors. Orientation requires linking the observed messages to platform behavior, user history, and the broader criminal environment. Boyd's model stresses that orientation is not just classification; it is the synthesis of information into a meaningful mental model. In chatbot cases, analysts may use linguistic analysis, network mapping, and account correlation to determine whether the account is likely human-operated, automated, or part of a coordinated bot network.

3. Decide

The third stage is **Decide**, where investigators determine the most appropriate investigative response. This may include preserving evidence, requesting platform records, escalating the case to cybercrime units, or conducting deeper forensic analysis of linked devices and accounts. Decision-making in this stage should be guided by the seriousness of the suspected offense, the confidence level of the evidence, and legal authority. The OODA model is valuable here because it encourages rapid but informed action rather than slow, disconnected procedures.

4. Act

The final stage is **Act**, where investigators implement the chosen response. Actions may involve securing the evidence chain, issuing preservation requests, archiving content, or creating a forensic report for prosecution. In chatbot investigations, the action stage should also include feedback, because the results of the intervention may reveal new evidence or new suspect accounts. Boyd's cycle is iterative, so investigators should return to observation after each action and refine their understanding as new information emerges.

A forensic study on conversational AI notes that users may abuse such tools for phishing schemes, dissemination of sensitive information, and other harmful activities, and proposes a forensic framework for investigating chatbot-related incidents. The study treats chatbot logs, prompts, and system outputs as potential evidence sources in criminal inquiries.

This matters because linked crime analysis depends on evidentiary linkage: investigators need to connect a chat interaction, a social-media action, and an offline consequence through a coherent digital trail. The forensic implication is that chatbot data should be preserved and analyzed alongside device artifacts, timestamps, and platform metadata.

Investigative Value

The main value of Boyd's cycle in chatbot investigations is that it turns a fragmented process into a continuous investigative loop. Since social media crimes can change really fast, with chatbots switching tactics, accounts, or platforms in just a few minutes, using the OODA loop helps investigators stay on top of things and keep track of what's happening while making sure digital evidence is handled correctly. When you combine this framework with things like forensic logging, analyzing the meaning of language, and understanding the platform, it becomes really useful. Boyd's cycle gives investigators a practical way to approach chatbot investigations on social media, helping them collect evidence in a systematic way, understand what the chatbot is doing in context, figure out the right actions to take, and respond in a way that keeps the investigation intact and moving quickly. In today's cyber investigations, the OODA loop is really valuable because it helps investigators make decisions that match the fast-

paced and sneaky nature of chatbot-enabled crimes. By using this loop, investigators can keep up with the changing tactics of chatbot crimes and make sure they're always one step ahead. This is especially important when dealing with crimes that involve social media, where things can change in an instant. The OODA loop is also helpful because it allows investigators to be more adaptive and responsive to new information, which is crucial in investigations where the situation can change quickly. By using this framework, investigators can make sure they're always looking at the big picture and considering all the factors involved in the crime, which helps them make better decisions and ultimately catch the people behind the chatbot crimes. Overall, Boyd's cycle and the OODA loop are essential tools for investigators dealing with chatbot crimes on social media, and they can help make the investigation process more efficient and effective.

Proposed Framework

A quantum-secure forensic framework for chatbot-linked social media crimes should include five integrated layers: evidence acquisition, post-quantum preservation, AI-assisted analysis, attribution modeling, and courtroom presentation.

A. First, evidence acquisition should capture posts, messages, replies, profile metadata, timestamps, and account connections as soon as a suspected event is identified. Because social media data are volatile, acquisition should occur with minimal delay and be accompanied by hash generation and secure logging.

B. Second, preservation should use post-quantum cryptographic methods or hybrid cryptographic methods that remain secure against quantum adversaries. This includes quantum-resistant digital signatures, encrypted evidence containers, and immutable audit trails. Research in quantum forensics explicitly recommends moving toward quantum-resistant algorithms and updated forensic methodologies.

C. Third, AI-assisted analysis should support detection of chatbot behavior, recurring linguistic templates, semantic similarity across accounts, and suspicious automation patterns. Social media forensics literature already shows the value of AI, NLP, and federated learning in identifying harmful or suspicious content at scale. Such methods are useful for tracing coordinated bot activity, false narratives, and repeated scam prompts.

D. Fourth, attribution modeling should connect chatbot output to a responsible actor or organization. This involves correlating conversation patterns with login activity, device artifacts, network data, and account recovery information. The goal is to distinguish whether the evidence points to a human operator, an automated system, or a hybrid arrangement.

E. Fifth, courtroom presentation should translate technical findings into a clear evidentiary narrative. Digital forensic literature emphasizes that evidence must be understandable to courts, not just technically accurate. For chatbot-linked crimes, this means explaining the forensic significance of automation, the preservation controls used, and the reasoning that links the chatbot communication to the accused.

Evidence Flow

Stage	Forensic purpose	Quantum-security relevance
Acquisition	Capture posts, messages, and metadata	Protect the transfer channel and initial hashes
Preservation	Store evidence with chain of custody	Use post-quantum signatures and immutable logs
Analysis	Detect chatbot patterns and crime indicators	Prevent future decryption or tampering risks
Attribution	Link activity to accounts, devices, or operators	Maintain trustworthy evidence provenance
Presentation	Present admissible evidence in court	Show reliability under quantum-safe controls

Table 2- Stages of Quantum-Related Digital Forensics and Their Relevance to Cybersecurity. Adapted from recent literature on quantum computing, digital forensics, and quantum key distribution.

Methodological Considerations

A strong academic study in this area should use a mixed-method design. Qualitatively, the study should review forensic standards, social media case studies, and post-quantum security literature. Quantitatively, it should test chatbot detection features using labeled social media datasets, while evaluating evidence preservation methods under simulated attack conditions. Recent research on ambient social media forensics demonstrates that blockchain and federated learning can support chain-of-custody management and distributed investigation.

The methodology should also include scenario analysis for several crime types: scam chatbots, grooming chatbots, harassment bots, and propaganda bots. Each scenario should be examined for evidentiary traces, such as linguistic repetition, account creation patterns, cross-platform reuse, and metadata anomalies. This approach is consistent with recent calls for interdisciplinary collaboration in digital evidence research and social media investigation.

Legal and Ethical Issues

Quantum-secure forensic systems raise legal and ethical questions. Investigators must balance preservation with privacy, especially when collecting data from social platforms that contain unrelated personal communications. Social media forensics research repeatedly notes the cross-border, privacy-sensitive nature of these investigations. The use of automated analysis tools in investigating chatbot-linked crimes raises important ethical concerns.

One key issue is that investigators need to be aware of the limitations of these AI tools and not exaggerate their accuracy. Experts who review digital evidence point out that AI-supported forensic work can be biased and difficult to interpret. To address these concerns, it's crucial to have human oversight of the analysis process, as well as thorough documentation and validation of the results. Additionally, investigators should provide

transparent reporting of their methods and findings to ensure the integrity of the investigation. A defensible approach therefore requires human oversight, documented validation, and transparent reporting.

Discussion

The convergence of chatbot crime and quantum security changes digital forensics in two ways. First, chatbot-linked crimes expand the range of evidence investigators must collect, especially conversational text, platform metadata, and automation indicators. Second, quantum computing changes the security assumptions behind that evidence, making long-term preservation a cryptographic problem as much as a forensic one.

Recent research supports the move toward secure, automated, and distributed forensic architectures. Social media forensics frameworks are increasingly using blockchain, federated learning, and ambient intelligence to preserve evidence and support investigation. Quantum forensics research, meanwhile, argues that digital forensic science must adapt to post-quantum security requirements. Together, these trends suggest that future forensic systems should be designed from the outset to be both analytically capable and quantum-resistant.

Conclusion

The rapid evolution of artificial intelligence and conversational chatbots has fundamentally transformed the digital threat landscape, creating new challenges for forensic investigators and the criminal justice system. Chatbot-linked crimes on social media, including financial fraud, identity theft, cyberstalking, online grooming, harassment, misinformation campaigns, deepfake-assisted deception, and coordinated disinformation are becoming increasingly sophisticated, automated, and difficult to detect. At the same time, the emergence of quantum computing presents a dual challenge, while it offers unprecedented computational capabilities that can enhance forensic analytics, it also threatens the security of conventional cryptographic systems that currently protect digital evidence and investigative records.

In this context, quantum security is becoming an essential component of forensic investigations involving chatbot-enabled cybercrime. Digital evidence collected from social media platforms is often highly volatile, distributed across multiple jurisdictions, and protected by encryption mechanisms that may become vulnerable to future quantum attacks. Consequently, investigators require forensic methodologies capable of ensuring the confidentiality, integrity, authenticity, and long-term admissibility of digital evidence throughout its lifecycle. The adoption of quantum-resistant cryptographic algorithms, secure evidence acquisition techniques, tamper-evident blockchain-based chain-of-custody systems, AI-assisted forensic analytics, and quantum-safe evidence repositories provides a comprehensive framework for addressing these emerging challenges.

A post-quantum forensic framework integrating secure evidence acquisition, blockchain-backed evidence preservation, artificial intelligence–supported analysis, and post-quantum cryptographic protection offers a promising direction for both research and practical implementation. Such a framework can strengthen evidentiary reliability by preventing unauthorized modification, ensuring traceability of investigative actions, facilitating automated detection of chatbot-generated content, and preserving digital evidence against future cryptanalytic attacks. Furthermore, combining machine learning with forensic intelligence can significantly improve the identification of coordinated bot networks, synthetic identities, manipulated multimedia, and malicious conversational patterns across multiple social media platforms.

Despite these technological advances, several challenges remain. Existing forensic standards and legal frameworks have yet to fully address the evidentiary implications of quantum-secure systems, blockchain-based evidence management, and AI-assisted investigative decision-making. Significant research is still required to develop standardized post-quantum forensic protocols, interoperable forensic tools, explainable AI models for evidence analysis, and internationally harmonized legal guidelines governing the admissibility of quantum-secured digital evidence. Collaboration among computer scientists, forensic experts, cybersecurity professionals, legal scholars, policymakers, and international law enforcement agencies will therefore be essential to establish robust governance mechanisms for future investigations.

Looking ahead, forensic science must evolve from reactive evidence collection toward intelligent, quantum-resilient investigative ecosystems capable of addressing increasingly sophisticated AI-driven cyber threats. We need to invest in new types of cryptography that can withstand quantum computers, build secure infrastructures for forensic work, develop advanced analytics using AI, create technologies for secure quantum communication, and train digital investigators in these new areas. As quantum technologies become more advanced, making sure our digital forensic practices are secure against quantum threats is not just a good idea, it's necessary to keep criminal investigations fair, protect the legal process, and make sure digital evidence is reliable and can be used in court in the future when quantum computers are common. Security in post-quantum cryptography, secure forensic infrastructures, advanced AI analytics, quantum communication technologies, and specialized training for digital investigators will be critical to maintaining trust in digital evidence. As quantum technologies mature, the integration of quantum security into digital forensic practice should be viewed not merely as a technological enhancement but as a strategic necessity for safeguarding the integrity of criminal investigations, protecting judicial processes, and ensuring that digital evidence remains reliable and legally defensible in the post-quantum era.

References

1. Alhazmi, S., Elleithy, K., & Elleithy, A. (2025). Digital forensics of quantum computing: The role of quantum entanglement in digital forensics—Current status and future directions. Quantum Reports, 7(4), 44. https://doi.org/10.3390/quantum7040044
2. Joseph, A., George, S., & Shatte, A. (2026). Quantum-driven digital forensics: Evidence acquisition, intrusion detection, cybercrime simulation, and DNA profiling. In J. C. Bansal, P. Jamwal, & S. Hussain (Eds.), Sustainable Computing and Intelligent Systems: Proceedings of SCIS 2025 (pp. 102–115). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-22917-5_9
3. Nguyen, C., & Costa, A. (2025). Digital forensics challenges in quantum computing era. ITSI Transactions on Electrical and Electronics Engineering, 11(1), 1–5. https://doi.org/10.65521/itsi-teee.v11i1.153
4. Memon, M., Naeem, M. A., & Memon, F. (2025). The integration of quantum computing and digital forensics: Opportunities and challenges. Spectrum of Engineering Sciences, 3(5), 773–785. https://doi.org/10.5281/zenodo.15532801
5. Alfassi, I., Gelles, R., Liss, R., & Mor, T. (2026). Cybersecurity of quantum key distribution implementations (Version 3) [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2508.04727
6. Soviany, S., & Gheorghe, C.-G. (2023). The QKD (Quantum Key Distribution) application in cyber security. Romanian Cyber Security Journal (ROCYS), 5(2), 87–101. https://doi.org/10.54851/v5i2y202309
7. Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. Nature, 299(5886), 802–803. https://doi.org/10.1038/299802a0
8. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (pp. 175–179). IEEE.
9. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661–663. https://doi.org/10.1103/PhysRevLett.67.661
10. Pirandola, S., et al. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012–1236. https://doi.org/10.1364/AOP.372001
11. Diamanti, E., Lo, H.-K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. npj Quantum Information, 2, 16025. https://doi.org/10.1038/npjqi.2016.25
12. Zhandry, M. (2019). How to record quantum queries, and applications to quantum indistinguishability. Journal of Cryptology, 32, 1410–1437. https://doi.org/10.1007/s00145-018-9309-2
13. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723
14. Unruh, D. (2017). Post-quantum security of Fiat-Shamir. In Advances in Cryptology – EUROCRYPT 2017 (pp. 65–95). Springer. https://doi.org/10.1007/978-3-319-56617-7_3
15. Bansal, J. C., Jamwal, P., & Hussain, S. (Eds.). (2026). Sustainable computing and intelligent systems: Proceedings of SCIS 2025. Springer Nature Switzerland.
16. Khan, A. A., Zhang, X., Hajjej, F., Yang, J., Ku, C. S., & Por, L. Y. (2023). ASMF: Ambient social media forensics chain of custody with an intelligent digital investigation process using federated learning. Heliyon, 10(1), e23254. https://pmc.ncbi.nlm.nih.gov/articles/PMC10755315/
17. Narasimhan, P., & Kala, N. (2024). Quantum Forensics, AI, and D4N6: The convergence of quantum computing, artificial intelligence, and digital forensics in post-quantum security. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(1), 306–320. https://ijsrcseit.com/CSEIT2425480
18. Reedy, P. (2023). Interpol review of digital evidence for 2019–2022. Forensic Science International: Synergy, 6, 100313. https://pmc.ncbi.nlm.nih.gov/articles/PMC10311174/