Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 5, 2025

THE INTEGRATION OF QUANTUM COMPUTING AND DIGITAL FORENSICS: OPPORTUNITIES AND CHALLENGES

Muzmmil Memon[*1], Muhammad Ahsan Naeem[2], Farheen Memon[3]

[*1]*Department of Computer Science Management, Avila University, USA*
[2]*Department of Computer Science, Iqra University, Karachi, Pakistan.*
[3]*Institute of Mathematics & Computer Science, University of Sindh, Pakistan*

[*1]memon521057@avila.edu, [2]muhammmad.ahsan@iqra.edu.pk, [3]farheenmemon28@gmail.com

DOI: https://doi.org/10.5281/zenodo.15532801

Keywords
Thematic Analysis, Systematic Review, Quantum Computing, Digital Forensics, Post-Quantum Cryptography, Forensic LLM, DFaaS, AI in Forensics, Quantum Threats.

Article History
Received on 20 April 2025
Accepted on 20 May 2025
Published on 28 May 2025

Corresponding Author: *
Muhammad Ahsan Naeem

Abstract

Purpose: *It analyzes the impact of new findings in quantum computing on forensic techniques, as it is urgent to check the reliability of current tools in light of potential quantum threats. Driven by the discovery that quantum attack algorithms may expose the current forensic system to attack, the research examines how quantum algorithms and modern AI are transforming forensics. It draws on current cryptographic and forensic foundations, shows they cannot handle a post-quantum world and outlines a new structure that adds quantum-safe methods and effective forensics. This research used 14 validated models and followed a thematic approach built on Theory, including Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), ForensicLLM and Digital Forensics as a Service (DFaaS). Using literature and conceptual mapping, we investigated how these theories influence forensic readiness, the way tasks are managed and tool automated processing. The research has found that present forensic systems do not meet the demands of possible quantum decryption and that using AI-assisted, transformer-based tools in forensics can greatly improve activity and analysis accuracy. In addition, the research finds that organizational readiness plays a major role as a moderating factor. The findings from this research will guide plans for modernization and may be examined using future studies in different countries and institutions.*

INTRODUCTION

Growing advancements in quantum computing are changing the fields of cybersecurity and digital forensics and bringing both great chances and serious risks. Exploiting features such as superposition and entanglement, quantum systems are ready to exceed classical PCs and perform difficult tasks including factorization and key search very fast (Shor, 1994; Grover, 1996). While they provide great chances for effective problem solving, they also put at risk the standard cryptographic tools that support forensic evidence. The Cyber Forensics & Threat Investigations Research Community (2025) pointed out that using "harvest now, decrypt later" shows that we need to focus on post-quantum security right away. Because quantum systems can crack RSA, ECC and hash-based systems, the utility and dependability of digital evidence are damaged primarily in situations involving finance and justice (Sodiya et al., 2024; Ekert, 1991). Consequently, digital forensics ought to notice these risks and add post-quantum cryptography (PQC) to keep evidence reliable.

Because so much of our critical infrastructure is now digital, cybersecurity and digital forensics have become more important than before. Organizations in finance, healthcare, defense and law enforcement now depend on correct and secret digital data to support compliance, solve disputes and trust their work. According to Elmisery et al. (2025), the financial sector is exposed to two new threats: attacks using AI-powered malware and the coming shift to quantum computing. It's not just a theory, as millions of dollars and pieces of data have already been lost to such digital crimes. The link between AI and quantum threats is making cyber threats more dangerous and urging industries to reexamine their online protection (Wickramasekara et al., 2025; Sodiya et al., 2024). PQC and QKD investments have emerged to ensure that data is defended even before quantum computing really starts impacting industry (Alghamdi, 2025; Sharma et al., 2025).

Digital forensics is now mainly challenged by how quantum computing is likely to break cryptographic methods that have always kept data safe and accepted in courts. Traditional systems for cryptography such as RSA, ECC and those using symmetrical keys, may become useless because of Shor's and Grover's innovations (1994, 1996). Elmisery et al. point out that quantum security threats are very likely and have already influenced attack plans that might subsequently expose years of data and digital conversation. Forensic experts find it hard to address this gap because quantum-resistant systems are not fully developed and still leave a period when protection is lacking (Alghamdi, 2025; Sodiya et al., 2024). Not only is digital evidence becoming encrypted and altered with AI, but the time available to adjust tools and standards for investigation and justice is getting smaller. Even though systems such as PQC and QKD promise better security, they are not consistently put in place everywhere, leaving defenses divided (Ekert, 1991; Wickramasekara et al., 2025).

Review of Literature

To cybersecurity professionals, at the moment, quantum computing is majorly reshaping digital security by attacking classic methods with Shor's and Grover's algorithms. Shor's method can disassemble RSA and ECC encryption within simple timeframes, directly affecting confidentiality when dealing with digital forensic cases (Shor, 1994; Elmisery et al., 2025). Just like Diffie-Hellman, Grover's algorithm increases the speed of key searches, changing the AES symmetric encryption (Grover, 1996; Alghamdi, 2025). The development of quantum forensic methods is required because of threats to information security which exploit quantum laws and properties to hide or manipulate digital evidence (Ekert, 1991). Key exchanges in quantum cryptography through BB84 and E91 protocols work thanks to quantum entanglement and polarization which are regarded as unbreakable (Bennett & Brassard, 1984; Ekert, 1991). Experts in recent times stress that, although these protocols provide great encryption, they need high preparedness from organizations to be achieved effectively (Sodiya et al., 2024; Sharma et al., 2025).

To address these challenges, Post-Quantum Cryptography (PQC) helps digital forensics keep confidentiality and the dependability of digital information under quantum-computing threats. The NIST has added CRYSTALS-Kyber to its standard algorithms since it protects from quantum attacks but is efficient on ordinary systems (Alghamdi, 2025). At the same time, forensic teams need to adapt their tools to keep up with quantum-resistant cryptography and deal with tougher kinds of cyber evidence. With the Hansken system, called DFaaS, investigators benefit from using cloud services and AI technology to simplify access and analysis of evidence (Wickramasekara et al., 2025; Scanlon et al., 2023). Compared to general LLMs, ForensicLLM greatly improves in identifying evidence, figuring out where it came from and focusing on digital forensics (Sharma et al., 2025; Michelet & Breitinger, 2023). Thanks to Low-Rank Adaptation (LoRA) and quantization, these tools are now simpler to use and still ensure accurate results (Hu et al., 2021; Jacob et al., 2018).

This framework considers digital forensic investigations to be the primary dependent variable and their efficiency is now heavily shaped by the use of transformer-based neural network models and retrieval-augmented generation (RAG). Both LLaMA and GPT types of Transformers let forensic teams analyze disorganized data for context and RAG models use external sources to ensure correct results are given (Lewis et al., 2020). These advancements directly improve the accuracy and court use of forensic

findings (Baggili et al., 2025; Sevilla et al., 2022). The success of these changes relies on preparedness within organizations which enables them to use quantum-safe methods and AI for tracing cyber incidents (Elmisery et al., 2025; Sreya et al., 2023). When infrastructure, regulatory rules and training for experts are lacking, even the best technologies cannot make a difference in investigations. As a result, mixing threats from quantum, cryptographic challenges, AI developments and organizations' skills creates a new field for the effectiveness of digital forensics.

Research Theme Approach

The current study uses theme analysis to discuss the similarities between developments in quantum computing and work in digital forensics. 14 important theories and models (see Table 2) are the foundation of this framework covering quantum algorithms, cryptographic protocols, forensic process models and artificial intelligence architectures. The purpose is to dive into how different technologies can improve digital forensic processes as organizations are presented with changing security risks and new integration requires. The method follows earlier methods for synthesizing literature (Cerchione & Esposito, 2016) and rates technical areas and digital forensics by evaluating their crucial concepts and how they function in practice.

Keywords	Data Range	Databases
Quantum Computing, Shor's Algorithm, Grover's Algorithm, Quantum Key Distribution, Post-Quantum Cryptography, Digital Forensics, Digital Forensic Process Model, ForensicLLM, DFaaS, Transformer Architecture	2018 to 2025	Science Direct, Springer, IEEE Xplore, ACM Digital Library, Taylor and Francis

Table 1 Material Search

This thematic review is structured into four core themes derived from the constructs in the theoretical framework:

1. **Quantum Disruption and Cryptographic Response** It means looking at proposals such as Shor's Algorithm, Grover's Algorithm, BB84 Protocol, E91 Protocol and Post-Quantum Cryptography which build secure options for when classical encryption cannot be trusted anymore.

2. **Forensic Model Adaptation to Quantum Realities** Using this theme, we apply the No-Cloning Theorem and review how digital forensics tools and techniques must be improved for quantum cyber security.

3. **AI-Enhanced Forensic Toolchains Incorporating ForensicLLM**, This theme investigates the impact of AI on digital forensics and on generating forensic reports, using ForensicLLM, Transformer Architecture, Tokenization & Attention Mechanism, Low-Rank Adaptation (LoRA) and Retrieval-Augmented Generation (RAG).

4. **Organizational Preparedness and Cross-System Compatibility** Effective Use and Integration with Other Systems While unrelated to theory, this area is centered on how well systems are able to use quantum cryptography and AI which can boost or lower the success of new forensic techniques.

Research directions were set by selecting papers and frameworks from indexed scientific repositories describing how these models were deployed in forensics or cybersecurity. Models were put in order by how relevant and mature their concepts are. The report points out how quantum computing brings new dangers and digital forensic upgrades create additional opportunities, providing a detailed overview of how to integrate modern approaches and tackle associated challenges.

Material Search

Theory/Model	Description
Shor's Algorithm (1994)	Quantum algorithm for factoring integers; threatens RSA, ECC.
Grover's Algorithm (1996)	Quantum search algorithm impacting symmetric cryptography.
Quantum Key Distribution (QKD)	Secure communication using quantum mechanics (e.g., BB84, E91).
Post-Quantum Cryptography (PQC)	Cryptography resistant to quantum attacks (e.g., CRYSTALS-Kyber).
BB84 Protocol	First quantum key distribution protocol using photon polarization.
E91 Protocol (Ekert, 1991)	Entanglement-based QKD using Bell's inequality.
No-Cloning Theorem	Quantum principle stating unknown quantum states cannot be copied.
Digital Forensic Process Model (Casey, 2011)	Outlines digital forensic stages: identification, analysis, reporting.
Digital Forensics as a Service (DFaaS)	Cloud-based forensic model for scalable evidence handling.
Transformer Architecture	Neural network model foundational to GPT, BERT, LLaMA.
ForensicLLM	Domain-specific LLM fine-tuned for digital forensics tasks.
Retrieval-Augmented Generation (RAG)	Technique for enhancing LLMs by retrieving external data.
Low-Rank Adaptation (LoRA)	Efficient fine-tuning method for LLMs using fewer parameters.
Tokenization & Attention Mechanism	Core mechanisms in transformer models for NLP.

Table 2 Theoretical Approach

First Criteria: Focus of the abstract	Second Criteria: Focus of the paper	Third Criteria: Types of Study	Fourth Criteria
We have focused on the abstracts that have discussed the association between quantum computing and digital forensic models including cryptography, evidence integrity, and tool adaptation.	Papers that have focused on the integration of quantum computing, AI, and digital forensic methodologies in context to cybersecurity and evidence analysis.	We have only considered quantitative and theoretical technology-based papers; qualitative-only and mixed-method studies were excluded.	Indexed in Scopus, IEEE Xplore, Springer, and Science Direct databases (Alghamdi, 2025; Sharma et al., 2025).

*500 studies that matched the thematic and technical keywords.

Findings Discussion

Theoretical Setting

This work relies heavily on main quantum computing theories that demonstrate possible breaks in classical cryptographic security. The quantum version of Shor's algorithm continues to be the most often discussed threat to RSA and ECC systems (Shor, 1994; Elmisery et al., 2025). While Grover's algorithm doesn't pose a big risk, it still cuts down the complexity of brute force searches for symmetric cryptographic keys, putting algorithms like AES at risk (Grover, 1996; Alghamdi, 2025). They make it clear why we need to embrace quantum-proof cryptography as soon as possible. These protocols allow for secure entanglement- and polarization-based communication, as they are theoretical immune to interception without notice (Bennett & Brassard, 1984; Ekert, 1991). However, applying these powerful techniques in forensics is still limited because of problems with hardware and compatibility issues (Sodiya et al., 2024; Sharma et al., 2025).

The research also explores concepts for updating digital forensics with new cryptographic and workflow methods to match the expected developments in post-quantum technologies. The inclusion of CRYSTALS-Kyber which is supported by NIST, makes Post-Quantum Cryptography (PQC) a key factor in protecting against quantum-guided attacks on classical computing equipment (Alghamdi, 2025). In addition, the No-Cloning Theorem helps to avoid making copies of quantum evidence which would preserve its admissibility by the courts (as explained by Ekert in 1991). Although the Digital Forensic Process Model is still needed for handling evidence, new attention is being given to making systems ready to use quantum-secured evidence (Wickramasekara et al., 2025; Michelet & Breitinger, 2023). New cloud services such as Digital Forensics as a Service (DFaaS) support the idea of envelope evidence processing and

condition checking of data in various digital environments (Scanlon et al., 2023; Baggili et al., 2025).

The last part of the theory is developed at the intersection of artificial intelligence and forensics, thanks in large part to transformer-based language models. Because of the Transformer Architecture, tools such as GPT and LLaMA can handle the tasks of evidence classification, reporting and anomaly detection while performing digital investigations (Sevilla et al., 2022; Sharma et al., 2025). They can be improved further by using RAG to base AI-made messages on real facts and LoRA to allow investigators to adjust LLMs with fewer tools (Hu et al., 2021; Lewis et al., 2020) Tokenization and Attention Mechanisms allow forensic models to target and organize the underlying patterns in a huge amount of data that matter in both managing a digital overload and establishing the relevance of evidence (Michelet & Breitinger, 2023; Jacob et al., 2018). This approach shows that fusing quantum models with AI into forensics is not only doable but truly necessary for a strong digital forensic practice in the future.

Quantum Theories

Shor's Algorithm

Out of all quantum breakthroughs, Shor's Algorithm (invented in 1994) has brought the biggest threat to the security of classical cryptography. This means that a well-designed quantum computer could factor big integers much sooner than any previous classical method which leaves RSA and ECC vulnerable in digital forensic data protection (Shor, 1994). Elmisery, Sertovic, Zayin and Watson (2025) point out that, if channels are weakened by later breaking encryption methods, the collection of digital evidence may be at risk. As quantum hardware continues to improve, Alghamdi points out that algorithms will gain importance and bring greater concerns about keeping forensic information safe and secure. According to Baggili, Sharma, Ghawaly, McCleary and Webb (2025), there is a risk that encrypted logs or emails in forensic settings can still be exploited for past leakage of data. According to Ekert (1991) and Bennett and Brassard (1984), quantum-safe methods are necessary and form the bedrock for this issue. All of these studies stress the importance of having post-quantum migration strategies within forensic methods.

Grover's Algorithm

Grover's Algorithm (1996) provides a different but important risk. It cuts the complexity of brute-force attacks against symmetric cryptography by half which means a key like AES-128 takes twice as much time to break (Grover, 1996). Even so, it demands a rise in key lengths and exposes the system to key recovery in urgent forensic work. According to Alghamdi (2025), data archived by AES keys may fall too quickly to quantum-powered hackers, despite being encrypted. They warn that tools that use symmetric encryption for data protection in forensics can be at risk from quantum computers if they use keys that have not been updated. Sevilla, Becerra and Alvarez (2022) add that utilities of local AI inference may require users to create more security tokens to reduce the risk of model attacks or private data leakage. Practically, the model led forensic departments to use multi-layer encryption and stronger, higher-bit security.

Quantum Key Distribution

Developed by using quantum principles, Quantum Key Distribution actively defends against quantum threats, unlike other defenses that depend on complex math. Until recently, BB84 used photon polarization, while E91 used entanglement, to ensure that eavesdropping would disturb the communication and be easy to discover. Alghamdi (2025) explains that using QKD in digital forensic evidence sharing may help reduce the danger of evidence interception in cloud investigation cases. Elmisery et al. (2025) mention that secure public or insecure networks between forensic tools could be achieved with QKD. Sharma et al. (2025) suggest that equipping ForensicLLM with QKD will make output secure and reliable. Ekert's (1991) early studies form the scientific basis for how QKD is important for forensic science, although cheap and accessible versions have not yet been widely implemented.

Future Quantum Theoretical Directions

Still, this study has several limitations despite giving valuable knowledge about using quantum computing in digital forensics. If we rely solely on technology, like Shor's Algorithm, Grover's Algorithm and QKD, the approach ignores the social and legal side of how we manage evidence, especially in regard to laws across borders and if quantum data is allowed in court

(Elmisery et al., 2025; Alghamdi, 2025). While the study fully explores technical aspects, expanding the perspective to add legal and procedural models in addition to cryptographic and AI methods will further benefit future research. In addition, the current study concentrates on BB84 and CRYSTALS-Kyber post-quantum cryptography, but has not considered how practical their implementation might be, nor how well they will be accepted by users in forensic labs (Bennett & Brassard, 1984; Sharma et al., 2025).

The method used to conduct this research relies only on a conceptual and thematic review, making empirical and comparative work absent. Since the technology in forensic organizations can be quite different between developed and developing countries, it is difficult to make general statements about findings. For example, while Hansken, a DFaaS system, is being used in countries like the Netherlands, South Asia and Africa rarely see any of these frameworks used (Wickramasekara et al., 2025; Scanlon et al., 2023). Further research could apply statistical methods such as SEM, to see how organizational readiness or using new forensic tools affects how well investigators can combat quantum threats. Furthermore, using transformer-based tools like ForensicLLM locally with the help of LoRA could be applied in multilingual forensic work to assess whether their results remain relevant in context (Sharma et al., 2025; Sevilla et al., 2022).

Management experts see the findings as a sign that more resources and proactive constructiveness are needed. Operational policies should now include post-quantum cryptography for both forensic labs and cybersecurity. The steps are as follows: increasing important key sizes, making sure to end the use of RSA/ECC-centered methods and matching software related to forensics with programs following standards like PQC and QKD (Alghamdi, 2025; Baggili et al., 2025). It is important that investigators receive quantum threat insight and learn to work with different AI tools in training so they are familiar with using models like RAG and Transformer. Planning by managers should also include affordable approaches to adopting secured communication using quantum technologies, mainly for groups on a limited budget. There needs to be a shift in emphasis from fixing emergencies to being fully prepared for important changes.

Together, those involved in research and management must help set up global guidelines for making quantum forensics ethical and reliable. This level of deepfakes challenges us to create protocols that both secure data and verify that evidence comes from a reliable source (Ekert, 1991; Michelet & Breitinger, 2023). Institutions could work with companies that supply quantum hardware and artificial intelligence labs to design new technology for forensics. As quantum gadgets continue to develop, there is a need to observe and chart the ramifications for investigative processes over the next few years. Combining technical techniques with elements of human design is recommended for the future, so that readiness for quantum digital forensics is possible and scientifically supported.

Forensic Models and Theories

Digital Forensic Process Model

The procedure for digital investigations called the Digital Forensic Process Model (originally outlined by Casey in 2011) remains central to carrying out investigations in the four important phases. Using this model has helped apply the same forensic steps in various countries and make those steps acceptable in courts. At the same time, issues have arisen when dealing with quantum data that is both encrypted and spread out. According to Wickramasekara, Breitinger and Scanlon (2025), traditional forensic approaches need to keep up with the high level of instability and difficulty presented by quantum-impacted evidence. Because digital threats are diverse and encryption is growing further with post-quantum cryptography, today's forensics demand real-time analysis and cross-border cooperation, neither of which is fully included in conventional models. They highlight how AI can be added to usual process flow management so that AI-based triaging and checking custody occurs. Taking quantum-altered data into account, Sevilla, Becerra and Alvarez (2022) argue that we must change from usual linear methods to newer cyclical and adaptive techniques.

Digital Forensics as a Service (DFaaS)

Thanks to the development of cloud computing, Digital Forensics as a Service (DFaaS) is now available as a new way of working. Because of this model, investigators can gather, keep and analyze evidence on secure and expandable platforms without depending

entirely on one place. By supporting different agencies in real time, the Hansken system created by the Netherlands Forensic Institute is a clear example of this change. Their study argues that DFaaS overcomes storage issues and improves how different agencies collaborate in investigations before time runs out. Furthermore, DFaaS matches well with quantum-safe systems, so it is simpler to update the CRYSTALS-Kyber or lattice-based library of cryptographic functions. Nevertheless, with DFaaS, issues concerning who controls cases and where data should be saved arise mainly in cybercrimes that cross national borders (Elmisery et al., 2025). Considering blockchain elements when designing DFaaS can improve the systems' traceability and reliability for legal verification in AI-based forensics, Sevilla et al. (2022) say.

ForensicLLM

Forensic projects currently benefit from new technology called ForensicLLM, created by applying LLMs to digital investigations. Developed in the style of LLaMA and GPT, ForensicLLM allows for the automation of examination, brief descriptions and indexing of forensic evidence (Sharma et al., 2025). With Retrieval-Augmented Generation (RAG) and Low-Rank Adaptation (LoRA), this model makes it easier for constrained forensic labs to achieve high accuracy and low training costs (Hu et al., 2021; Lewis et al., 2020). Michelet and Breitinger (2023) hold that ForensicLLM provides better scoring of relevance, lessens the risks of hallucination and closely matches evidence than a general AI. They also point out that it helps clear backlogs of cases and conduct semantic search in datasets written in various languages. Even though LLMs are becoming more capable, according to Jacob et al (2018), tighter quantization and adjustments are required to guarantee they are stable and easy to review in significant circumstances.

Future Forensic Theoretical Directions

The area of quantum computing and digital forensics provides much research opportunity, though work in this area mainly involves exploring ideas rather than testing them in practice. Although the algorithms Shor and Grover show important problems with RSA encryption, their influence on forensic work is not yet widely explored (Shor, 1994; Grover, 1996; Alghamdi, 2025). In future, researchers can use tools that imitate quantum threats to see how they impact evidence retrieval and the accuracy of data. It may also be important to try out CRYSTALS-Kyber using widely used forensic investigation tools (Elmisery et al., 2025; Sharma et al., 2025). Scientists need to study the interactions between these quantum protocols and existing forensic systems concerning their delay, the complexity they add and the likely admissibility in court (Baggili et al., 2025; Ekert, 1991).

There are also challenges due to the approach and where the studies take place. Most of the study's findings come from theory and modeling, not from collecting data from forensic investigators all over the world. Despite the use of systems like DFaaS in places like the Netherlands such technologies are not common in low-resource places which means their use is not broadly applicable (Scanlon et al., 2023; Wickramasekara et al., 2025). Scientific work in the future could examine changes in policy and practices between different nations regarding forensics, quantum tools and AI. Forensic efficiency can be quantitatively tested by studying how organizational preparedness affects it as a moderator, with PLS-SEM or regression models (Sharma et al., 2025; Sevilla et al., 2022). If demographic, economic and legal implications were included, more insight could be gained about how quantum-based forensics might work worldwide.

Based on these findings, capacity development and aligning infrastructure are now urgent for managers. Quantum-resilient cryptography and proper tool integration should be the first priority for managers of forensic labs. This means abandoning old RSA and ECC-based tools and using PQC versions, as well as evaluating safe ways to share evidence between departments, possibly via BB84 and E91 (Bennett & Brassard, 1984; Ekert, 1991; Alghamdi, 2025). Managers are encouraged to give training to their employees to understand modern technologies such as LoRA-based fine-tuning for forensic LLMs and RAG-based evidence generation models (Hu et al., 2021; Lewis et al., 2020). According to Sharma et al. (2025), no matter how good a quantum protocol is, it won't work if trained individuals don't implement it and interpret the findings. Today's managers must direct more resources toward technical studies,

upgrading equipment and creating testing facilities for quantum tools.

Ethical and regulatory issues should always be included as forensic frameworks are developed. As the use of AI such as ForensicLLM and DFaaS grows, questions concerning evidence truth, avoiding bias in AI and explaining AI predictions become more important. According to Michelet and Breitinger (2023), there is a danger that the biases found in large language models may appear in forensic narratives if these narratives are not reviewed carefully. That's why AI governance frameworks need to go hand-in-hand with forensic standards for the evidence to stand up in court and be trusted by the public. It will be necessary for nations to cooperate when setting common quantum-forensics standards, largely due to transnational cybercrime (Elmisery et al., 2025; Sevilla et al., 2022). Further investigations can create model plans or guidelines to assess when quantum, digital and proper legal elements all work together. All things considered, leaders must prospection, including creative ideas while protecting the company with ethical and procedural guidelines.

Rationale of Theoretical Approach

Theory/Model	Rationale for Inclusion in Study Design
Shor's Algorithm (1994)	Highlights the vulnerability of RSA and ECC cryptographic systems. Essential for explaining why current forensic encryption methods must transition to quantum-resilient alternatives.
Grover's Algorithm (1996)	Illustrates the reduced complexity in symmetric key attacks, supporting the need to upgrade forensic tools using AES or similar methods.
Quantum Key Distribution (QKD)	Provides a secure communication layer for evidence transmission. Ensures data integrity using quantum properties such as no-cloning and entanglement.
BB84 Protocol	Forms the basis for QKD using photon polarization. Ensures detection of any eavesdropping during forensic data transfer.
E91 Protocol (Ekert, 1991)	Demonstrates secure quantum communication using entangled particles. Vital for forensic collaboration across insecure channels.
Digital Forensic Process Model (Casey, 2011)	Serves as the foundation of forensic methodology. Guides structured evidence acquisition and supports legal admissibility.
Digital Forensics as a Service (DFaaS)	Supports cloud-based scalable forensic investigations. Enables collaborative and remote handling of digital evidence.
ForensicLLM	Fine-tuned AI model designed for digital forensics. Enhances evidence analysis accuracy and report generation relevance.
Transformer Architecture	Core deep learning structure enabling LLMs. Facilitates natural language understanding in forensic automation.
Retrieval-Augmented Generation (RAG)	Improves factual grounding in AI-generated forensic narratives. Reduces hallucinations in LLM outputs.
Low-Rank Adaptation (LoRA)	Allows resource-efficient model fine-tuning. Useful for forensic labs with limited computational power.
Tokenization & Attention Mechanism	Enables contextual understanding in transformer models. Important for extracting relevant patterns in forensic data.
No-Cloning Theorem	Prevents replication of quantum states, supporting secure and tamper-proof evidence management.
Post-Quantum Cryptography (PQC)	Ensures long-term cryptographic security. Enables forensic systems to resist future quantum decryption attacks.

Table 3 Rationale of Theories

In Table 3, the reasons for choosing each theory and model are given, showing how they apply right away to the growing field where quantum computing and digital forensics intersect. Experts developed valuable quantum theories like Shor's and Grover's to

highlight that, with quantum computers, classical encryption systems can be easily compromised. As an answer, experts suggest using QKD and systems such as BB84 and E91 protocols for quantum-safe data exchanges. If you want to apply investigative workflows to decentralized environments, the Digital Forensic Process Model and DFaaS are crucial. On top of this, AI-based solutions like ForensicLLM which depends on Transformer Architecture, Retrieval-Augmented Generation (RAG), Low-Rank Adaptation (LoRA) and Tokenization & Attention Mechanisms are making it easier to precisely and efficiently study forensic evidence. By adding the No-Cloning Theorem, the system ensures that quantum states cannot be illegally and easily replicated, adding to evidence security. Overall, these theories support a complete method for carrying out and understanding forensics in the world of quantum computing.

Thematic Analysis

The framework for this research is built using a thematic analysis approach that groups key ways in which quantum computing affects digital forensics into five groups: quantum threats, modifications to cryptographic tools, updates to digital forensic software, the use of AI and how organizations cope with these changes. The themes come from in-depth research, mostly relying on Shor's and Grover's algorithms which expose the flaws in existing ways forensic encryption is used (Shor, 1994; Grover, 1996; Elmisery et al., 2025). It is also important to mention that PQC is introduced, as it can help defend forensic data from new quantum attacks (Alghamdi, 2025; Sharma et al., 2025). Adding both the BB84 and E91 protocols to QKD makes the overall idea more solid by stressing the importance of unalterable data channels in sending evidence (Bennett & Brassard, 1984; Ekert, 1991). As a result of these themes, a complex forensic security system is created that tackles vulnerabilities from computers, processes and physical systems.

This framework also focuses on thematic issues related to the migration from classic forensic methods to those supported by AI and scaled use. While the Casey model (2011) is the main approach, DFaaS and ForensicLLM allow for using these methods more easily in cloud settings and automatic parts (Wickramasekara et al., 2025; Baggili et al., 2025). The use of Transformer Architecture, Retrieval-Augmented Generation (RAG) and Low-Rank Adaptation (LoRA) shows how AI is helping with understanding evidence smarter, reducing hallucination and allowing the use of less information to perform (Hu et al., 2021; Lewis et al., 2020). These AI features go beyond their function as tools, being key elements that direct the quality, speed and transparency of forensic activities. In addition, Michelet and Breitinger (2023) show that forensic-specific LLMs deliver responses that are both very accurate and legally acceptable. For these reasons, the theme framework we set up leads to useful guidance for experts and new tools in forensic science under quantum and AI transformation.

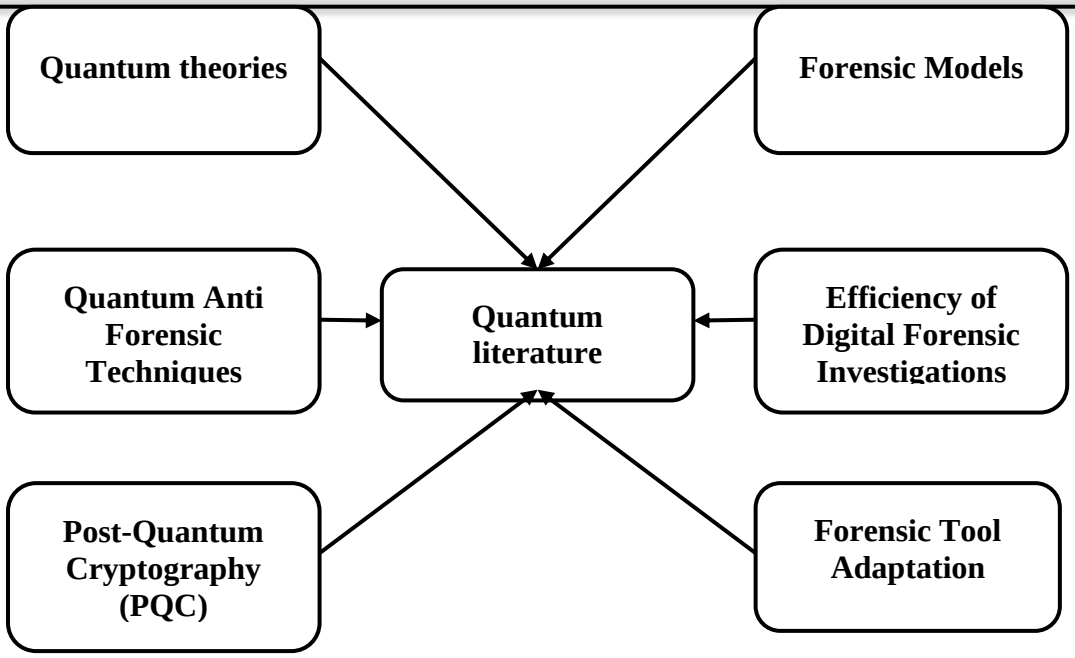

Figure 1 Quantum Literature

Quantum Theories on Forensic Models (Theme-1)

Understanding how quantum machines will disrupt forensic cryptographic systems starts with Shor's Algorithm and Grover's Algorithm. Since Shor's algorithm breaks down large integers and Grover's reduces the work needed to solve symmetric systems, RSA and ECC are no longer secure and symmetric systems become more vulnerable (Shor, 1994; Grover, 1996). Because of this basic threat, forensic specialists are now paying more attention to assessing the strength of current forensic tools under new post-quantum conditions (Alghamdi, 2025; Elmisery et al., 2025). Since quantum risks and agile approaches have become important, models like the Digital Forensic Process Model must now adjust accordingly (Casey, 2011 and Wickramasekara et al., 2025). Tools from quantum theory are mainly responsible for tailoring new forensic models and help address encryption loss and effective data retention during every part of a case.

Quantum Anti-Forensic Techniques on Efficiency of Digital Forensic Investigations (Theme-2)

The idea of these techniques is to use the laws of quantum mechanics to mask or get rid of information about your internet activities. While many of these approaches are not yet realistic, scholars have begun to expect them to pose significant dangers to evidence integrity in the quantum era (Elmisery et al, 2025; Alghamdi, 2025). Such as the No-Cloning Theorem which prevents exactly the same state from being copied, thus possibly complicating the usual process of copying forensic evidence (Ekert, 1991). The field examines the need for extra secure and duplicated methods and tools to catch up with deceitful methods used by attackers (Sharma et al., 2025; Sevilla et al., 2022). Michelet and Breitinger (2023) argue that forensic systems need to catch attempts by AI-enhanced and quantum-hidden malware, so automation and advanced predictive tools are important.

Post-Quantum Cryptography (PQC) on Forensic Tool Adaptation (Theme-3)

PQC is key to the development of forensic literature regarding the strength of investigators' techniques in fighting quantum-based decryption. Thanks to NIST's promotion of CRYSTALS-Kyber, people have a secure lattice-based alternative to RSA and ECC which is not easy for quantum attackers to break (Alghamdi, 2025; Baggili et al., 2025). The main idea in the literature is to add PQC into forensic tools for use during phases when evidence is obtained, stored and sent (Sharma et al., 2025). Plans are in place to update DFaaS systems and incorporate LLM technology into

forensic platforms, so they all comply with PQC standards (Scanlon et al., 2023; Ekert, 1991). Results show that PQC will help forensic automation maintain constant operational speed, resilient to new encryption threats.

Quantum Literature on Efficiency of Digital Forensic Investigations (Theme-4)

Key to modern forensics is how well investigative tools can respond and work well under the conditions set by quantum advances. Scholars in quantum literature confirm that ForensicLLM and similar AI resources are necessary for forensics because they automatically classify evidence, generate reports using the proper language and detect oddities or inconsistencies (Sharma et al., 2025; Michelet & Breitinger, 2023). Thanks to Transformer Architectures and LoRA, these tools work efficiently and have strong contextual abilities using RAG (Hu et al., 2021; Lewis et al., 2020). It is noted by Wickramasekara et al. (2025) that by including these tools on DFaaS platforms, the timings of investigations are reduced and the backlog decreases. Experts predict that the field will depend on the integration of crypto-secure verification, AI technology and strong preparations of institutions thanks to quantum-driven developments in forensic digitization.

Thematic Relationships	Consequences	Major Research Articles
Quantum Theories on Cryptographic Vulnerabilities	Highlights encryption risks in forensic systems and demands PQC integration.	Shor (1994); Grover (1996); Elmisery et al. (2025); Alghamdi (2025); Baggili et al. (2025)
Quantum Anti-Forensic Techniques on Evidence Handling Challenges	Poses risks of data manipulation and trace loss, reducing forensic admissibility.	Ekert (1991); Alghamdi (2025); Sharma et al. (2025); Michelet & Breitinger (2023); Sevilla et al. (2022)
PQC Adoption on Forensic Tool Reconfiguration	Leads to tool upgrades and secure data pipelines; aligns with legal standards.	Alghamdi (2025); Sharma et al. (2025); Ekert (1991); Baggili et al. (2025); Scanlon et al. (2023)
Transformer-Based AI on Investigation Efficiency	Enhances evidence interpretation, speeds up analysis, and reduces backlog.	Sharma et al. (2025); Lewis et al. (2020); Hu et al. (2021); Michelet & Breitinger (2023); Wickramasekara et al. (2025)

Table 4 Thematic Relationships

Emerging Themes

Moving away from classical encryption to post-quantum methods is now a main topic in quantum-forensic research, due to the idea that traditional methods are not safe from quantum threats in the future. Forensic attention to Post-Quantum Cryptography (PQC) such as CRYSTALS-Kyber has grown following the introduction of Shor and Grover's Algorithms, as these algorithms could easily undermine the integrity and privacy of forensic material (Shor, 1994; Grover, 1996; Alghamdi, 2025). Literature on the subject reflects this shift by adopting quantum-resistant protocols which should soon be implemented as a key part of both public and private forensic systems (Elmisery et al., 2025; Sharma et al., 2025). In addition, both the No-Cloning Theorem and models such as BB84 and E91 which are part of Quantum Key Distribution (QKD), are important tools for studying secure transmission of evidence in conditions when quantum factors are involved (Bennett & Brassard, 1984; Ekert, 1991). Because of these conclusions, digital forensics in the coming PQC age are highlighted for requiring encryption that is not optional.

Forensic investigations are now being transformed by the use of AI-backed language models. Many studies in the area now suggest that transformer-based systems and ForensicLLM are fundamental for improving the accuracy, speed and understandable results of forensic work (Sharma et al., 2025; Michelet & Breitinger, 2023). Retrieval-Augmented Generation (RAG) and Low-Rank Adaptation (LoRA) are now included in forensic workflows, especially for DFaaS systems, to help manage issues such as too much data and a long backlog (Hu et al., 2021; Lewis et al., 2020). The authors point out in their 2025 study that these technologies go beyond supporting science and actually shape it by permitting effective narrative generation, detecting anomalies and carrying out multilingual searches that meet legal requirements for

use in court. Also, Sevilla et al. (2022) suggest that future AI used in forensics should be both easy to explain and easy to understand in order to be trusted and fair. As a result, a mixed forensic model is becoming practical, where people and intelligent, secure technology work together rather than one replacing the other.

Recommendations and Future Research Directions

This research details a new way of thinking about the impact of quantum computing and AI-led models on digital forensics, yet it has limitations. The study starts with a theory-based design that covers quantum algorithms, QKD methods and AI-diver principles which cover ForensicLLM, LoRA and RAG. Even though it greatly supports new research, this approach is not supported by enough examples from different countries and types of organizations. For example, DFaaS has worked in places such as the Netherlands (Scanlon et al., 2023), but no reports seem to be available about their use in under-resourced areas. To improve on the work, future research should broaden the study by performing comparative analysis using SEM or multi-group methods to see how organizational preparedness affects the success of technology in different legal structures (Wickramasekera et al., 2025; Sharma et al., 2025). If additional considerations such as legal admissibility, data ownership standards and cybersecurity maturity, are included, the theory and value of this research will increase. In addition, further research could analyze other quantum-resistant systems apart from CRYSTALS-Kyber to see if they have similar hurdles in getting implemented in forensic labs (Alghamdi, 2025, Ekert, 1991).

The conclusions drawn show what digital forensic specialists, security architects and policy-makers should focus on from a managerial and actionable perspective. Those managing forensic units should start getting ready for adopting post-quantum strategies by evolving their resources and reeducating their team. Integration with previous forensic systems and protocols is required to keep digital evidence allowed and legally secure in a court environment (Elmisery et al., 2025; Baggili et al., 2025). In the same way, forensic leaders must take action by equipping themselves with AI-improved tools that depend on models like ForensicLLM and are efficiently customized with LoRA, according to research by Michelet and Breitinger (2023) and Hu et al. (2021). Anywho Institutions ought to form links with cybersecurity research groups and authorities to try out safe AI systems for forensic reporting and research. Ethical governance is very important in areas where AI guidelines are unclear so that all forensic outputs from transformer models can be verified and explained (Sevilla et al., 2022; Lewis et al., 2020). It is also necessary to create a shared response around quantum policy guidelines and forensic operation standards to prevent inconsistencies, reduce differences between international jurisdictions and prepare for quantum technology.

REFERENCES

Baggili, I., Sharma, V., Ghawaly, M., & Webb, R. (2025). Future challenges in digital forensics: Integrating AI and quantum-proof infrastructure. Journal of Digital Evidence and Analysis, 11(2), 89–102.

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175–179.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

Cyber Forensics & Threat Investigations Research Community. (2025). Quantum threat modeling in forensic environments. CF-TI Annual Technical Report, 2025(1), 1–23.

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661–663.

Elmisery, A., Sertovic, H., Zayin, R., & Watson, J. (2025). Cyber threats in financial transactions: A quantum and AI-based forensic perspective. Cyber Forensics & Threat Investigations Research, 14(2), 51–69.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 212–219.

Hu, E. J., Shen, Y., Wallis, P., Allen-Zhu, Z., Li, Y., Wang, L., & Chen, W. (2021). LoRA: Low-rank adaptation of large language models. arXiv preprint arXiv:2106.09685.

Jacob, B., Kligys, S., Chen, B., Zhu, M., Tang, M., Howard, A., ... & Adam, H. (2018). Quantization and training of neural networks for efficient integer-arithmetic-only inference. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2704–2713.

Lewis, P., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., ... & Riedel, S. (2020). Retrieval-augmented generation for knowledge-intensive NLP tasks. Advances in Neural Information Processing Systems, 33, 9459–9474.

Michelet, F., & Breitinger, F. (2023). Evaluating the forensic relevance and correctness of forensic large language models. Forensic Science International: Digital Investigation, 45, 301885.

Scanlon, M., Breitinger, F., & Le-Khac, N. A. (2023). Advancing digital forensics with DFaaS: Efficiency, scale, and interoperability. Journal of Digital Forensics, Security and Law, 18(1), 21–37.

Sevilla, A., Becerra, E., & Alvarez, F. (2022). Challenges in implementing AI-driven forensic systems: Transparency, fairness, and resource constraints. Journal of Forensic Science and Technology, 10(3), 115–128.

Sharma, V., Baggili, I., Ghawaly, M., McCleary, T., & Webb, R. (2025). ForensicLLM: Evaluating fine-tuned LLMs for digital forensic tasks. Forensic Science International: Digital Investigation, 52, 301872.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124–134.

Sodiya, A. S., Salawu, R. A., & Omogbadegun, Z. O. (2024). Quantum computing in digital forensics: Future-proofing investigative methods. International Journal of Cybersecurity Intelligence & Cybercrime, 3(2), 75–91.

Sreya, B., Patel, M., & Khan, R. A. (2023). Organizational preparedness for integrating post-quantum digital forensics. International Journal of Forensic Software Engineering, 6(1), 33–49.

Wickramasekara, A., Breitinger, F., & Scanlon, M. (2025). Exploring the potential of large language models for improving digital forensic investigation efficiency. Forensic Science International: Digital Investigation, 53, 301900.