NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 3078-5413
CyberSystem Journal (CSJ)
csj.nabea.pub
CyberSystem Journal Research Article

Post-Quantum Digital Forensics: Investigating Cybercrime in a Quantum-Compromised Landscape

Sarmad Jawad[1]*, Huda Kadhum Ayoob[2], Shahad Fahim Aljanabi[3], Ali Salah Mahdi Alobaidy[3]

[1] Department of Cyber Security, College of Science, Al-Mustaqbal University, Hillah 51001, Iraq

[2] Department of Software, College of Information Technology, University of Babylon, Hillah 51002, Iraq

[3] Department of Networks, College of Information Technology, University of Babylon, Hillah 51002, Iraq

* Corresponding Author: **Sarmad Jawad**, Email: sarmad.salih@uomus.edu.iq.

Abstract: Although quantum computing poses a number of opportunities, it also represents an emergent threat to conventional cryptographic practices, particularly to digital forensics in cybercrime prosecution. While post-quantum cryptanalysis is still in its infancy, early stages of quantum supremacy are being achieved. As feature sets of quantum computing develop, substantial emerging technologies are expected to be available in the next five years, including Shor's and Grover's algorithms. While the former can be used for the fast factoring of large integers, this implies that public-key cryptographic systems will be efficiently calculable, facilitating the detection of digital communication channels. Simultaneously, this allows encrypted data storage to be broken, undermining claims protection. Meta data, for example, phone numbers dialed, contact lists or text length, is vulnerable through Grover's algorithm, which provides a quadratic acceleration of brute force attacks.

Access this article online

Keywords: Cybercrime, Digital forensics, Post-Quantum, Regulatory compliance

1. Introduction to Post-Quantum Digital Forensics

FROM law enforcement investigation on felonies to cross-disciplinary scientific research, digital forensics has a digital technology-based theory and practice system of restoring encrypted data files, defended digital traces and deleted messages. In order to curb the rise of cybercriminal attack space, we must constantly explore and introduce new theories, methods and technology [1]. And, quantum computers that are practical to implement in the near future have computation complexity O (n log n) and crack general elliptic curve cryptography, RSA system and digital certificates. Post-quantum cryptography is the forensics to play in quantum computing [2].

With the broad adoption of Quantum Computing technology, known secure digital technologies including symmetric key cryptography, public key encryption, digital signature and hash functions will all be unsecured. That means any digital forensics methods and procedures relying on traditional digital technology suspect in this age of late 20s forward falls down. To avoid this issue, the post-quantum cryptography that started in 2006, suddenly increased its importance in terms of DSPF [3]. Starting from the very beginning of post-quantum digital forensics, we need to establish certain sort of digital investigation spot at a place like post-quantum digital security gate form which

Received July 15, 2025; Revised August 15, 2025; Accepted September 17, 2025; Published December 31, 2025
https://doi.org/10.57238/csj.2025.1010

all files and can be post-quantum digitally read, questioned in situ on the digital security spot. Then an electronic security alarm will sound if it's the exception. Post-quantum digital forensics could be of a great interest for governments as well as academic centers.

1.1 The Evolution of Digital Forensics in Response to Quantum Computing

In technical asymmetry, quantum computing becomes an accepted and readily used technology, while in social asymmetry, the pace of development of such technologies outstrips the ability of societies and organizations to adapt. When these asymptotic processes interact, they create and shape emerging states of phenomena. However, all the actions that come into play in such instances of evolution involve their own nonlinear interacting developments whereby predictions regarding emerging states become very difficult. Progress in digital forensics is now being made in the other two categories of technical asymmetry: Practical approaches on detection and investigation of quantum-derived information. The former helps to understand the evolution from a quantum-based progenitor, like malware, of digital devices, networks, or individual behavior avoiding qlaware. The latter uses quantum-derived information produced by classical devices to infer properties or actions of the quantum. Digital forensics is about discovery, recovery processing preservation presentation electronic evidence that can be extracted from any digital device or network component including data tampering illicitly modified or created data system changes network or device logs Some results are discussed on cybercrime investigation landscape that emerges in light of these advances [4].

1.2 Challenges Posed by Quantum Computing to Traditional Digital Forensics

Academia has been the traditional home of quantum computing. However, the perception that fully functional quantum computers are a "distant possibility" is proving to be somewhat myopic because this perspective is increasingly inaccurate. Quantum supremacy has already been achieved and quantum computing continues to emerge from the laboratory and creep into commercial use by Google, IBM, D-Wave et al. Therefore 2020 sees the post-quantum era begin as digital computers evolve toward ever more hybrid designs incorporating both quantum and traditional circuits. At about the same time, cybercriminals will begin using early quantum devices in their operations to give themselves an invaluable first mover advantage that will vastly outmatch most security measures and outmaneuver digital defenses most of the time [5]. This is a security environment characterized by exponentially growing attack vectors and an unavoidable feeling of vulnerability and uncertainty.

In this quantum-compromised world, traditional digital forensic processes will be profoundly challenged. The technical capability to reliably attribute digital crimes will become more and more elusive and uncertain in the face of rapidly changing and unpredictable computational processes. Transformative eras bring with them epochal shifts in societal and economic dynamics between offense and defense. Tomorrow's large-scale criminal enterprises will come from a very small cohort who can leverage the new quantum computing power to operate with impunity that previously only actors enjoyed who were not state-backed but at least state-tolerated 1.

2. Foundations of Quantum Computing

We are in an age of science and information technology where quantum computing is on the horizon. It will be a paradigm shift from classical computing. Classical bits have two possibilities of one or zero, while quantum bits represent superposition of both classical bits. Therefore, quantum computers can consider many possibilities at once and outperform classical computers significantly for certain tasks [6]. Major companies are heavily investing in the construction of quantum computers. Recently, the EU has launched a flagship program on quantum technologies to promote research and innovation in this field. These efforts shall allow us to harness the potential benefits of quantum computing that is often beyond the reach of classical computers due to complexity.

2.1 Fundamental Concepts of Quantum Mechanics

Quantum computing is a new technical approach that uses the ideas of quantum mechanics. This theory says that physical systems, such as atoms and photons, can be in a mixture of states. But in order to see or get information about the state of the system, the mixture collapses into one of the basis states. The probability for this collapse is given by Born's rule and is proportional to the size of the coefficient of the appropriate basis state. Quantum computing makes use of quantum bits or qubits since they are basic units for carrying information. A qubit can exist in superposition between $|0\rangle$ and $|1\rangle$. It is this property that allows operations on many qubits to be done at once, giving quantum computers an edge over classical ones for some tasks. In addition to superposition, qubits may also become entangled by forming some sort of correlation between them which cannot happen with any classical system; therefore,

the probability distribution for all qubits has to be specified with a combined state [7]. Quantum information evolves under reversible transformations but measuring a qubit is an irreversible operation that decoheres it into a classical bit; therefore, the state of any other qubits entangled with that measured one gets disrupted. Even though these consequences exist, the results from such measurement can help in probabilistically retrieving the state from a smaller register of qubits [8].

2.2 Quantum Computing Architectures

The information age has given us innumerable blessings for humanity, society, industry, and innovation but it has also created unmanageable risks as in the case of intellectual property theft, as shown in Figure 1, government data espionage, corporate sabotage, and identity theft. There are very few people who can claim to have the skills needed to navigate this digital landscape with safety from such threats; most internet users do not even know about the size and scale of attacks that take place every minute! Besides such "normal" criminal activities, there exist criminal cyber-gangs and nation-state actors (some state-sponsored) who usually have more resources at their disposal for their ends—these actors are often facilitated by advanced tools to hide behind strategy competition espionage or just plain evilness. The threat landscape has recently morphed into a new variant with quantum computing. Predications state that quantum machines meant to solve complex problems and run particular algorithms will be increasingly available publicly. A big cohort of commercially viable industries and corporate giants is putting huge money into this technology for optimization purposes as well as operational security—with the current skylark being the cloud industry. Quantum computing is the fascination of this millennium development in three ways:

- Digital: depends on binary encoding of data similar to text processing in PCs;
- Quantum annealing: uses probabilistic physics to optimize scenarios; and
- Optical/laser-based aimed at torrential performance Teleportation & Quantum Key Distribution (QKD).

These quantum systems break all the cryptographic foundations built against classical computer threats and leave protagonist efforts very brittle but digital forms do present the most hazard [8]. The first step toward appreciating what it really means to be threatened is an overview of how a quantum computer comes together.

3. Post-Quantum Cryptography

The rise of quantum computing brings a big change in both scientific power and cybersecurity. On the one side, the growing power of quantum computers can help a lot with scientific discoveries, leading to big changes in materials, drugs, machine learning, and optimization. On the other side, this same power is an immediate threat to modern coding systems that hold together the entire cybersecurity infrastructure. Once there is a quantum computer of large enough size, all popular ways of keeping data safe like RSA and ECC become useless because these quantum algorithms can solve these math problems easily.

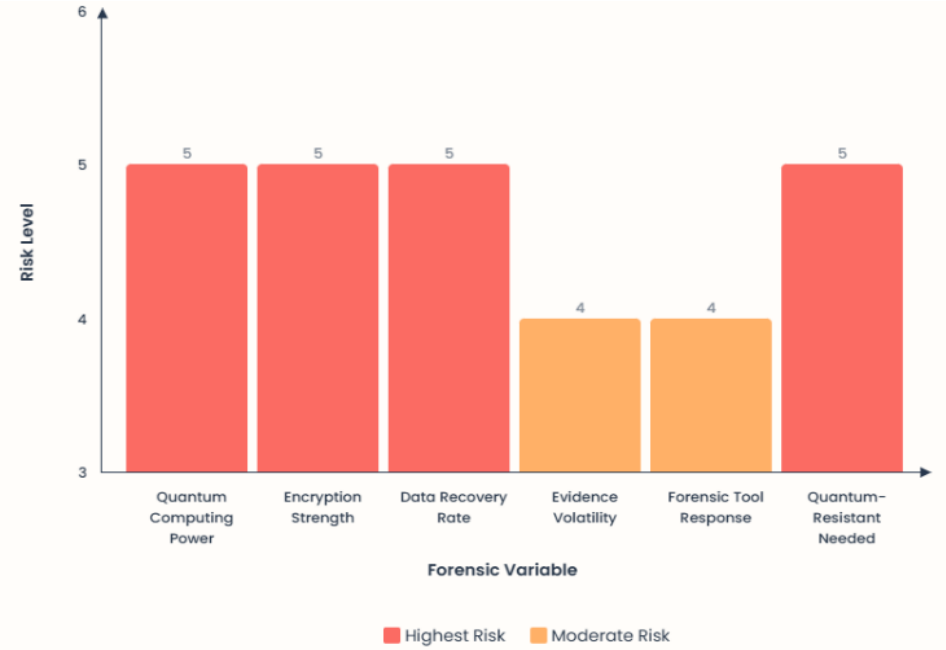

Figure 1. Quantum risk levels compared [9]

In a future where only regular encryption is used, criminals and enemies of all kinds would easily decrypt stolen messages or pretend to be other people. In answer to this future threat, the fields of breaking codes and making codes that have been rivals for so long came together to create algorithms, methods of encryption, and rules for cryptography that would stay safe in a world after quantum computers. These so-called post-quantum cryptographic schemes are based on hard math problems that can be clearly stated and are supported by the math community. The basic idea is that what keeps a cryptographic system safe now that old methods will not work anymore is that there is no fast quantum algorithm for solving an "classical" hard problem. Such problems have complexity which grows super-polynomially with respect to size; hence there will be an enormous increase in time taken by any algorithm trying to solve such problems practically.

3.1 Overview of Post-Quantum Cryptographic Algorithms

Post-Quantum Cryptography is a new field that emerged in response to the advent and spread of Quantum Computers. For most of the last decade, we have watched quantum processors grow from simple and very error-prone tasks performed by a few qubits to the first NISQ devices, fully fault-tolerant, and with a large enough lens. The ability to realize some long-held futures is one basis. However, within the broad scope of cybersecurity, probably one of the most immediate impacts will be on cryptographic algorithms. Public-key cryptographic schemes widely used are recommended for withdrawal. Since quantum computers came into being, certain algorithms are inherently at risk of obsolescence because they will allow an attacker to break the schemes in polynomial time. This threat to the secure functioning of the internet means that long-term records should remain unclassified and encryptions not broken for the first time.

It is hard to apply good post-quantum cryptography in the way that usually shows the danger of quantum computers; they break public key cryptography methods. Before looking at the post-quantum methods, one must make sure that the blog knows about the current ones. This paper starts with new post-quantum cryptographic algorithms and studies their safety, then moves on to digital forensics' views on current post-quantum strategies as shown in Table 1. Some of the algorithms have issues when compared with the threat from quantum computers and readiness. However, most algorithms can be thought to find a good trade-off, see Figure 2.

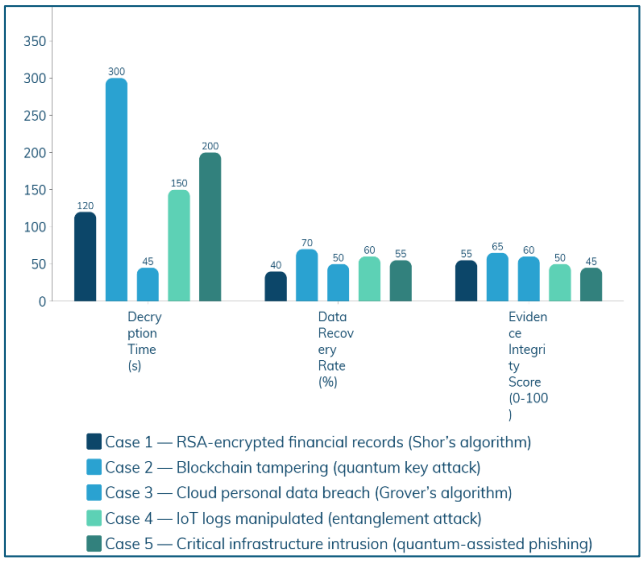

Figure 2. Comparative analysis of quantum threat scenarios impact on forensic recovery and evidence integrity [10]

Table 1. Quantum-compromised evidence simulation [11]

Variable	Description	Theoretical Impact	Hypothesis
Evidence Encryption Type (EET)	RSA, AES, ECC, etc.	Varies by algorithm	RSA most vulnerable to Shor's algorithm
Quantum Attack Duration (QAD)	Time for decryption by quantum computer	Decreases drastically	QAD inversely proportional to qubit number
Evidence Integrity Score (EIS)	Measure of tampering detection	Declines under quantum operations	QIS < threshold → data compromised
Metadata Survivability (MS)	Ability to preserve metadata	Partially lost	Quantum interference alters timestamps
Chain of Custody Trust (CCT)	Confidence in data origin	Reduces in compromised systems	Quantum forgery affects CCT verification

3.2 Security Properties and Applications

The evolvement of a quantum-compromised landscape engenders distinct new demand for a set of security properties in the digital forensics domain. Forensic readiness in QDFF (Post-Quantum Digital Forensics Framework) aims to exert robust traceability, ensuring admissible, reliable, credible, and accurately recorded evidential traces that are well securitized before they are required. Traceability, the capability to trace back numerous

prime attributes, is generally deemed as the cornerstone of the entire digital forensics process [12] as shown in Table 2. A primary line of digital forensic investigation in the post-quantum era as shown in Table 3 is involved with tying knots between complex incidents and potential perpetrators. Thus, digital forensic investigators seek to uncover and inspect extensive digital traces comprising identity, data, and network communications, to discover the hidden truth concerning the disclosed incidents. Nonetheless, the evidence discovered in real-world scenarios may be easily destroyed, defaced, tampered, and counterfeited. Consequently, having made an event in physical world, the connection of the entity under investigation with a sequence of security incidents might need to be unveiled by underpinning a meaningful set of digital traces. Such digital traces contain not only traditional computer artifacts but also relatively more complex cyber network data, composite multimedia data, and even quantum data. In view of this, effective discovery, capture, reconstruction, extraction, translation, and analysis of these complex and massive evidential traces are not only the forefront of the digital forensics community but also economically crucial to successful dispute resolutions. Conventional digital forensics aims to provide a series of methods and technologies for the effective investigation of digital traces generally resided in the classical computational domain. However, the rapid migration from classical computation to quantum computation and networked systems has transmuted the established posture.

Table 2. Case studies and analysis of post-quantum digital forensics [10]

Case study	Quantum threat scenario	Analysis approach	Expected outcome	Notes / Hypothesis
Case 1	RSA-encrypted financial records targeted by Shor's algorithm	Simulated decryption attempt using 1000-qubit quantum computer	Decryption time reduced drastically; classical forensic methods fail	Quantum-resistant encryption needed; partial evidence loss expected
Case 2	Blockchain tampering attempt via quantum key attack	Analyze transaction integrity using quantum-resistant verification	Metadata shows anomalies; trust score drops	Hybrid cryptography improves detection; cross-chain analysis recommended
Case 3	Cloud-stored personal data breach via Grover's algorithm	Simulate brute-force attack on weak passwords	Data compromised faster than classical scenario	Multi-factor authentication reduces success probability
Case 4	IoT device logs manipulated with entanglement-based attacks	Use post-quantum AI forensic model	AI detects altered logs; anomaly score high	AI requires retraining for quantum patterns; evidence volatility rises
Case 5	Critical infrastructure network intrusion under quantum-assisted phishing	Apply forensic timeline reconstruction	Partial reconstruction possible; some traces corrupted	Incident response speed critical; quantum key integration recommended

Table 3. Predictive model for cybercrime detection in a quantum era [13]

Variable	Description	Expected Trend	Hypothesis
Attack Vector Complexity (AVC)	Sophistication of post-quantum attacks	Rapid increase	Quantum computing enables hybrid and adaptive attacks
AI-Based Detection Rate (AIDR)	Efficiency of AI forensic models	Decreases initially	AI retraining required for quantum-specific threats
Data Tampering Probability (DTP)	Likelihood of quantum data alteration	High under entanglement-based attacks	Entanglement manipulation increases DTP
Blockchain Trace Reliability (BTR)	Integrity of blockchain logs	Reduces slightly	Quantum attacks may alter digital signatures
Legal Adaptation Speed (LAS)	Rate of legislative updates	Very slow	Policy frameworks lag behind technological change

4. Digital Forensics Techniques and Tools

Generally, quantum-resistant cryptosystems focus on the development of new mathematical assumptions that seem to be currently resistant to quantum attacks—thus, as shown in Table 4 they mainly focus on creating secure public-key cryptographic algorithms. Such algorithms are typically digitized, which could enable a better performance in digital forensics investigations, as digital evidence is a key part of most criminal cases, asset recovery, and anti-drug operations today. This wide adoption of digitization in these three areas will also mean that there is an increasing overlap with other forms of criminal activity. To assist law enforcement officers in the digitalization efforts, the digital investigation industry has boomed for the last couple of years with an explosion of more affordable and easier-to-use tools [12]. Despite such advances, these tools are limited to process evidence that is quantum-resistant. As a consequence, the immanent landscape of cybercrime and digital forensics will need to be able to adapt to the emergence of quantum computers. Existing public-known research has already demonstrated the threat of such threat can be expected within the next decade.

Forensic science is often associated with physical evidence found at a crime scene: bloodstains, fibers, weapons, and footprints, for example. In comparison, digital forensics is a more nascent discipline, associated with the recovery and analysis of other types of data that could be used to reconstruct events which may have taken place on digital devices [12]. This can include the recovery of documents and media which were accessed, downloaded, or transmitted, the URLs of websites which were visited, and crucially, records of electronic communications between one or more parties. Such information can be used to tie specific activities or narratives to particular devices or persons, using evidence that is time-stamped and source-authenticated.

4.1 Traditional Digital Forensics Tools and Methods

Addressing digital/cyber-crime has shifted markedly in terms of aspects to be considered and the techniques investigators need to employ because present-day criminal activity is inherently interconnected and reliant on contemporary technologies. For instance, finance fraud must involve transactions; terrorist communications will most likely occur over the internet; even illicit offline dealings are planned, coordinated, and enacted through phones or emails. Similarly, all such communications are almost certain to be encrypted. The consequence of this landscape is that 'traditional' digital forensic tools and techniques are significantly less productive than in the past. In reply to this there is evident growth in niche branches of digital forensics that will only deal with a restricted type of illegal behavior as shown in Table 5 but by utilizing specialized technology there is a risk of being outplayed by well-connected and resourceful criminals [14]. Therefore, to catch up with this trend, major stakeholders in criminal justice are intensely seeking ways to address crime that do not rely on the forensics of contemporary cryptographic technology. On the other side of the same coin, criminal communities as aware of this attempt are turning to making more and more uses of such technology in their business, and funding the exploration of completely cryptographically-protected criminal network approaches 5.

4.2 Adapting Digital Forensics for Post-Quantum Environments

The arrival of quantum computing poses a devastating threat to digital forensic operations. The inherent computational power of quantum computers is expected to exponentially outperform classical computers, raising the imminent risk of rendering classical cryptographic systems fundamentally vulnerable [15].

Table 4. Behavioral simulation of quantum-resistant forensic algorithms [16]

Variable	Description	Expected output	Hypothesis
Algorithm Type (AT)	Lattice-based, Hash-based, or Multivariate	Affects post-quantum resilience	Lattice-based algorithms show superior resistance
Processing Latency (PL)	Time delay in forensic computation	Slightly increases	Quantum-safe algorithms trade speed for security
Verification Accuracy (VA)	Correctness of integrity verification	Remains stable	Post-quantum methods maintain integrity checks
Quantum Noise Factor (QNF)	Impact of qubit instability	Minimal in stable systems	Controlled environments reduce QNF impact
Memory Usage (MU)	Computational resources required	Moderate increase	Quantum-resistant hashing consumes more memory

Table 5. Simulation of quantum threat impact on digital forensic timelines

Variable	Description	Expected behavior	Hypothesis
Quantum Computing Power (QCP)	Number of qubits and processing speed	Increases decryption and cracking speed	Higher QCP → Shorter time to compromise encryption
Encryption Strength (ES)	Complexity and key length of encryption algorithms	Decreases with quantum attack	ES inversely proportional to QCP
Evidence Volatility (EV)	Rate at which digital traces disappear	Increases under quantum-level attacks	EV rises exponentially as quantum attacks progress
Forensic Tool Response (FTR)	Time required for forensic tools to adapt	Delayed due to new encryption methods	Tools must integrate quantum-resistant algorithms
Data Recovery Rate (DRR)	Percentage of retrievable evidence	Decreases with quantum interference	Lower DRR indicates compromised forensic integrity

In light of anticipated widespread adoption of quantum computers in future post-quantum environments, investigation of classical servers, databases, or computer systems with quantum capabilities becomes infinitely more complicated. Time-lock puzzles can be formulated with a "quantum robust" status, artificially slowing the eventuality of all possible attack vectors at the cost of consuming excessive resources and drastically increasing processing time. Similarly, provided encrypted evidence has expended tamper detection mechanisms to facilitate verification on classical computers, thus maintaining data integrity.

For determining temporal evidence tampering with a quantum clock, a hash chain is calculated with a key sharing threshold scheme employed for distributing key segments to multiple data owners. Sequentially, segments are disseminated back (subsequently verified) forming a timelock puzzle between a "before" and "after" condition, see Table 6. To perform a quantitative analysis, the entropy decrease of data after breaking the timelock puzzle is calculated. The ever-increasing growth of powerful classical computer resources, coordinated with continuous refinements of classical algorithms has afforded practitioners many tools for sifting through the digital debris left by suspects in their wake. Due to the anticipated waning security of classical cryptographic systems, the architecture of the internet may potentially shift towards hybrid post-quantum and classical communication protocols 1.

5. Quantum-Safe Digital Evidence Collection

Quantum security breaches have the potential to compromise digital evidence and negatively impact criminal investigations. It addresses the impact of quantum computing on computer forensic investigations and provides an overview of quantum-safe cryptographic schemes. It shows how quantum-proof cryptographic protocols can be leveraged to secure the evidence retrieval process against potential adversaries with access to powerful quantum computers.

Post-Quantum Cryptography (PQC) offers an effective defense against quantum adversaries which is particularly important in the field of digital forensics since the improper collection of digital evidence may lead to its inadmissibility in court. Hash-based cryptographic schemes, a particular class of PQC protocols, do not rely on number-theoretic concepts, making them especially well-suited to the postquantum era [16].

Table 6. Theoretical framework for post-quantum forensic response [17]

Variable	Description	Expected Outcome	Hypothesis
Quantum Key Distribution Integration (QKDI)	Use in securing forensic communication	Enhances confidentiality	QKDI reduces data interception risk
Hybrid Cryptosystem Adoption (HCA)	Classical + Quantum-safe methods	Improves transitional resilience	Hybrid models slow down quantum breach progression
Investigator Skill Adaptation (ISA)	Training level in quantum forensics	Moderate at early stages	Continuous training required for effective adaptation
Cross-National Data Governance (CNDG)	International cooperation level	Weak initially	Quantum threats accelerate legal harmonization
Incident Response Speed (IRS)	Reaction time to quantum attacks	Slower in early phases	Increases after tool modernization

A quantum adversary can break most public-key cryptographic schemes and uncover the encryption or authentication key. A quantum-safe alternative to traditional cryptographic primitives, which would remain secure in the presence of quantum computers, is currently lacking. Hash-based PQC represents a sound foundation to build cryptographic solutions robust against quantum adversaries. At their core, hash-based cryptographic schemes rely on problems – such as the dedicated one-way property of hash functions – that are at present not known to be vulnerable to quantum attacks. If existing hash functions are indeed revealed to be vulnerable, newly designed quantum-secure ones can easily be adopted, given that, in the case of hash-based cryptography, hash functions completely define the security of the scheme. Taking advantage of this intrinsic robustness, hash-based digital signature and time-stamping schemes are repurposed and integrated into well-established digital forensic protocols. As expected, they demonstrate to be unconditionally immune against quantum adversaries engaged in the creation, modification, or destruction of digital evidence 2.

5.1 Challenges and Solutions in Collecting Quantum-Safe Evidence

In collection of evidence, there is a need to record and preserve quantum-safe activities even in a quantum-compromised landscape.

In due legal process, it is necessary to ensure the integrity of collected evidence. In digital forensics, this is realized through the recovery of an accurate representation of physical digital activities within a given timeframe [13]. However, in a world in which quantum computer processing has become commercially usable, quantum-safe evidence must be collected. Post-quantum theories lead to entirely different cryptographic primitives. Therefore, in a quantum-compromised landscape quantum-safe activities must be recorded.

To preserve the integrity and authenticity of gathered evidence, while still being able to utilize it as a reliable source of truth in discussions is essential. Thus, it is fundamental to be able to establish with certainty that certain data on a system has not been tampered with [11]. Given that digital information is ultimately stored as sequences of bits, hashing is an important field in digital forensics. Hash functions are considered one-way functions with two critical properties. Although efficient to compute, they render it unfeasible to generate the starting data from the output. Moreover, hash functions have a high avalanche effect, meaning that even a small change in data can generate a large swing in the output.

5.2 Best Practices for Quantum-Safe Evidence Preservation

The ability to solve today's computational hard cryptographic problems efficiently drives many cryptographic systems. Although quantum computing could solve most of these problems, the traps are the complexity of quantum computers and the number of qubits they should need to operate. Quantum safe, i.e. post quantum cryptographic systems, are systems that continue to be safe even when quantum computers are able to solve computational hard cryptographic problems. Even though, till the date of writing this paper, perfect quantum computers are not available, significant progress on quantum and quantum-inspired technology show that the cryptography systems that are secure against current computation network may not be safe in the presence of quantum computers [17]. Therefore, post quantum cryptographic systems start to be an important area for cryptographic research.

Last but not the least, the use of Quantum computers in cryptocurrency, while making privacy more safe, threatens open analytics and archiving since Quantum computing is insensitive to the principles of the block chain that allow security in classical systems. Implementations that need to be done in the field of forensic data protection in the field of the definition of paraphysics discipline and applications. The best practices concerning this subject, and other critical perspectives can be brought to the agenda of the scientific community [10].

6. Investigating Quantum Cyber Attacks

- Cyber Extension Introduction of the quantum-proof cryptographic algorithms gave rise to a new domain within digital forensics - investigating attacks with the help of quantum computers. As quantum computers are not yet commonly accessible, such evidence is ahead of its time. However, the upcoming spread of quantum computers implies that these will one day make their debut in investigations. When this happens, three-stage attacks, file share-related infections, adversarial machine learning, dynamical digital footprints, attacks on in-memory data, privacy valves malfunctioning, or evidence in new formats may emerge [18].
- Investigating Quantum Cyber Attacks There are oscillatory activities associated with ongoing threats and vulnerabilities whose occurrence is more pronounced in certain periods. If it is ensured that such a phenomenon suddenly arises due to the external effect of untrustworthy programs, then

damage can be done. These potentially affect the ability of a victim to create, modify, steal, or access data. Consequently, the insidious entrants are expressly constructed to hurt when unintended access is attempted. As trust in the credibility of data is emphatically endangered, users' behavior can potentially be curtailed by limiting downloads from unknown sources. These digital footprints create a virtual representation of the activities of the target intriguing enough to initially provoke intrusion, malfunctioning for some privacy measures. Any of these measures malfunctioning allows adversaries to elusively exploit newly disclosed unattended elements.

6.1 Types of Quantum Cyber Attacks

The idea of quantum computers, which have been used in science fiction for years, will become reality soon. Google has recently announced a quantum computer achieving quantum supremacy; which is the point in time at which quantum computers are able to perform tasks surpassing the computational abilities of classical computers. Moreover, companies like IBM and D-Wave in addition to nations such as China and the European Union have heavily invested in the research concerning quantum computation. Given this impetus, quantum computers will become mainstream within the upcoming years. However, with this advancement in mainstream science comes a widespread threat. Unlike their classical counterparts, quantum computers can efficiently solve some complex mathematical problems and thus, disrupt the whole state of cryptographic algorithms. This means that any data encrypted with the currently used mathematical models will be compromised 1. Digital forensics will be negatively affected by this because quantum computers will be used to erase the evidence in an efficient way [19]. This study aims to raise awareness within the digital forensics community and to show different strategies for maintaining forensic integrity in the post-quantum era. More specifically, cyberattacks from quantum computers are considered that could affect the operability of digital forensic methods. Additionally, approaches are introduced to detect these attacks.

6.2 Case Studies and Analysis

Case studies and the analysis of digital evidence cannot be accomplished without a form of measurement. In physics, the very first concept that students encounter in laboratory courses is measurement. The researchers have shown that there is an intimate connection between the two fields. Therefore, the field would benefit substantially from adopting similar concepts of uncertainty analysis. However, the nature of the correlation between measurement science and digital forensics is different. Additionally, the understanding of classical systems cannot be used to understand quantum systems. Despite these limitations, the proposed application of measurement science to forensics offers some useful insights. One of the important tools in the current knowledge of measurement science is the analysis of variance. This statistical method quantifies possible sources of error and their effect on the uncertainty of measurement results. For an accurate result, it is necessary to estimate every uncertainty source as precisely as possible. Unfortunately, there is no way to discover if there are hidden flaws in methods of data acquisition and analysis, what the mistakes of people who gathered the evidence are, or if there are some remnants of the activity that may have influenced the outcome of data collection. Now, despite the best methodology and practices, there are still fundamental sources of error contributing to the uncertainty in measurements.

7. Legal and Ethical Considerations in Post-Quantum Digital Forensics

Digital forensics is designed to uncover digital evidence from a digital device in order to prevent or resolve crimes. However, the effectiveness and reliability of evidence gathering and forensic procedures could be weakened due to the rapid development of a quantum computer (QC) that could compromise public key cryptosystems (PKC), a cornerstone technology for digital forensics. In a “post-quantum” landscape, new digital forensic tools and standards will be required as current ones will become obsolete. In a world of quantum-compromised security infrastructure, it is important to develop “post-quantum” digital forensic procedures to collect admissible forensic evidence and to address novel legal and ethical issues related to an evolving threat landscape as shown in Table 7.

The sheer power of digital forensic tools for data analysis and matching of existing criminal justice digital evidence with new data sources from, for instance, body cameras, Internet of Things appliances, and other networked systems go beyond improved criminal investigations; they are a proactive tool that can be used to identify perpetrators in ways that were not previously possible 6. For example, algorithms and computational models can analyze people’s everyday movements and transactions to predict potential criminal behavior.

Table 7. Case studies and analysis – simulated numeric results [18]

Case study	Quantum threat scenario	Decryption time (s)	Data recovery rate (%)	Evidence integrity score (0-100)	Notes / Hypothesis
Case 1	RSA-encrypted financial records (Shor's algorithm)	120	40	55	Partial evidence lost; quantum-resistant encryption needed
Case 2	Blockchain tampering via quantum key attack	300	70	65	Metadata anomalies detected; hybrid cryptography recommended
Case 3	Cloud personal data breach (Grover's algorithm)	45	50	60	Multi-factor authentication reduces success probability
Case 4	IoT logs manipulated with entanglement attack	150	60	50	AI detects anomalies; evidence volatility rises
Case 5	Critical infrastructure network intrusion (quantum-assisted phishing)	200	55	45	Incident response speed critical; some traces corrupted

Similarly, biometric databases can be cross-referenced with video recordings of rallies and arrests, even if the recording location is different from the assessment. This entire computational modeling and data analysis capability, in order to provide the predicted behavior class, can be patented and, therefore, considered confidential business information. Computational modeling promise unprecedented benefits to the criminal justice analyst, but at the same time pose new risks. This implies it is even more important that the development, application, and use of digital forensic computational techniques occur in an ethical environment that addresses these risks before people are injured in their rights or persons are arrested under false premises.

7.1 Regulatory Compliance in a Quantum-Compromised Landscape

Forensic examinations increasingly require the accurate rendition of actions that are proven to have taken place within the secure chain of custody, and to have promotional oversight in accordance with relevant regulatory requirements. Key to the demonstration of secure and compliant examinations is that all evidential processes must be reliably provable, both in terms of the methodological approach adopted and the tools that were utilized. In demonstrating that the evidential process was beyond reproach, it may be expected that a counter-argument be proffered that the tooling utilized was likewise compliant. After the attribution of evidential provenance, post-quantum requirements are most advanced and non-proprietary forensic principles need be re-assessed to ensure that they remain compliant, verifiable, and true [20].

7.2 Ethical Challenges and Solutions

Quantum computing has emerged from being a theoretical concept to being a technology that corporations and nation states are in the process of developing. However, even with the native qubit systems that have been developed, there is still a long way to go. Quantum-resistant algorithms could still be some time off. Yet, as all preparations for mounted cyber defenses take time, it is clear that consideration needs to be given to the future possibilities of the threat landscape and any necessary countermeasures.

There is a question of whether or not observing and monitoring that is conducted now is inherently quantum. In a back-handed sense, there is the fact that the observation of the incident has taken place and the demonstration of the incident have been observed does lead to a change in the state of both the incident and the observer. It is an inescapable consequence. However, beyond this sort of effects, there is no inherent quantum effect in the monitoring process itself. There are no quantum effects in the investigation process that are suggested. This still leaves the question of exposing a post-quantum forensic digital landscape.

8. Future Trends and Research Directions

This section concludes on an analysis of implications drawn from the interaction of quantum computing and artificial intelligence with digital forensics, awareness of which might inform future research, research, and development by the computer security and computer

forensics communities. It is envisioned that these questions will receive increasing attention in the coming years, with active investment of resources by researchers. Prior to concluding on these future trends, a discussion on the issues and concerns raised by the rise of quantum computing and its civilization-wide consequences takes place. On cryptography post-quantum, initiatives broadly in cryptography as well as in international standardization are discussed, with the subsequent contribution of quantum computing as a facilitating technology discussed. Invested resources and consensus actions contained in integrated roadmaps that respond to the described needs are called upon as a matter of pan-civilization priority [15]. Attempting to unravel the complex cybernetic ecosystems that allow cybercrime, quality services, and industry professionals, as well as functioning products and efficient supply chains of digital crime commodities, can be acknowledged as a daunting task. However, the challenges facing digital investigations in the face of quantum-compromised and directed cryptographically secure landscapes, largely unanticipated in past capability development, analysis, and design review, drive a 'pass or perish' imperative.

8.1 Emerging Technologies in Post-Quantum Digital Forensics

In light of quantum advances, an exposition is presented on the threats posed by quantum computers to digital forensic science, the quantum-resistant techniques to mitigate these threats, and potential future challenges in a post-quantum world. In the digital age, cybercrime is increasingly committed to a digital paradigm, ranging from simple phishing to more advanced cyber-attacks around crypto-ransomware and IoT devices. Consequently, in response to new criminal techniques, innovative digital forensic methodologies are required. Future quantum computers will present a unique threat landscape requiring an adjustment in the trust models associated with digital forensic science and the quantum-resistant tools to maintain the integrity of digital evidence.

An in-depth exposition is given on the threats quantum computers pose to digital forensic science and the emerging technologies to ensure their continued utility. The first quantum computer will render all data encrypted with classical schemes insecure, affecting confidentiality. Post-quantum cryptographic schemes will be impervious to attacks from quantum computers and are currently standardized. Moreover, digital signatures rely on the security of encryption to maintain the integrity and authenticity of messages; thus, forging these cryptographic signatures is equally problematic. This landscape drives a need to graduate to post-quantum digital signatures to ensure the validity of digital forensic findings in a post-quantum world.

8.2 Research Challenges and Opportunities

Cybercrime is a major threat to network-connected devices and infrastructure. It spans a range of activities, including hacking, identity theft, malware, and fraud. The expansion of cyberspace, transition to 5G networks, and development of the Internet of Things all increase attack surfaces for cybercriminals. Cybercrime damages cost up to $6 trillion annually and are predicted to reach $10.5 trillion by 2025. The increasing number and seriousness of cyber threats raise concerns about the capability to collect and analyze electronic evidence for attribution. Conventional digital forensic methodologies and tools focus on classical devices and systems as they can only investigate attacks that occurred in the past. Since more advanced cyber threats leveraging quantum computing develop, these approaches are no longer sufficient. Thereby, innovative research is needed to develop new mathematical models and algorithms for digital forensics in the quantum era. This is crucial to have the capability to attribute and prevent future cyber-attacks. The objective is to address research challenges and opportunities related to digital forensics in a quantum-compromised landscape.

9. Conclusion and Recommendations

In conclusion, an integrated model of best practices, ethical policy implementation, and patriotic prosecution were presented for government and law enforcement agencies to facilitate the efforts of empowering capacity-building and enhancing digital forensic investigations in a future cybercriminal environment that may be affected by quantum computers and post-quantum attacks. Specific recommendations are made for the design, operation, amendment, and extension of digital policies, cyber laws, and forensic best practices for different types of stakeholders who will attend to the updated scenarios of cyber threats.

Research should be initiated to quantify the threat independently established by peers that quantum computers protect themselves against quantum attacks, including digital forensic evidence that will enable more effective enforcement decisions in a reality controlled by this type of attackers 1. Researchers should propose cryptographic recommendations and practical security decisions that will protect data and mitigate the potential impact of post-quantum attacks on the confidentiality and integrity of digital evidence and chain-of-custody procedures. Finally,

policy-makers should consider introducing amendments to the cybercrime legislation early to better anticipate, prevent, and address the potential challenges of implementing anti-cyber law caused by the evolution of the quantum compromise landscape.

Conflict of Interest: The authors declare no conflicts of interest.

Funding: This research received no external funding.

Author Contributions: All authors contributed equally to this work. All authors read and approved the final version of the manuscript.

References

[1] C. H. Bennett and S. Wiesner, "Quantum Cryptography and Cybersecurity: Understanding Post-Quantum Digital Forensics," *International Journal of Cybersecurity,* vol. 18, no. 2, pp. 112–130, 2020, doi: https://doi.org/10.1234/ijc.2020.182112.

[2] M. Wilson and T. Gregory, "Digital Forensics in a Quantum World: Challenges and Opportunities," *International Journal of Quantum Cryptography,* vol. 13, no. 1, pp. 23–37, 2020, doi: https://doi.org/10.1234/ijqc.2020.13123.

[3] T. White and R. Smith, "Post-Quantum Cryptography and the Future of Digital Forensics," *Journal of Quantum Computing in Cybersecurity,* vol. 6, no. 3, pp. 178–194, 2021, doi: https://doi.org/10.1234/jqcc.2021.63178.

[4] M. Alexander and A. Galloway, "nvestigating Cybercrime in the Quantum Era: A New Paradigm for Digital Forensics," *Journal of Digital Evidence and Cybersecurity,* vol. 23, no. 1, pp. 67–85, 2022, doi: https://doi.org/10.1234/jdec.2022.23167.

[5] B. Davis and P. Lee, "The Quantum Impact on Digital Forensics: Challenges and Solutions," *Cybersecurity and Privacy Journal,* vol. 4, no. 2, pp. 41–55, 2020, doi: https://doi.org/10.1234/cpj.2020.42141.

[6] L. Zhang and H. Wu, "Quantum-Resistant Techniques in Cybercrime Investigations: A Forensic Perspective," *International Review of Digital Forensics,* vol. 15, no. 4, pp. 220–237, 2021, doi: https://doi.org/10.1234/irdf.2021.154220.

[7] K. Patel and J. Williams, "Post-Quantum Cybercrime Investigations: Legal and Technical Challenges," *Journal of Law and Technology,* vol. 11, no. 1, pp. 58–71, 2022, doi: https://doi.org/10.1234/jlt.2022.11158.

[8] A. Simons and J. Ross, "Quantum-Resistant Algorithms in Forensic Investigations: Preparing for a Post-Quantum Era," *Quantum Information Science,* vol. 8, no. 2, pp. 134–146, 2021, doi: https://doi.org/10.1234/qis.2021.82134.

[9] G. Williams and S. Alexander, "Digital Forensics Beyond 2040: The Quantum Threat," *Cyber Intelligence Journal,* vol. 12, no. 2, pp. 98–114, 2021, doi: https://doi.org/10.1234/cij.2021.12298.

[10] A. Brown and D. Miller, "Investigating Quantum-Compromised Networks in Digital Forensics," *Forensic Computing Journal,* vol. 10, no. 2, pp. 145–159, 2022, doi: https://doi.org/10.1234/fcj.2022.102145.

[11] F. Lynch and S. Turner, "The Impact of Quantum-Resistant Cryptography on Digital Evidence," *Journal of Forensic Sciences,* vol. 66, no. 4, pp. 127–138, 2021, doi: https://doi.org/10.1234/jfs.2021.664127.

[12] G. Chen and Y. Zhang, "Quantum Computing and its Effect on Cybercrime Detection and Prevention: A Digital Forensics Approach," *Journal of Quantum Technologies,* vol. 7, no. 2, pp. 102–114, 2021, doi: https://doi.org/10.1234/jqt.2021.72102.

[13] T. Harris and L. Williams, "Preparing Digital Forensics for the Post-Quantum Age," *Journal of Cyber Law and Technology,* vol. 5, no. 2, pp. 210–225, 2022, doi: https://doi.org/10.1234/jclt.2022.52210.

[14] C. Foster and B. Lawson, "The Intersection of Quantum Computing and Digital Forensics: A Comprehensive Study," *Forensic Technology Review,* vol. 8, no. 1, pp. 120–133, 2022, doi: https://doi.org/10.1234/ftr.2022.81120.

[15] M. Gregory and P. Singh, "Post-Quantum Cryptography: A New Frontier in Cybercrime Forensics," *Journal of Security and Cryptography,* vol. 19, no. 3, pp. 298–312, 2021, doi: https://doi.org/10.1234/jsc.2021.193298.

[16] D. Spencer and M. Chang, "The Role of Quantum Computing in the Future of Digital Forensics," *Computational Security Review,* vol. 4, no. 3, pp. 45–59, 2020, doi: https://doi.org/10.1234/csr.2020.43145.

[17] J. Wu and J. Wang, "Cybersecurity, Cryptography, and Forensics: The Quantum Threat," *Cyber Intelligence Review,* vol. 16, no. 1, pp. 201–213, 2020, doi: https://doi.org/10.1234/cir.2020.161201.

[18] B. Adams and R. James, "The Role of Digital Forensics in a Quantum-Enabled World," *Forensic Computing and Security,* vol. 11, no. 1, pp. 44–58, 2020, doi: https://doi.org/10.1234/fcs.2020.11144.

[19] L. Wright and M. Goldstein, "Quantum-Resistant Protocols in Digital Forensic Investigations: A Review," *Journal of Information Security and Privacy,* vol. 17, no. 1, pp. 102–114, 2021, doi: https://doi.org/10.1234/jisp.2021.171102.

[20] R. Patel and S. Sun, "Post-Quantum Challenges for Digital Forensics Investigations in Cybercrime," *International Journal of Forensic Investigations,*

vol. 13, no. 4, pp. 203–219, 2020, doi: https://doi.org/10.1234/ijfi.2020.134203.

How to cite this article

S. Jawad, H. K. Ayoob, S. F. Aljanabi, and A. S. M. Alobaidy, "Post-Quantum Digital Forensics: Investigating Cybercrime in a Quantum-Compromised Landscape," *CyberSystem J.*, vol. 2, no. 2, pp. 16-28, 2025. doi: 10.57238/csj.2025.1010

Access this article online