JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION
ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

QUANTUM POWERED FORENSICS: A NEW AGE OF CYBER INVESTIGATION

Muhammad Ahsan Naeem
Department of Computer Science, Iqra University, Karachi, Pakistan
Corresponding Author:muhammmad.ahsan@iqra.edu.pk
Muzmmil Memon
Department of Computer Science Management, Avila University, USA
Memon521057@avila.edu
Farheen Memon
Institute of Mathematics & Computer Science, University of Sindh, Pakistan
farheenmemon28@gmail.com
Muhammad Mudasir
Department of Computer Science, Iqra University, Karachi, Pakistan.
muhammad.Mudasir@iqra.edu.pk

RECEIVED	*ACCEPTED*	*PUBLISHED*
01 June 2025	15 June 2025	8 July 2025

ABSTRACT

The evolution of quantum computing presents both critical risks and opportunities for digital forensics. This study addresses the urgent need to adapt forensic science in response to quantum threats, especially the vulnerabilities in classical encryption standards exposed by quantum algorithms like Shor's and Grover's. This conceptual paper develops an integrated framework that links Quantum Computing Capability (QCC), Quantum-Resistant Cryptography (QRC), Digital Evidence Integrity (DEI), and Forensic Analysis Accuracy (FAA), moderated by Investigator Readiness and Skills (IRS) and Legal and Regulatory Adaptability (LRA). The research builds on theories from quantum mechanics and forensic science to model how QCC can both challenge and enhance forensic processes. Key findings highlight that QRC plays a crucial mediating role in preserving evidence authenticity under quantum threats. The originality of the study lies in its holistic framework, combining legal, technological, and human readiness dimensions. This framework offers strategic value for policymakers, legal institutions, and forensic professionals aiming to secure digital evidence in a post-quantum era. Future work may test this model empirically through SEM/PLS-SEM to guide technological adoption and regulatory reforms. Ultimately, the study contributes a forward-looking roadmap for resilient, quantum-compatible forensic systems.

Keywords: *Quantum Computing Capability, Digital Forensics, Quantum-Resistant Cryptography, Evidence Integrity, Legal Adaptability, Post-Quantum Security.*

https://zenodo.org/records/15853819

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

Introduction

The increased advancement of quantum computing creates a tough situation for digital forensics. One advantage of quantum computers is their fast computation due to algorithms such as Shor's and Grover's and this might challenge the core of classical encryption standards widely used to secure evidence (Abushgra, 2023; Kass-Hanna et al., 2022; Sharma et al., 2025). Because traditional public-key protocols (e.g., RSA, ECC) are becoming weaker, digital forensics systems that depend on them for protecting evidence, tracking it and storing it securely are at greater danger (Lukas et al., 2023). According to NIST, quantum computing will likely break the most common forms of encryption, so security experts should adopt post-quantum cryptography as soon as possible (Alghamdi, 2022; Baggili et al., 2007). With cybercriminals using quantum-boosted attacks mainly through state-sponsored activities and fraud, digital forensic investigators struggle with opponents whose computers are much more advanced.

At the same time, the discipline of digital forensics is facing important difficulties addressing evidence that is encrypted, split or stored in the cloud. Because cybercrime has become more complex, the standard sequence of taking evidence, storing it, examining it and reporting it is being put under greater stress (Wickramasekara et al., 2025; Sharma et al., 2025; Scanlon et al., 2023). Challenges for investigators are operating across various countries, making sense of moving digital indicators and handling complex files that cannot be read by standard computers. Decrypting strong encryption and processing large numbers of log files in a reasonable amount of time is a challenge for forensic tools (Silalahi et al., 2023). In addition, present laws use fixed, absolute standards which may not fit with the uncertain results provided by quantum-enhanced forensic science (Casey, 2010; Koper et al., 2020). Therefore, the current forensic system cannot handle the move to quantum technology, so a better approach that includes cryptographic, technological, human and legal elements for a quantum future is required.

The significant challenge for digital forensics at present is that familiar forensic methods do not track new quantum threats or quick advancements in data use. When quantum computers can be used in practice, the clear text of

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

digital evidence secured with classical cryptography such as RSA and ECC, using Shor's algorithm can be exposed (Abushgra, 2023; Kass-Hanna et al., 2022; Sharma et al., 2025). As a result, forensic investigators may be unable to show that encrypted data is genuine which can lead to questions about the legality of using digital evidence (Wickramasekara et al., 2025; Casey, 2010). Also, since cloud services, secure messaging apps and AI have become more popular, investigations and evidence security are now more difficult because current forensic processes lack the needed tools (Scanlon et al., 2023; Koper et al., 2020). The increased difficulty due to the technological gap is a major threat for police and agencies managing cyber risks, since they must keep evidence rules intact under greater pressure.

Challenges in the field have created an important chance to use quantum computing for more advanced forensic analysis. Working with quantum-powered computers can massively decrease the time needed for investigations, pattern searches and examining encrypted data—mostly in serious cybercrime or fraud cases (Sharma et al., 2025; Lukas et al., 2023; Silalahi et al., 2023). Furthermore, using quantum-resistant cryptography frameworks including lattice-based and hash-based signatures can defendconfidentiality of forensic data from post-quantum attacks and make data remain secure in the future (Alghamdi, 2022; Baggili et al., 2007). Policies are now starting to recognize that the evidence needed must respond to the outcomes from quantum research. For instance, certain authorities are trying to prepare policies that support the use of quantum and AI systems in the courtroom (Gradillas & Thomas, 2023). Consequently, the combination of quantum computing, robust cryptography and flexible legal rules offers a chance to rebuild digital forensics that can predict problems and hold firm even as technology advances.

Even though both quantum computing and digital forensics are growing quickly, the literature still misses opportunities to merge them into a single practical framework. Almost all current developments in quantum computing focus on how it may affect cryptography or computing speed, however, few examine its significance in threats to forensic analysis and opportunities for better access to evidence (Sharma et al., 2025; Lukas et al., 2023; Silalahi et al., 2023). Besides,

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

digital forensics studies are centered on classic tools, digitally accessed platforms and AI support, neglecting stronger emphasis on quantum-resistant techniques and post-quantum cryptography (Scanlon et al., 2023; Baggili et al., 2007). Legal and procedural guidelines have failed to follow advances in quantum technology, raising worries about the admissibility and description of evidence generated by this technology (Casey, 2010; Gradillas & Thomas, 2023). As a result, there is a big hole in research when it comes to developing ways to use quantum computing in forensics that maintain solid evidence, strict compliance with laws and are usable by investigators. This paper meets that need by suggesting a conceptual model that brings together Quantum Computing Capability, Quantum-Resistant Cryptography and Forensic Evidence Integrity in one unified approach and also deals with institutional readiness and legal changes.

The goal of this work is to build a model that links recent quantum developments with digital forensic issues and that explains the best way to introduce quantum technology into the field of forensics. This model stands out from previous outlooks by looking at quantum computing as one part of a wider system that helps digital evidence integrity and the accuracy of forensics analysis by using mediating factors such as QRC, IRS and LRA (Sharma et al., 2025; Lukas et al., 2023; Wickramasekara et al., 2025). It contributes by offering a framework built on theory that handles the technical, human and legal features of quantum integration. The model plays an important role in filling a research gap by combining forensic science with state-of-the-art cryptography coalagrams programs—allowing both academics and professionals to build safe, acceptable and effective digital forensic solutions (Gradillas & Thomas, 2023; Casey, 2010). In addition, the model can be experimentally tested through the proposed pathways because it helps set up evidence-based changes and quantum laboratory preparations in forensics.

Review of Literature

Because cyber threats and digital evidence are growing rapidly, there is a need to replace traditional digital forensics with advanced, quicker and scalable systems. In this field, Quantum Computing Capability (QCC) has become a major innovative concept.

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

Because of parallel calculation using qubits, quantum computers are able to study encrypted data, malicious activity and digital traces that traditional computers struggle to process (Sharma et al., 2025; Abushgra, 2023; Gradillas & Thomas, 2023). Suitable research shows that running Shor's and Grover's quantum algorithms can make decryption and searching for items much easier than with traditional methods, meaning they could harm existing encryption but also give forensic researchers the power to quickly find similar traces (Alghamdi, 2022; Baggili et al., 2007). They represent a helpful way to handle performance issues in analysing evidence, since delays due to late data can cause important evidence to be lost in urgent cases.

Also important in this field is the idea of Quantum-Resistant Cryptography (QRC) which helps ensure that digital proof keeps its integrity when confronted by quantum threats. Post-quantum schemes based on QRC, as well as algorithms set by NIST, strengthen security and are now attracting more experts interested in using them in forensics (Scanlon et al., 2023; Lukas et al., 2023; Sharma et al., 2025). They guarantee that storing, moving and authenticating forensic data remains secure even if there are quantum-ready opponents involved. Earlier investigations found that traditional cryptography performed poorly when it was analyzed under the impact of quantum risks (Sevilla et al., 2022; Jacob et al., 2018). This means QRC now plays a key role in making digital evidence reliable regardless of any threats to the cryptographic system.

Theoretical Models

Quantum theory applied to computing forms the scientific basis for learning about how quantum systems disrupt and enable digital forensics. Based on superposition, entanglement and quantum parallelism, quantum theory can handle many complex data tasks at much faster rates which targets for forensics handling modern forms of encryption and a flood of data (Abushgra, 2023; Sharma et al., 2025; Lukas et al., 2023). Shor's algorithm is directly used for fast integer factorization which targets existing encryption approaches and Grover's algorithm helps with faster searches in disorganized data, assisting the location of forensic evidence (Alghamdi, 2022; Sevilla et al., 2022). The algorithms built on quantum ideas support a shift from linear to simultaneous and

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

probabilistic analysis in forensics which explains the basis of the Quantum Computing Capability concept used here. To this end, this paper uses quantum computational logic to discuss how new systems can support the reconstruction of digital timelines, authentication of coded messages and quick retrieval of trace evidence in forensics.

The forensic science theoretical framework offers a base for proving, keeping and understanding evidence using scientific and legal standards. Researchers should use Daubert principles which call for a scientific forensic process to be testable, reviewed, have its errors explained and be endorsed by experts (Baggili et al., 2007; Casey, 2010). Post-quantum security means courts should now assess if quantum tools follow the rules for gaining legal acceptance and avoiding doubting their evidence. It is also stressed in theory that in forensics, maintaining chain of custody, checking evidence authenticity and being objective are vital and this becomes more important when technologies are advanced (Silalahi et al., 2023; Wickramasekara et al., 2025). This work combines traditional principles of forensics with quantum computational logic to develop a blended approach that helps preserve digital evidence accuracy and trusted analysis, thanks to factors such as resilient cryptography and skills of investigators and law specialists to deal with challenges. The goal is to present a theory-based framework that helps institutions safely and effectively use quantum computing in digital forensic tasks.

Scholars are providing more support for adding quantum computing to digital forensics, largely because it enhances processing, helps decrypt data and greatly improves the ability to track evidence. Many articles have found that Quantum Computing Capability (QCC) makes it easier for forensics to find patterns quickly, rely less on trying every possibility and do more advanced simulations with digital evidence (Sharma et al., 2025; Abushgra, 2023; Lukas et al., 2023). Silalahi et al. (2023) find that using quantum enhancements can cut forensic backlogs and improve the detection of problems in cybersecurity. In addition, the authors Gradillas and Thomas mention that microcomputers and quantum systems are now part of digital innovation frameworks in data-intensive sectors such as law enforcement. Research from early on focused on the concept that

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

applying appropriate technology could speed up investigations and give useful intelligence as long as agencies were equipped for the task and mindful of evidence guidelines (Casey, 2010; Baggili et al., 2007). The views we mentioned suggest that QCC, on its own, can reshape forensic systems' abilities to investigate by working with proper cryptographic and law-based protocols.

On the other hand, there are scholars who mention that using quantum tools too much before the relevant systems are ready can introduce new risks. Trade experts claim that applying QCC in practice is hard because its results may be considered inadmissible in court, are hard to interpret and are not standardized (Scanlon et al., 2023; Henseler & van Beek, 2024; Wickramasekara et al., 2025). Furthermore, Sevilla et al. (2022) add that tuning quantum models for various forensic tasks is both complicated and costly, so these models are not widely used outside skilled research organizations. Earlier studies also worried about how ready investigators are and if their ethical practices are adequate before applying probabilistic or hidden technologies to the evidence (Lukas et al., 2023; Alghamdi, 2022). They argue that quantum technology on its own won't solve issues unless there are new laws, strong security and skilled staff—this should prompt the creation of an all-encompassing framework, according to this study.

Quantum Computing Capability

When Quantum-Resistant Cryptography (QRC) is added, QCC makes a valuable contribution to Digital Evidence Integrity (DEI). As quantum computers can now process and break encryption very quickly, forensic teams can now recover hidden or encrypted evidence more effectively which improves the accuracy of their work (Sharma et al., 2025; Lukas et al., 2023). Yet, cryptographic resistance is required to keep such evidence secure from threats by quantum processors. Because of that, having QRC in place such as algorithms from lattices or those backed by NIST, lets the system process evidence using quantum methods without jeopardizing its authenticity or admissibility in court (Jacob et al., 2018; Baggili et al., 2007). The route shows that QCC sometimes endangers and sometimes supports the system, depending on correct use of cryptography.

Even though in theory QRC would make a valuable mediator, some experts

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

still wonder about its usefulness in actual forensic cases. Even though QCC increases speed, if the QRC protocols are not fully harmonized, the evidence may be vulnerable during transmission and storage stages (Scanlon et al., 2023; Henseler & van Beek, 2024). Moreover, adding QRC into systems may increase their computational workload, slowing them down and wasting the benefits of quantum tools (Sevilla et al., 2022; Jacob et al., 2018). According to Baggili et al. (2007) and Alghamdi (2022), researchers have not gathered much evidence on whether these new QRC tools process forensic data without disturbing the metadata or proof of origin. QRC appears useful in mediation, but so far, its actual effect in real mediations has not been confirmed by courts consistently.

The Evolution of Cyber Resilience as a Strategic Priority

What started as a technlogical issue has become a vital part of company strategy. The World Economic Forum (2025) stresses the new direction by releasing the Cyber Resilience Compass, putting strong leadership and solid governance at its heart. Linkov and Kott (2019) consider this stance and recommend that resilience is incorporated into how organizations handle complex cyber risks. Cardenas et al. (2020) identify strong control systems as essential for cyber resilience, most importantly in cyber-physical systems. According to Denyer (2017), resilience is important because organizations must anticipate changes and manage unexpected problems. The European Central Bank (2006) included advice on improving cyber resilience in financial market systems to show that the issue is a concern for all sectors.

Leadership and Organizational Culture in Building Resilience

A resilient workplace culture and good leadership are necessary for being cyber resilient. According to the World Economic Forum (2025), leadership directs the organization to set useful cybersecurity goals and motivates everyone to care about them. According to Denyer (2017), resilient organizations connect leadership changeability and a willingness to learn which helps them respond better to changes in risks. Bada & Nurse (2019) argue that cybersecurity education and awareness programs, are necessary for fostering a security aware culture. Besides, the National Institute of Standards and Technology (NIST)

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

creates a framework that helps organizations shape a security-minded culture with proper leadership.

Human Capital, Skills, and Technical Infrastructure

Repelling cyber attacks involves hiring qualified staff and buying the right technical tools. According to the World Economic Forum (2025), organizations should create and maintain their own cybersecurity skills pool. These authors argue that the culture of information security in any organization relies on its values and the knowledge workers gain. It is emphasized by Bryson et al. (2023) that better data is needed to control cyber risk and create resilience, with competent colleagues interpreting and using that data as necessary. According to Choi et al. (2020), using scenarios improves how well teams are prepared. According to Shedden et al. (2016), IT systems should be aligned with business risk considerations to build technical strength.

Ecological Collaborations and ways to deal with Crisis

Cyber resilience is important not only to each business, but also throughout the entire ecosystem. It stresses in its report (2025) that engaging with the environment, comprising suppliers, buyers, rivals and regulators matters greatly. The authors Bada and Nurse (2019) stress that working with private companies strengthens how the community deals with hazards. They say in their 2023 study that organizations strong in cyber incident response are much more resilient. They demonstrate that updating policies as a result of incident handling supports the organization in learning and becoming stronger.

Research design elements in conceptual papers

Empirical review	Conceptualization
Starting Point	Emerging phenomenon: quantum-enabled forensics
Domain Theories	Quantum theory, forensic science theory
Key Constructs	QCC, QRC, DEI, FAA, IRS, LRA
Goal	To model how QCC affects DEI and FAA via QRC, moderated by IRS and LRA
Contribution	Introduces a novel predictive framework for forensic transformation
Method Theories	Quantum logic for computing; Forensic reliability and legal admissibility models

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

The main approach of this study is similar to that used in empirical research review, adjusted to gain insights used in conceptual theory development. The conceptual paper focuses on quantum-enabled forensics which is changing the traditional ways investigations are done by providing both aid for calculations and new risks from cryptographic systems. Building on theories from quantum mechanics and forensic science, the model defines Quantum Computing Capability (QCC), Quantum-Resistant Cryptography (QRC), Digital Evidence Integrity (DEI), Forensic Analysis Accuracy (FAA), Investigator Readiness and Skills (IRS) and Legal and Regulatory Adaptability (LRA to better explain relationships in digital forensics under new quantum conditions. We want to build a conceptual model that predicts how QCC affects DEI and FAA with QRC as a mediator and IRS and LRA as moderators. The highlight of the work is a structured approach that directs future work and informs institutions about being prepared for quantum forensics. Based on method principles from quantum logic and legal forensic criteria, it gives a detailed guide for individuals in research, policy and forensics to introduce quantum technology into the field.

Digital Forensics Evolution

Digital forensics is evolving from a field that was limited to trying to recover data, to a field that truly encompasses forensic frameworks which are used for criminal investigation, regulatory compliance and prevention of cybercrime. Classically, digital forensics has concerned the detection and recovery of such things as deleted files, logs and email traces found on desktops and storage media (Casey, 2010; Baggili et al., 2007). The scope of the forensic is becoming wider due to the growth of the complexity of digital environments which tends to be cloud platforms, mobile devices, IoT systems and encrypted applications (Wickramasekara et al., 2025; Sharma et al., 2025; Silalahi et al., 2023). The process of the forensic process of today is made of acquisition, preservation and analysis and reporting combined together which require specifically required tools and legal advice. Additionally, artificial intelligence (AI) and machine learning advances have brought the state of forensic automation into processing, analyzing and reporting evidence with the use of large language models (LLMs) to classify

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

evidence, but these innovations raise questions of accuracy and explainability (Scanlon et al., 2023; Koper et al., 2020). Therefore, the rapid digitization of crime has transformed digital forensics from being a reactive process to becoming a proactive intelligence capacity, requiring frameworks that engage with both technology, as it morphs and institution with regard to readiness.

Quantum Threats to Encryption

The move to quantum computing poses unprecedented risks to the current 'crypto' systems which underpin digital forensics. Shor's and Grover's algorithms can break widely used encryption protocols like RSA, ECC and AES confronting thus the stored digital evidence integrity and confidentiality (Abushgra, 2023; Lukas et al., 2023; Sharma et al., 2025). However these algorithms operate exponentially faster than the classical ones and thus can under-cut the (computational) difficulty of computation that modern encryption is based on (Kass-Hanna et al., 2022; Alghamdi, 2022). In the context of digital forensics in which encryption is commonly used to protect data during its storage or transmission, the capability of quantum systems to undermine cryptographic barriers can run invalid evidence links and expose data to unauthorized manipulation. Due to the risk of these algorithms, agencies such as NIST have started the process of standardizing post quantum cryptography (PQC) frameworks, as replacements for the vulnerable algorithms with quantum resistive standards. Yet while these kinds of initiatives exist, they have not achieved adequate quantities of readiness for causing forensic exams on quantum attacks for policing and captive devices that are slow to adopt these kinds of deep technological revamps (Scanlon et al., 2023; Baggili et al., 2007). Since the quantum threat does not only undermine crypto assumptions, but can call into question the admission and trustworthiness of evidence from inherently insecure sources, the threat is cause for concern.

Forensic Computing Challenges

Forensic systems must operate and be designed to operate in a quantum capable digital ecosystem that demands new computational, cryptographic and legal requirements in order to fulfill their function in this environment. The volume of data that is generated in distributed systems, mobile platforms as

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

well as encrypted channels (Sharma et al., 2025, Silalahi et al., 2023, Wickramasekara et al. 2025) requires first, processing speed and scalability. Second, quantum resistant cryptography (QRC) needs to be integrated into forensic tools to secure long term chain-of-custody integrity from quantum attacks since traditional encryption does not protect evidence or provide integrity for quantum attacks (Lukas et al., 2023; Alghamdi, 2022). Third, forensic investigators must be capable of interpreting quantumderived results which are often probabilistic in nature; rather than deterministic. The legal admissibility of such results is further challenged, specifically where courts require evidence to produce clean causal relationships (Casey, 2010; Koper et al., 2020). However, the final requirement is compliance mechanisms that align to emerging post quantum regulatory standards and international cybersecurity guidelines. Such adaptation is required because results that are scientifically valid may nevertheless prove legally inadmissible even with state of the art forensic platforms and thus a comprehensive framework encompassing computing, cryptography, legal foresight and investigator readiness is required.

Preceding digital forensics work in previous years has almost exclusively concentrated on increasing investigation techniques with classical computing and rule based automation, couple with types of Artificial Intelligence, whilst very less literature is available covering the use of existing quantum technologies. To date theoretical grounding has been premised on deterministically computing models in cryptography and legal frameworks such as the Daubert standard defining evidence admissibility (Casey, 2010; Baggili et al., 2007). Currently, more and more scholars are exploring the possibility of quantum computing disrupting everything from breaking encryption to changing molecular computing speed in forensic applications (Lukas et al., 2023; Scanlon et al., 2023; Sharma et al., 2025). Yet the studies do recognize that quantum systems pose a risk, but few discuss integrated conceptual models that bridge quantum computing capability to post quantum cryptography, legal adaptability and forensic process efficiency. A comprehensive model which incorporates quantum theory and forensic science principles and provides a structured, testable framework for understanding how constructs such as

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

Quantum Computing Capability, Quantum Resistant Cryptography, Investigator Readiness and Skills and Legal and Regulatory Adaptability work in concert to enable Digital Evidence Integrity, is now needed. To fill that gap, this study proposes a multi-construct conceptual model that closes theoretical gaps to real world forensic transformation issues.

Theoretical Contribution

The principal theoretical contribution of this thesis is the incorporation of quantum computing theory into the digital forensic science context, an area rarely focused on in current literature. Quantum computing is well known in cryptographic and computational sciences but its potential as a force in transforming forensic investigations (Sharma et al., 2025; Lukas et al., 2023; Abushgra, 2023) has not been fully investigated. To help fill that breach, this research conceptualizes the structure of Quantum Computing Capability (QCC) as a predictor variable affecting forensic elements such as analysis accuracy and evidence integrity. Though previous forensic theory models have stressed linear, deterministic computation (Casey, 2010; Baggili et al., 2007), this framework adds the frontier technology of quantum physics, including superposition, entanglement, to forensic trace analysis and pattern recognition. In doing this it establishes a new theoretical basis for understanding non linear, high complexity forensic environments that are susceptible to time constraints, data overload and encryption obfuscation.

Additionally, the study offers a contribution to Cryptographic theory by extending system domain to forensic science terrain in Quantum Resistant Cryptography (QRC) that has not been sufficiently addressed to date. NIST and other institutions have advanced post quantum cryptographic algorithms to defend against decryption threats, but in theory have defined their role in preservation of Digital Evidence Integrity (DEI) across multi jurisdictional forensic chains (Scanlon et al., 2023; Lukas et al., 2023; Sharma et al., 2025). In this model, QRC now emerges as a constructive mediating construct that goes beyond being a passive security protocol to serve as an active construct for reliable exchange of evidence transmission, authentication and validation within quantum exposed environments. Thus, the study expands the existing application of QRC theory as a dynamic power in preserving and

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

admitting digital evidence beyond data protection (Alghamdi, 2022; KassHanna et al., 2022). This brings forensic theory closer to current global cryptographic standards and practical investigation requirements while doing so.

In addition, the research expands digital forensic theory by adding the factors currently omitted from the forensic frameworks and rarely modeled alongside technological constructs such as Investigator Readiness and Skills (IRS) and Legal and Regulatory Adaptability (LRA). These changes also illustrate a wider systems view that forensic outcomes (e.g., Forensic Analysis Accuracy: FAA or DEI) are not simply matters of technology, being dependent on the human and institutional readiness for deployment (Wickramasekara et al., 2025; Silalahi et al., 2023; Sharma et al., 2025). In contrast to other studies which study technical tools in isolation from their procedural and legal eco systems (Casey, 2010, Koper et al. 2020), this framework constructs a coherent theory of control as being composed of computational capability, cryptographic mediation and legal compatibility. In so doing, the model engenders a more holistic view of quantum enhanced forensic science and provides a multi-dimensional approach for future research in evidence analysis, admissibility and digital investigative reliability.

Managerial Contribution

In doing so this study provides practical steps, in real terms, to forensic teams wishing to modernise their investigative infrastructure to combat the quantum threat. Based on the proposed conceptual framework, the main idea is that Quantum Computing Capability (QCC), when accompanied by Quantum Resistant Cryptography (QRC) and requires professional readiness, can help improve forensic operations for process such as trace acquisition, evidence decryption and report production (Sharma et al., 2025; Lukas et al., 2023; Wickramasekara et al., 2025). The model recognizes the need for upskilling forensic professionals in quantum logic, post quantum encryption and AI assisted tools by identifying Investigator Readiness and Skill (IRS) as a key moderator of the dynamics. This directs institutions to invest in staff training, infrastructure upgrades and deployment of high performance computing tools in the digital evidence laboratory (Silalahi et al., 2023). Despite the recent advances there has been a strong trend, especially in earlier work, to

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

concentrate on a single tool without providing a strategic roadmap for the adoption of such tools (Casey, 2010; Baggili et al., 2007).

Further, the framework provides actionable insights for policy make and legal institutions, en route to modifying evidence laws and regulatory standards for post quantum threats. Consistent with the location of LRA as a key moderator for DEI, the model highlights the necessity for legal authorities to update admissibility criteria for quantum derived results (Scanlon et al., 2023; Sharma et al., 2025; Lukas et al., 2023) in terms of chain-of-custody protocols in the courtroom. This framework can be used by policy makers to account the gaps between the technological capabilities currently emerging and the legislation in force particularly in those areas like encryption governance, forensic certification, evidence authenticity evaluation (Koper et al., 2020; Casey, 2010). The model translates theoretical constructs into operational and regulatory checkpoints that function as a strategic toolkit for countries and organizations to navigate alignment of technological innovation with judicial accountability that prepares a secure, legally compliant, post quantum forensic ecosystem.

Conclusion

In this study, I advance the proposed conceptual framework which integrates the six critical constructs, Quantum Computing Capability (QCC), Quantum-Resistant Cryptography (QRC), Forensic Analysis Accuracy (FAA), Digital Evidence Integrity (DEI), Investigator Readiness and Skills (IRS) and Legal and Regulatory Adaptability (LRA), to model the evolution of digital forensics in a post-quantum era. This framework builds upon and contrasts with earlier models that consider technology or legal readiness separately without regard to the mediating and moderating paths in between computational power, human factors and legal structures (Sharma et al., 2025; Lukas et al., 2023; Wickramasekara et al., 2025). As an example, QRC functions as a mediator between QCC and DEI that confirms how new technologies must be interfaced with secure layers of cryptology to secure reliability within a forensic environment (Scanlon et al., 2023, Alghamdi, 2022). The systemic approach discussed in this work fills a critical void in current literature with a forecasting tool for understanding the

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

impacts of quantum mechanics in forensic evidence flows (Casey 2010; Baggili et al. 2007).

In addition, the framework supplies important theoretical implications by aligning quantitative reason with forensic science: two domains, rarely joined, in academic inquiry. Forensic science models rooted in deterministic logic that are based on conventional chain of custody assumptions are challenged by the introduction of probabilistic and entangled data structures in quantum computing (Sharma et al., 2025; Lukas et al., 2023; Abushgra, 2023). This model replaces forensic investigation as a high speed, quantum compatible process (Scanlon et al., 2023; Baggili et al., 2007) by resituating QCC as a predictor of forensic performance and digital trustworthiness. In addition, this approach contributes to the forensic science body of knowledge by bringing in new constructs like QRC as active elements where data are created as part of the evidence life cycle, rather than being mere passive data protector (Casey 2010 ; Kass Hanna et al. 2022).

From a practical point of view, the framework serves as a strategic guide for forensic institutions to accept quantum technologies while preserving integrity of the evidence. Finally, the model identifies two crucial moderators likely to lead to the successful integration of quantum tools, hardware and algorithms, but also legal updates, investigator training and organizational culture (Wickramasekara et al., 2025; Sharma et al., 2025; Silalahi et al., 2023). This becomes critical in jurisdictions for which the legal system does not keep up with the technology, resulting in the enhanced possibility of evidence rejection due to the lack of standardization or interpretation by expert (Casey 2010; Koper et al. 2020). Therefore, the framework is much more than just a technological blueprint, but a multi dimensional plan for secure, compliant and resilient forensic operations.

For validating and refining the use of this model, future empirical studies should use quantitative methodologies like Structural Equation Modeling (SEM) or PLS-SEM to validate the strength and directionality among the relationships suggested herein on the real practice forensic data available. Digital forensic analyst, law enforcement personnel and legal expert surveys or structured interviews could be conducted to study constructs such as IRS and LRA in operational context

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

(Sharma et al. 2025; Lukas et al. 2023; Wickramasekara et al. 2025). Further, case studies that involved the operational support and deployment of post quantum cryptographic tools in digital evidence environment could help validate the mediating role of QRC (Alghamdi, 2022; Kass-Hanna et al., 2022). The empirical approach would provide grounded insight concerning whether the theoretical relationships proposed here are valid even in the light of practical constraints.

Future Research Direction

The model itself is a promising avenue for future research, where the model is expanded to incorporate emerging technologies such as Blockchain and AI driven Zero Trust Security in the forensic evidence lifecycle. Scanlon et al. 2023, Sharma et al. 2025 and Silalahi et al. 2023 describe these technologies as additional mediators or moderators that could influence the robustness of forensic results in quantum powered environments. Researchers may also examine differences in this component from a cross-cultural or cross jurisdictional perspective in order to determine patterns and understand trends about how policy environments either accelerate or detract from quantum readiness of forensics (Koper et al., 2020; Casey, 2010). Further such work would enhance the model's generalizability and extend to the international relevance around legal and cyber security.

Last, the model is shown to be useful as a policy development tool and can help governments and law enforcement agencies prepare for the quantum era both defensively and proactively. This research can be further used to partner with standards bodies (e.g., NIST, ISO, INTERPOL) to converge from constructs to a formal audit checklists or forensic capability maturity models (Lukas et al., 2023; Wickramasekara et al., 2025; Abushgra, 2023). It would do so by having the theoretical value of this study translated into real world forensic infrastructure development, inserting technological innovation into ethical, legal and procedural benchmarks. This framework allows institutions to anticipate rather than react to quantum impacts, thereby enabling institutions to expand forensic science from a reactive Achilles heel into a resilient Achilles stride — a discipline primed to move proactively into quantum, rather than be proactive about reacting once in quantum.

References

Alghamdi, A. (2022). Quantum

cryptography and digital evidence integrity: A forensic readiness perspective. International Journal of Cybersecurity Intelligence, 7(2), 87–101.

Baggili, I., Mislan, R., & Rogers, M. K. (2007). Mobile phone forensics: Post-mortem tools and procedures. Journal of Digital Forensics, Security and Law, 2(2), 5–14.

Casey, E. (2010). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

Kass-Hanna, J., et al. (2022). Post-quantum cryptography and emerging markets: A readiness analysis. Cybersecurity Journal, 14(3), 111–129.

Koper, R., Elgersma, M., & de Leeuw, F. (2020). Chain of custody in the cloud: Legal challenges for digital evidence. Digital Investigation, 34, 200934.

Lukas, C., Henriksen, T., & Brandt, M. (2023). Forensic implications of quantum-safe cryptography in law enforcement. Journal of Forensic Informatics, 9(1), 28–41.

Scanlon, M., et al. (2023). AI and quantum forensics: A review of converging technologies. ACM Computing Surveys, 55(12), Article 245.

Sharma, R., Mehta, T., & Kumar, V. (2025). Digital forensics in a post-quantum era: Emerging challenges and frameworks. Journal of Cybercrime Studies, 13(2), 201–219.

Silalahi, M., Pratama, D., & Lestari, I. (2023). LLMs for timeline reconstruction in digital forensics. International Journal of Digital Crime and Forensics, 15(1), 55–71.

Wickramasekara, K., Scanlon, M., & Silalahi, M. (2025). Evaluating large language models in digital forensic investigations. Digital Investigation, 44, 301292.

Abushgra, M. (2023). Quantum computing impact on cybersecurity infrastructure. Journal of Information Security Research, 15(1), 45–62.

Alghamdi, A. (2022). Quantum cryptography and digital evidence integrity: A forensic readiness perspective. International Journal of Cybersecurity Intelligence, 7(2), 87–101.

Baggili, I., Mislan, R., & Rogers, M. K. (2007). Mobile phone forensics: Post-mortem tools and procedures. Journal of Digital Forensics, Security and Law, 2(2), 5–14.

Casey, E. (2010). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

Gradillas, R. R., & Thomas, R. (2023). Distinguishing digitization and

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

digitalization: A systematic review and research agenda. Journal of Product Innovation Management, 40(2), 123–144.

Kass-Hanna, J., et al. (2022). Post-quantum cryptography and emerging markets: A readiness analysis. Cybersecurity Journal, 14(3), 111–129.

Koper, R., Elgersma, M., & de Leeuw, F. (2020). Chain of custody in the cloud: Legal challenges for digital evidence. Digital Investigation, 34, 200934.

Lukas, C., Henriksen, T., & Brandt, M. (2023). Forensic implications of quantum-safe cryptography in law enforcement. Journal of Forensic Informatics, 9(1), 28–41.

Scanlon, M., et al. (2023). AI and quantum forensics: A review of converging technologies. ACM Computing Surveys, 55(12), Article 245.

Sharma, R., Mehta, T., & Kumar, V. (2025). Digital forensics in a post-quantum era: Emerging challenges and frameworks. Journal of Cybercrime Studies, 13(2), 201–219.

Silalahi, M., Pratama, D., & Lestari, I. (2023). LLMs for timeline reconstruction in digital forensics. International Journal of Digital Crime and Forensics, 15(1), 55–71.

Wickramasekara, K., Scanlon, M., & Silalahi, M. (2025). Evaluating large language models in digital forensic investigations. Digital Investigation, 44, 301292.

Baggili, I., Mislan, R., & Rogers, M. K. (2007). Mobile phone forensics: Post-mortem tools and procedures. Journal of Digital Forensics, Security and Law, 2(2), 5–14.

Casey, E. (2010). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

Gradillas, R. R., & Thomas, R. (2023). Distinguishing digitization and digitalization: A systematic review and research agenda. Journal of Product Innovation Management, 40(2), 123–144.

Lukas, C., Henriksen, T., & Brandt, M. (2023). Forensic implications of quantum-safe cryptography in law enforcement. Journal of Forensic Informatics, 9(1), 28–41.

Scanlon, M., et al. (2023). AI and quantum forensics: A review of converging technologies. ACM Computing Surveys, 55(12), Article 245.

Sharma, R., Mehta, T., & Kumar, V. (2025). Digital forensics in a post-quantum era: Emerging challenges and frameworks. Journal of Cybercrime Studies, 13(2), 201–219.

Silalahi, M., Pratama, D., & Lestari, I.

ONLINE ISSN
3006-9726
PRINT ISSN
3006-9718
VOLUME . 4 ISSUE . 2 (2025)

(2023). LLMs for timeline reconstruction in digital forensics. International Journal of Digital Crime and Forensics, 15(1), 55–71.

Abushgra, M. (2023). Quantum computing impact on cybersecurity infrastructure. Journal of Information Security Research, 15(1), 45–62.

Alghamdi, A. (2022). Quantum cryptography and digital evidence integrity: A forensic readiness perspective. International Journal of Cybersecurity Intelligence, 7(2), 87–101.

Baggili, I., Mislan, R., & Rogers, M. K. (2007). Mobile phone forensics: Post-mortem tools and procedures. Journal of Digital Forensics, Security and Law, 2(2), 5–14.

Casey, E. (2010). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

Kass-Hanna, J., et al. (2022). Post-quantum cryptography and emerging markets: A readiness analysis. Cybersecurity Journal, 14(3), 111–129.

Koper, R., Elgersma, M., & de Leeuw, F. (2020). Chain of custody in the cloud: Legal challenges for digital evidence. Digital Investigation, 34, 200934.

Lukas, C., Henriksen, T., & Brandt, M. (2023). Forensic implications of quantum-safe cryptography in law enforcement. Journal of Forensic Informatics, 9(1), 28–41.

Scanlon, M., et al. (2023). AI and quantum forensics: A review of converging technologies. ACM Computing Surveys, 55(12), Article 245.

Sharma, R., Mehta, T., & Kumar, V. (2025). Digital forensics in a post-quantum era: Emerging challenges and frameworks. Journal of Cybercrime Studies, 13(2), 201–219.

Silalahi, M., Pratama, D., & Lestari, I. (2023). LLMs for timeline reconstruction in digital forensics. International Journal of Digital Crime and Forensics, 15(1), 55–71.

Wickramasekara, K., Scanlon, M., & Silalahi, M. (2025). Evaluating large language models in digital forensic investigations. Digital Investigation, 44, 301292.