Master Degree Project

UNIVERSITY OF SKÖVDE

Adapting Digital Forensics Processes for Quantum Computing

Insights from Established Industry Guidelines Supplemented by Qualitative Interviews

Master Degree Project in Informatics with a specialization in Privacy, Information and Cyber Security

Second Cycle 30 credits
Spring term 2024

Student: Tobias Svenblad
Supervisor: Oskar MacGregor
Examiner: Rose-Mharie Åhlfeldt

Abstract

This thesis explores the evolving landscape of digital forensics in the context of quantum computing advancements, which challenge the foundational integrity of digital evidence. The focus is on the globally recognized digital forensic guidelines, NIST SP 800-86 and ISO/IEC 27037:2012, and their capacity to safeguard evidence against the unique capabilities of quantum systems. This thesis identifies vulnerabilities within existing forensic models through a comprehensive document analysis and expert interviews and proposes strategic modifications to enhance their robustness.

Key findings suggest that traditional digital forensic methodologies, while robust under current technological standards, must address quantum data's multi-state, entanglement, and no-cloning properties, which can fundamentally alter digital evidence. The thesis advocates for a paradigm shift in forensic processes to incorporate quantum-resistant techniques that ensure the integrity and admissibility of evidence. Additionally, it highlights the necessity for ongoing education and collaborative research to effectively adapt digital forensics to this new technological era. This research contributes to the theoretical framework and practical applications of digital forensics, aiming to future-proof forensic practices against the disruptive nature of quantum computing.

keywords: digital forensics, quantum computing, forensic guidelines, NIST SP 800-86, ISO/IEC 27037:2012, evidence integrity, quantum-resistant techniques, quantum superposition, quantum entanglement, no-cloning theorem, forensic process adaptation, quantum forensics, digital evidence, quantum era challenges, forensic methodology

Acknowledgement

To my wife, Janina, and our two daughters, Ellinore and Isabelle – you are my heart, home, and inspiration. Your unwavering love and support carried me through this journey. Thank you for putting up with my late nights and distracted conversations and for constantly reminding me of what truly matters. I love you more than life itself.

To Martin, Pierre, Roger, and Gustav – who knew virtual mayhem could be so good for the soul? Thanks for the epic battles, the hilarious fails, and for keeping my spirits high. You guys are the best kind of distraction. Thanks for always being there to help me unwind, recharge, and remember not to take everything too seriously.

Lastly, I would like to sincerely thank my supervisor, Oskar MacGregor, and my examiner, Rose-Mharie Åhlfeldt. Their guidance and insights were invaluable in shaping this thesis from its inception to its completion.

Contents

1 | Introduction

The increasing sophistication of digital technology, while revolutionizing modern life, simultaneously introduces new challenges to the field of information security. As technology continues to evolve, so too does the digital landscape, and with it, the domain of digital forensics. Digital forensics, a crucial discipline within computer science, employs scientific principles and rigorous processes to analyze electronically stored information, reconstructing the sequence of events leading to a specific incident (Garfinkel, 2010; Raghavan, 2013). It involves various techniques and tools to detect, track, and identify cybercrimes, analyze system activities, and provide evidence for legal proceedings (de Braekt et al., 2016). The methodology for conducting digital forensic investigations includes data detection, acquisition, processing, analysis, and reporting (Kent et al., 2006).

Central to the integrity of digital forensics is the unwavering principle of evidence preservation. Ensuring that digital data remains unaltered and uncompromised throughout its lifecycle is paramount for its admissibility in court (Alghamdi, 2021). For evidence to be deemed admissible, the tools and techniques employed must be scientifically valid and consistently produce accurate results, a rigor achieved through comprehensive empirical testing (Maras, 2014).

Digital forensic practitioners, in their pursuit of justice, must continually adapt to the ever-evolving landscape of technological threats. These threats encompass the increasing sophistication of malware, the complexities introduced by advanced encryption methods, and the sheer volume of data encountered during investigations (Karie & Venter, 2015). Amidst these mounting challenges, the emergence of quantum computing presents unique and significant challenges to the very foundations of digital forensic practices.

Quantum computing, an emerging field with the potential to revolutionize various industries, leverages the laws of quantum physics to perform computations that are impossible for classical computers. Unlike classical computers, which use bits to represent information as either 0 or 1, quantum computers utilize quantum bits, or qubits. Qubits can exist in a superposition of states, meaning they can be 0, 1, or both simultaneously (Marella & Parisa, 2022). This, along with other quantum phenomena like entanglement (a phenomenon where two or more quantum particles (not just qubits) become linked in such a way that their properties become interdependent, regardless of the distance between them), allows quantum computers to process vast amounts of data and perform complex calculations at unprecedented speeds (Erhard et al., 2020; Kuzyk, 2019; Ourabah & Tribeche, 2017). While still in its developmental stages, quantum computing promises groundbreaking advancements in diverse fields, including chemistry (Cao et al., 2019; Dral, 2020), finance (Ganapathy, 2021), cryptography (Pirandola et al., 2020), and materials science (Maletin et al., 2023). Recent breakthroughs, such as Google's claim of achieving quantum supremacy (Arute et al., 2019; Pichai, 2019; Tavares, 2019), have likely contributed to increased interest and investment in this field. Projections suggest that approximately 5,000 quantum computers will be operational by 2030, although the full realization of their potential for complex problem-solving may not be achieved until 2035 or later (Stackpole, 2024). This timeline is corroborated by expert

opinions gathered for this thesis, with one digital forensics academic suggesting a widespread adoption of quantum computing within the next two decades.

However, the very characteristics that make quantum computing so promising also pose profound challenges to traditional digital forensic methodologies. The ability of quantum data to exist in multiple states simultaneously (superposition) and its capacity for entanglement across different locations directly contradict the established forensic principles of data integrity and non-alteration (Alghamdi, 2021). Observing or measuring quantum data inherently alters its state, introducing uncertainty as to whether observed changes are the result of malicious activity or simply artifacts of the measurement process. Additionally, the potential for quantum computers to break widely used encryption algorithms raises concerns about the confidentiality and integrity of digital evidence stored or transmitted using these methods.

This thesis delves into the critical intersection of quantum computing and digital forensics, with a specific focus on how the unique properties of quantum systems could undermine the reliability of digital evidence. It aims to rigorously assess the vulnerabilities of existing forensic methodologies, particularly the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-86 (Kent et al., 2006) and the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27037:2012 guidelines, in the face of quantum advancements. These guidelines are widely acknowledged and implemented by federal agencies and organizations worldwide, emphasizing their importance and influence in shaping forensic practices globally. By exploring potential adaptations to these widely adopted frameworks, this research seeks to safeguard the integrity and admissibility of evidence in the burgeoning age of quantum computing.

1.1 Aims and Objectives

This thesis explores how established and industry-recognized digital forensic guidelines might need to evolve to address the challenges to digital evidence integrity posed by quantum computing.

The specific objectives of this thesis are:

1. Critically analyze the impact of quantum computing's potential for seamless data alteration on digital evidence reliability and trustworthiness.
2. Propose modifications to existing forensic models to enhance the integrity and protect the admissibility of digital evidence extracted from quantum systems or potentially manipulated using quantum techniques.

1.2 Research Question

This thesis will try to answer the following question: *How can digital forensic models be adapted to safeguard digital evidence integrity when confronted with the specific challenges posed by quantum computing's data alteration potential?*

1.3 Outline

The following chapters outline this thesis:

1. **Introduction:** Sets the stage by outlining the research's motivation, objectives, and scope and laying the foundation by discussing the growing significance of quantum computing in digital forensics, highlighting how it impacts the reliability and integrity of digital evidence.

2. **Background:** Explores digital forensics and quantum computing principles, showing how quantum mechanics challenges existing forensic models and practices through a comprehensive review of relevant academic literature.

3. **Methodology:** Describes a mixed-methods approach combining a document analysis of well-known digital forensics guidelines, and semi-structured qualitative interviews with digital forensics experts to examine how digital forensics can adapt to the quantum era.

4. **Result:** Analyzes the findings from the document analysis and interviews, focusing on the vulnerabilities of current forensic models to quantum computing and suggesting necessary adaptations.

5. **Discussion:** Critically examines the results, proposing a novel forensic model suitable for the quantum context, discussing potential future challenges, and outlining directions for further research.

6. **Conclusion:** Summarizes the main findings and their implications for digital forensics in quantum computing, emphasizing the need for ongoing adaptation and collaborative research.

2 | Background

Digital forensics employs scientific methods to identify, collect, examine, and analyze digital data, with a strict emphasis on maintaining a chain of custody. The chain of custody is a legal term that refers to a chronological documentation on how evidence is handled and tracked in investigations and trials, ensuring its integrity from collection to presentation in legal proceedings (Kent et al., 2006). Traditional practices rely on classical computing principles, including data duplication for preservation (prioritizing volatile memory like RAM), specialized software tools for analysis, and legal presentation of findings. However, the rapidly evolving technological landscape is challenging these established methods. The exponential growth in data volumes (Sikos, 2021), the proliferation of complex encryption methods that protect user data but complicate forensic analysis (Li & Liu, 2020), and the rise of advanced malware techniques that evade traditional detection (Karie & Venter, 2015) are a few examples. Additionally, the shift towards cloud computing has introduced new layers of complexity regarding data jurisdiction and access, pushing the limits of traditional forensic tools and methods and necessitating a reevaluation of established practices in the field.

Among these evolving challenges, the rise of quantum computing introduces a distinct and formidable disruption that redefines the foundational principles of digital forensics. Unlike classical computing, which uses bits in states of 0 or 1, quantum computing utilizes quantum bits, or qubits, which can exist in multiple states simultaneously (Wong, 2023). This ability of qubits to exist in multiple states simultaneously—known as superposition—enables quantum computers to perform computations at exponentially greater speeds than its classical counterpart. This capability is further enhanced by quantum entanglement, a phenomenon where pairs or groups of quantum particles (such as atoms, photons, or qubits) become interconnected such that the state of one directly influences the state of another, regardless of distance (Taddei et al., 2013).

The unique properties of quantum computing extend computational frontiers (Arute et al., 2019; Marella & Parisa, 2022) and pose unprecedented challenges to digital forensics. Observing quantum systems can collapse their superposition states, potentially altering or destroying the evidence in ways that contravene forensic standards (Bassi et al., 2013). The superposition collapse of states can be thought of like a coin spinning in the air–while it is spinning, it is both heads and tails. But once someone catch it and look, it is definitely one or the other. Furthermore, the quantum No-Cloning Theorem illustrates a fundamental impediment to traditional forensic practices: replicating unknown quantum states is impossible (Kuzyk, 2019), complicating the duplication of evidence for analysis and preservation.

Given the substantial implications of quantum technology, developing new digital forensic methodologies that are cognizant of quantum phenomena is essential. These methodologies must address the challenges presented by quantum computing and uphold the integrity, admissibility, and trustworthiness of digital evidence. This chapter sets the stage for a comprehensive examination of how quantum computing could undermine traditional digital forensics, highlighting the critical need for innovative practices that can adapt to and integrate these advancements. The subsequent chapters will delve deeper into existing digital forensic guidelines, explore their vulnerabilities

within a quantum context, and propose the necessary adaptations suited for the emerging quantum era.

2.1 Preliminaries

To effectively address the challenges that quantum computing presents to digital forensics, a foundational understanding of both domains is essential. In this thesis, *quantum computing* is defined as "a computer that uses the quantum states of subatomic particles to store information," according to the Oxford English Dictionary.

2.1.1 Digital Forensics Processes and Legal Significance

Digital forensics, as described by Kent et al. (2006), is "a branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting on data stored electronically." This meticulous process exists primarily to support two noteworthy areas: the legal or investigative purposes of criminal activity and incident response. The latter involves responding to and managing the aftermath of a security incident, such as a cyberattack or a data breach (Kävrestad et al., 2024). Digital forensic process models offer structured frameworks that ensure the integrity and admissibility of digital evidence in legal proceedings. Numerous digital forensic process models exist, each with its own approach and areas of emphasis. Although researchers and investigators have tried to standardize a single unified model, widespread adoption has been limited, likely due to the tailored nature of many models designed for specific environments, like law enforcement, which can hinder their adaptability to other contexts (Valjarevic & Venter, 2015).

Given the wide variety of existing digital forensics processes, this thesis focuses on two internationally recognized guidelines: the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-86: Guide to Integrating Forensic Techniques into Incident Response*, by Kent et al. (2006), and the *International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27037:2012 - Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence.* This choice is motivated by several critical reasons. NIST SP 800-86 and ISO/IEC 27037:2012 are widely acknowledged and influential within the digital forensics community, providing a solid foundation for forensic practices. These guidelines are widely acknowledged by federal agencies worldwide, emphasizing their importance, influence, and acceptance in the digital forensics community (Ramadhan et al., 2022), providing a robust foundation for exploring necessary adaptations in the era of quantum computing. As quantum computing disrupts the core assumptions about data handling that form the foundation of these guidelines, focusing on adapting them has several key advantages. First, it ensures immediate practical relevance. Many agencies and organizations already adhere to these guidelines, meaning the changes this thesis proposes will directly lead to real-world implementation. Second, the high-profile nature of these guidelines means their adaptation could shape the evolution of digital forensic practices globally.

Furthermore, this thesis will concentrate on the digital forensic process outlined in NIST SP 800-86 and ISO/IEC 27037:2012 to maintain a defined scope. While other guidelines such as *ISO/IEC 27041:2015 - Information technology. Security techniques. Guidance on assuring suitability and adequacy of incident investigative method* or *ISO/IEC 27042:2015 - Information technology. Security techniques. Guidelines for the analysis and interpretation of digital evidence* address additional aspects of the digital forensics process, they fall outside the specific focus of this thesis. Additionally, this work does not consider digital forensic processes described in journals, conference proceedings, or draft/proposing standards, such as NISTIR 8354-DRAFT

(Lyle et al., 2022), focusing solely on these internationally recognized guidelines to anchor the discussion.

NIST SP 800-86

Kent et al. (2006) outlines a four-step investigative model in the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-86: Guide to Integrating Forensic Techniques into Incident Response* (see Figure 2.1):

- **Collection:** This phase entails systematically identifying, labeling, and acquiring potential evidence sources, including computers, mobile devices, cloud storage, or network logs. Creating forensic duplicates of the original data is often critical to preserving evidence integrity at this stage.
- **Examination:** The collected data is meticulously scrutinized using specialized forensic tools and techniques. The main focus here is extracting data of interest while preserving original data integrity. Investigators aim to reduce the scope of data and focus on identifying relevant evidence that supports investigative goals.
- **Analysis:** The extracted and relevant data is then subjected to rigorous analysis by forensic experts. This phase involves using various methods and techniques to derive critical insights that address the questions driving the investigation. Analysts might trace system activity, recover deleted files, or decrypt encrypted data to gather evidence supporting a hypothesis.
- **Reporting:** The final stage involves creating a comprehensive report documenting the forensic process. This report includes details about procedures followed, tools used, and findings derived from the analysis. For the report to hold credibility in a legal context, it must be clear and detailed and present evidence admissibly.

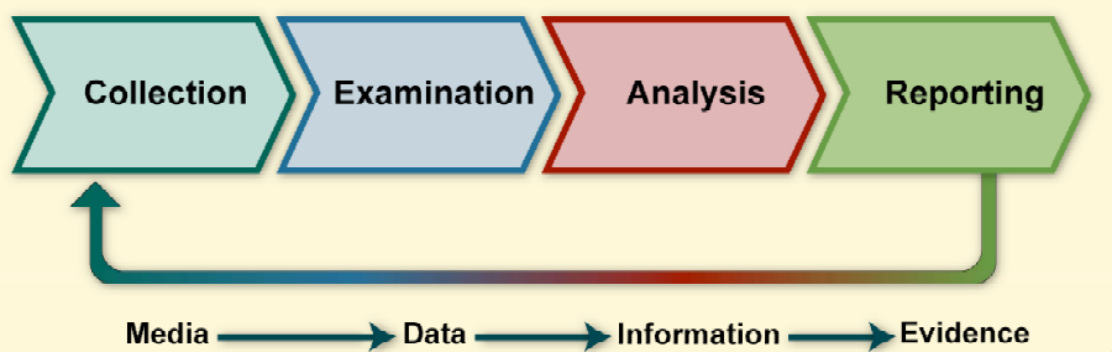

Figure 2.1: The NIST SP 800-86 forensic technique process (Kent et al., 2006).

ISO/IEC 27037:2012

The *International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27037:2012: Guidelines for identification, collection, acquisition and preservation of digital evidence* also follows a four-step process model outlined below:

- **Identification:** This initial phase involves recognizing and documenting potential digital evidence. It requires the search for electronic sources that could contain relevant information, ensuring that all such sources are accurately identified by investigators and legally considered as potential evidence.
- **Collection:** Once the investigators have identified potential evidence sources, the next step is the collection process. During this process, investigators gather physical or logical items containing digital evidence. The main challenge in this phase is ensuring that investigators collect evidence in a way that maintains its integrity and validity for forensic purposes.
- **Acquisition:** Following collection, acquisition involves creating exact copies of digital evidence. This step is critical in ensuring the forensic examination proceeds on duplicate data to preserve the original evidence's integrity. This process also includes verifying that the acquired data is a true and accurate representation of the original.
- **Preservation:** The final step involves maintaining and safeguarding the integrity and original condition of the digital evidence. Preservation strategies must protect evidence from physical and environmental damage and unauthorized alterations, ensuring the evidence remains stable and reliable for analysis and potential legal proceedings.

Importance of Digital Evidence Integrity

The integrity of digital evidence stands as a cornerstone in digital forensics, as emphasized by the established digital forensics processes detailed previously (Koroniotis et al., 2019). Integrity is essential for ensuring evidence is trustworthy and reliable, as investigators actively shield it from unauthorized alterations from the point of collection to its presentation in court. Traditional forensic methodologies prioritize secure collection, duplication, and meticulous handling to maintain the pristine state of digital evidence (Prayudi & Sn, 2015; Shah et al., 2017).

Maintaining the integrity of digital evidence is crucial for multiple reasons. Foremost, the trustworthiness of evidence is paramount in legal proceedings, where it underpins the ability to reach fair and just verdicts. A lapse in the integrity of digital evidence can lead to miscarriages of justice, with judges and juries making decisions based on compromised information. Furthermore, investigators utilize digital evidence to develop leads, identify suspects, and reconstruct crime scenes. Should the integrity of this evidence be compromised, it could significantly derail investigations, leading to delays, wasted resources, or even the failure to resolve criminal cases (Weilbach & Motara, 2019). In contexts such as intellectual property disputes or data breaches, the integrity of digital evidence becomes particularly critical. It is foundational in determining culpability and securing appropriate redress. Altered evidence can tarnish reputations and precipitate severe legal and financial repercussions for individuals and organizations (Campbell et al., 2003).

In the forthcoming chapters, this thesis will delve into the challenges that quantum computing introduces at each stage of these established digital forensic processes. It will focus on how the unique attributes of quantum systems, particularly their susceptibility to alteration, could compromise the traditional methods employed to safeguard evidence integrity. This analysis aims to illuminate how quantum computing could impact the reliability of digital evidence in the new era of quantum technology.

2.1.2 Quantum Mechanics & Computing Principles

To fully grasp the implications of quantum computing for digital forensics, a foundational understanding of the underlying principles is crucial. Quantum mechanics, the scientific study of

the behavior of matter and energy at the smallest scales, is inherently complex and counterintuitive. It is defined not just by its mathematics and experimental predictions but also by various interpretative frameworks that attempt to explain its often perplexing phenomena.

In quantum mechanics, several interpretations offer differing views on the nature and behavior of particles and measurements. These interpretations are crucial in providing conceptual clarity and guiding experimental approaches in quantum physics and, by extension, quantum computing. This thesis specifically focuses on the following interpretations, chosen to discuss relevant quantum phenomena:

1. **The Copenhagen Interpretation (Buckley et al., 1979) for superposition:** Even though the Copenhagen Interpretation does not apply universally across all areas of quantum physics (Shestakova, 2020), the interpretation remains the most prevalent and traditionally taught in the academic context (Zhang, 2023). It provides a pragmatic framework that is particularly useful in explaining the wave-function collapse—a phenomenon central to understanding how measurement affects quantum states. This aspect is essential for discussing the implications of quantum computing in digital forensics, particularly how measuring quantum information could fundamentally alter the data, thereby challenging the integrity of digital evidence.
2. **The Relational Interpretation (Rovelli, 1996) for entanglement:** Given that quantum entanglement involves states that are intrinsically connected regardless of distance, the Relational Interpretation offers a profound perspective by emphasizing how the properties of entangled particles are relative to the observer's frame of reference. This interpretation helps elucidate the subtleties of entangled states in quantum computing, which can impact forensic analyses where observing one part of the system instantaneously affects its entangled counterpart.

The selection of these interpretations reflects their ability to address specific aspects of quantum computing that are pivotal to understanding and managing the forensic challenges posed by this new technology. Each interpretation has been selected not only for its academic rigor and historical significance but also for its practical relevance to the specific quantum phenomena that underpin quantum computing technologies. This approach ensures a nuanced and precise discussion suitable for the forensic implications explored in this thesis.

Quantum Computers

Unlike classical computers that rely on transistors, quantum computers utilize various physical systems to create qubits–the fundamental unit of quantum information. The most promising platforms include superconducting circuits, trapped ions, and photonic systems.

Superconducting circuits leverage superconducting materials, such as the chemical elements niobium (Nb) and tantalum (Tb) (Shen, 1972), at extremely low temperatures, forming circuits with unique quantum properties (Devoret & Schoelkopf, 2013). The circuits have infinite conductivity and zero resistance at near absolute zero temperatures. Josephson junctions are crucial in manipulating quantum states, potentially vulnerable to disruption during forensic observation (Golubov et al., 2004). Companies like IBM and Google are pioneers in this realm, exploring quantum capabilities (Chan, 2019; Shrimangale, 2024).

Scientists build trapped-ion quantum computers by carefully controlling ions (charged atoms) with lasers and electromagnetic fields (Cirac & Zoller, 1995). These systems can achieve long coherence times (i.e., how long a state remains reliable) (Häffner et al., 2008). These systems may necessitate specialized examination techniques to prevent the inadvertent alteration of their quantum states during forensic analysis.

Lastly, photonic systems use photons (light particles) as information carriers, offering advantages including the potential for integration with existing optical networks (Wang et al., 2019). Forensic considerations include gathering and examining photonic evidence without impacting its fragile nature.

Superposition

The principle of superposition allows qubits to exist in multiple states simultaneously, unlike classical bits that are constrained to 0 or 1. This capability of superposition underpins the potential for immense computational power, as noted by (Arute et al., 2019; Marella & Parisa, 2022).

However, superposition also introduces significant challenges in digital forensics. When a qubit in superposition is measured, it collapses into one of its definite states (0 or 1). This collapse implies that the data could alter instantaneously at the measurement point. Such a phenomenon critically threatens traditional forensic methods that rely on digital evidence remaining unaltered throughout the investigatory process.

The implications of superposition are well illustrated by Erwin Schrödinger's famous thought experiment, Schrödinger's Cat, introduced in 1935. In this experiment, a hypothetical cat in a box, linked to a quantum event, is simultaneously dead and alive until someone opens the box and observes the cat. Through this thought experiment, Schrödinger aimed to underscore the counterintuitive nature of quantum systems and the difficulties in reconciling these concepts with our macroscopic experiences. Schrödinger intended the thought experiment as a critique of the Copenhagen interpretation, highlighting the seemingly absurd implications of applying quantum mechanics to macroscopic objects like cats. He wasn't trying to make a definitive statement about the cat's state, but rather to provoke thought and debate about the interpretation of quantum mechanics. Nevertheless, the thought experiment has gained a famous reputation since and is often used to illustrate the complexities of superposition.

Furthermore, Park (1970) initially thought of and mathematically proved what would later become known as the No-Cloning Theorem by (Wootters & Zurek, 1982), who more formally derived it. The No-Cloning Theorem states the impossibility of perfectly replicating an unknown quantum state, implying that traditional approaches to cloning the digital evidence material become inapplicable. Quantum error correction schemes could circumvent this limitation, which relies on encoding quantum information across multiple entangled qubits to introduce redundancy in a manner that does not directly measure and collapse the original state (Kuzyk, 2019). However, the theorem highlights the fragility of quantum systems; any attempt to directly copy a qubit would inevitably alter the original due to superposition (Pang & Wu, 2010). This limitation could necessitate the development of meticulous quantum state preparation methods and carefully designed interactions within quantum algorithms. Such strategies must mitigate the risk of unintentional state disturbance while implementing quantum error correction schemes that circumvent the challenges introduced by the theorem.

For digital forensics, the concept of superposition and the inherent changes induced by observation pose profound challenges. Forensic methodologies traditionally depend on the ability to duplicate and examine evidence without altering it. Quantum systems, however, challenge this foundational principle, potentially necessitating a significant paradigm shift in how evidence is collected and analyzed. This shift becomes critical as interacting with quantum data to investigate it could inadvertently compromise the evidence it seeks to preserve. Furthermore, unlike classical computing, where data often remains recoverable from a disk even after power loss, turning off a quantum computer could completely eradicate the evidence.

Quantum Interference

Quantum interference demonstrates how probabilities, not deterministic states, underlie quantum computation. Scientists and investigators can amplify specific outcomes while suppressing others by carefully manipulating the interaction of qubits in superposition. This principle is key to the power of quantum algorithms:

- **Grover's Search Algorithm** (Grover, 1996): Provides a speed advantage for searching unsorted data, potentially making traditional database encryption methods less secure, which could necessitate new ways to protect sensitive data in the quantum era.
- **Shor's Algorithm** (Shor, 1994): Efficiently factors large numbers, threatening current cryptographic methods like RSA (Rivest–Shamir–Adleman), the public-key cryptosystem. The capability of quantum computers to perform complex calculations at unprecedented speeds raises the specter of "encryption cracking," which could actively render the mechanisms designed to secure data obsolete (Sharma et al., 2021). This capability directly challenges the ability to ensure confidentiality and integrity of evidence within the chain of custody (Bhatia & Ramkumar, 2020).

The reliance of quantum systems on probabilistic outcomes further complicates forensic analysis. Consider digital evidence stored on a system utilizing quantum interference mechanisms. It might be impossible to extract a "perfect" copy of that evidence without introducing changes due to the act of observation. Also, proving such evidence's origin could be problematic if the quantum algorithms scrambled or obfuscated its source.

Quantum Entanglement

Quantum entanglement is a phenomenon where two or more qubits become inextricably linked, such that their states are no longer independent. Measuring one entangled qubit immediately determines the state of its counterpart(s), even if the counterpart(s) reside vast distances away (Einstein et al., 1935; Griffiths & Schroeter, 2018). This seemingly instantaneous correlation defies our classical understanding of locality and has significant implications for computation and communication.

Entanglement poses unique challenges for digital forensics, particularly the chain of custody. Consider a scenario where entangled qubits store and transmit sensitive evidence. If examining one qubit collapses its state, it instantaneously alters the correlated entangled qubits, potentially destroying other evidence segments. This mechanics fundamentally challenges traditional evidence collection and analysis notions, where information is often assumed to be independent and observable without consequence.

Moreover, entanglement introduces questions about how to establish the provenance and authenticity of evidence in a quantum-influenced world. Verifying the integrity of quantum evidence becomes a challenge if its state intrinsically links it to other entangled systems that may have been tampered with or altered outside the scope of direct observation.

While entanglement presents challenges, it also holds potential for novel forensic techniques. Imagine using entanglement as a tool to guarantee the authenticity of digital evidence. By deliberately entangling parts of the evidence, any attempt to modify one piece would be detectable due to the corresponding change in the entangled counterpart(s). Further research is needed to explore the practical feasibility of such approaches.

Understanding the principles of quantum hardware, superposition, entanglement, and interference is critical as we re-imagine digital forensics for the quantum era. It underscores the need to proactively develop new forensic models and evidence-handling procedures that ensure the integrity and admissibility of evidence derived from or influenced by quantum systems.

3 | Method

This chapter outlines the methodological framework employed within this thesis. It begins by clarifying the research approach adopted, a mixed-methods design combining document analysis and qualitative interviews. The chapter then details the methods used for data collection and the data analysis techniques employed. Finally, the chapter critically discusses the validity and reliability of the methodology used, acknowledging its limitations and proposing avenues for future research.

3.1 Research Approach

This thesis employed a qualitative mixed-methods approach to explore the challenges posed by quantum computing to digital forensics, specifically examining how existing forensic methodologies under NIST SP 800-86 and ISO/IEC 27037:2012 need to adapt to maintain the integrity and admissibility of digital evidence in the context of quantum computing.

A mixed-methods approach was chosen to leverage the structured, systematic analysis afforded by document analysis and the nuanced, contextual insights provided by qualitative interviews. This combination allowed for a comprehensive exploration of the challenges and potential adaptations required for digital forensic processes in the face of quantum computing advancements. By integrating these two methods, the research aimed to provide a robust and well-rounded understanding of the issues at hand.

The primary methodological component was a document analysis of key forensic standards, guided by Bowen's (2009) framework, "Document Analysis as a Qualitative Research Method." This approach was selected due to the centrality of these documents in guiding forensic practices and the ability of document analysis to provide a detailed, systematic examination of formal documents like these standards. Unlike broader literature reviews, document analysis allows for a focused examination of how quantum computing principles directly impact the specific guidelines and procedures outlined in these standards. This method is particularly well-suited for analyzing the intricacies of formal documents and extracting precise information to address the research questions posed in this thesis.

Complementing the document analysis, the second methodological strand involved semi-structured interviews with professionals directly involved in or with expertise in quantum computing and digital forensics. To ensure comprehensive coverage, a semi-structured interview guide was developed based on key themes identified in the document analysis. This guide included open-ended questions that prompted detailed discussions on specific challenges posed by quantum computing to digital forensic methodologies, potential modifications to current practices, and the future direction of forensic science in a quantum computing context. The semi-structured format allowed for flexibility in discussions, enabling interviewees to elaborate on their experiences and insights, thereby ensuring that all relevant areas were thoroughly explored.

3.2 Document Analysis

The document analysis was a critical component of this research, providing a foundation for understanding the current state of digital forensic guidelines and their limitations when confronted with the advancements in quantum computing. This particular methodology was based on the Western Carolina University article "Document Analysis as a Qualitative Research Method" by Bowen (2009). This section details the selection criteria for the documents analyzed and the methodological approach taken.

3.2.1 Selection of Documents

The documents selected for this analysis included key international guidelines that are widely recognized and implemented within the digital forensics community. Specifically, the analysis focused on:

- NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response
- ISO/IEC 27037:2012: Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence

The selection of these documents was guided by several factors. First, their relevance to current forensic practices was paramount. The documents needed to be directly applicable to the challenges and opportunities presented by quantum computing. Second, the authority and acceptance of these guidelines within the field were crucial. By focusing on widely acknowledged and implemented standards, the research aimed to ensure that its findings were firmly grounded in recognized best practices. Finally, the selected documents needed to provide comprehensive guidance on all aspects of evidence handling, encompassing the entire spectrum from initial collection to meticulous preservation. This comprehensive approach ensured that the analysis could thoroughly assess the potential impact of quantum computing on each stage of the forensic process.

3.2.2 Methodological Approach

The analysis of the selected documents followed a systematic and rigorous approach, drawing upon established qualitative research methods, particularly content analysis and thematic analysis, as described by Bowen. The process involved several key steps:

1. **Familiarization:** The initial step involved thoroughly reading both NIST SP 800-86 and ISO/IEC 27037:2012 to gain a deep understanding of the forensic processes they outlined. This step was crucial for familiarizing the researcher with the content, structure, and underlying principles of the documents.
2. **Data Extraction:** Relevant sections of the documents were identified and extracted for detailed analysis. This included sections that specifically addressed evidence collection, preservation, analysis, and reporting. These sections were chosen based on their direct relevance to the research questions and the potential impact of quantum computing on these processes.
3. **Thematic Coding:** The extracted data were then systematically coded using MAXQDA[1], a qualitative data analysis software. This involved identifying recurring themes and patterns

[1] https://www.maxqda.com/

related to the challenges and opportunities presented by quantum computing. Key themes included evidence integrity, chain of custody, data acquisition, analysis techniques, and reporting requirements. The coding process was iterative, allowing for the refinement and adjustment of codes as new insights emerged.

4. **Application of Quantum Principles:** The coded themes were then analyzed through the lens of quantum computing principles, such as superposition, entanglement, and the no-cloning theorem. This step involved a detailed examination of how these quantum phenomena could potentially disrupt or challenge the existing forensic processes outlined in the documents.

5. **Interpretation and Synthesis:** The findings from the previous steps were interpreted and synthesized to identify potential vulnerabilities and areas where the current forensic guidelines might need to be adapted. This involved a critical evaluation of the existing frameworks and the development of recommendations for modifications or new approaches that could better address the challenges posed by quantum computing.

By following this systematic and rigorous approach, the document analysis provided a comprehensive and nuanced understanding of the potential impact of quantum computing on digital forensics. The findings from this analysis served as a foundation for the subsequent qualitative interviews, informing the development of interview questions and guiding the overall research direction.

3.3 Qualitative Interviews

Complementing the document analysis, the second methodological strand of this work involved conducting qualitative semi-structured interviews. This method was particularly suitable for its flexibility and effectiveness when exploring complex and nuanced topics like the practical implications of quantum computing on digital forensics (Creswell & Poth, 2024). Semi-structured interviews allowed for in-depth discussions where interviewees could elaborate on their experiences, perceptions, and suggestions. This format balanced obtaining targeted information aligned with the research objectives while allowing space for unexpected insights to emerge (Wholey et al., 2015), which is crucial in a rapidly evolving field like quantum computing.

The primary objective of the interviews was to complement and enhance the theoretical insights obtained from the document analysis by examining practical implications and real-world scenarios. This method aimed to uncover practical challenges and potential solutions related to the integration of quantum computing into digital forensics. The interview data were analyzed using a thematic analysis approach, ensuring that key themes and patterns were systematically identified and interpreted (Schultze & Avital, 2011). This process included iterative reading and coding of the interview transcripts to develop a comprehensive understanding of the experts' perspectives. The robustness of the findings was further ensured by employing reflexivity techniques, such as maintaining a reflective journal to document decision-making processes and interpretations throughout the research.

3.3.1 Participant Selection and Interview Process

Participants were selected through a purposive sampling method (Campbell et al., 2020), focusing on their expertise and significant involvement in areas relevant to both quantum computing and digital forensics. The selection criteria included their professional experience, contributions to relevant research, and their active engagement in the field. This approach was designed to ensure

that the collected insights were both current and practically applicable, thereby enriching the theoretical findings from the document analysis. The purposive sampling method allowed for the identification of individuals who could provide deep, expert insights into the impact of quantum computing on digital forensics.

The individuals interviewed for this thesis were:

- **Digital Forensics Academic (Netherlands):** An academic expert in digital forensics, providing insights into the academic and practical impacts of quantum computing on digital forensics.
- **Incident Response Expert (Finland):** A senior member of an incident response team, providing a hands-on perspective on the challenges faced by forensic professionals in the industry.
- **Forensic Investigator (U.K.):** A principal investigator and qualified expert witness, offering practical insights into the adaptations required for forensic methodologies.
- **Digital Forensics Expert (Sweden):** This expert provided insights into the practical challenges and adaptations required in the field of digital forensics when dealing with quantum computing technologies.
- **Quantum Physicist (U.S.):** This physicist offered a deep understanding of quantum principles and their potential impact on digital forensic processes.

Each interview, lasting approximately 45 minutes, followed a semi-structured guide (Adeoye-Olatunde & Olenik, 2021), developed based on key themes identified in the document analysis. This guide included open-ended questions that prompted discussion on specific challenges quantum computing posed to digital forensic methodologies, potential modifications to current practices, and the future direction of forensic science in a quantum computing context. Before the interviews, participants were offered confidentiality, ensuring their identities would be protected and specific details shared during the interviews would not be disclosed without their consent. All interviews were conducted using Microsoft Teams video conferencing, recorded with participant consent, and transcribed for analysis.

3.3.2 Interview Guide

The semi-structured interview guide was developed to ensure comprehensive coverage of the necessary aspects of the research (Kallio et al., 2016). The questions were designed to elicit detailed responses and allow interviewees to share their experiences and insights freely. The exact questions can be found in Annex A.

The guide covered the following key themes:

1. The perceived impact of quantum computing on current digital forensic models and frameworks.
2. Proactive steps the digital forensics community should take to prepare for the integration of quantum computing.
3. Potential effects of quantum computing on the integrity, admissibility, and reliability of digital evidence.
4. Key features that future digital forensic frameworks should include to address quantum computing challenges.

5. Theoretical and practical approaches to adapting forensic models for quantum computing capabilities.

6. Policy and ethical considerations for digital forensic practices in quantum computing environments.

The flexibility of the semi-structured format ensured that discussions could adapt to the flow of conversation, allowing for the exploration of unexpected but relevant topics.

By using this structured yet flexible approach, the research ensured that the interviews provided both depth and breadth of insight into the intersection of quantum computing and digital forensics. The resulting data were rich in detail, offering valuable perspectives that complemented the findings from the document analysis.

3.4 Data Analysis

This section delineates the methodologies and sequential steps in analyzing the document analysis and qualitative interview data. The aim is to transparently outline the analytical procedures, ensuring the rigor and reproducibility of the findings.

3.4.1 Analysis of Documents

The analysis of the NIST SP 800-86 and ISO/IEC 27037:2012 documents involved a systematic approach to identify potential vulnerabilities and areas for adaptation in the face of quantum computing advancements. The process began with a thorough reading and familiarization with the content and structure of both documents. This initial step was crucial for understanding the underlying principles and processes outlined in the guidelines.

Following familiarization, relevant sections of the documents were extracted for detailed analysis. These sections specifically addressed evidence collection, preservation, analysis, and reporting, as these areas are most likely to be impacted by quantum computing technologies. The extracted data were then systematically coded using MAXQDA. This involved identifying recurring themes and patterns related to the challenges and opportunities presented by quantum computing. Key themes that emerged included:

- **Evidence Integrity:** The ability to maintain the unaltered state of digital evidence throughout the forensic process.
- **Chain of Custody:** The chronological documentation of evidence handling to ensure its integrity.
- **Data Acquisition:** The methods and techniques used to collect digital evidence.
- **Analysis Techniques:** The processes used to examine and interpret digital evidence.
- **Reporting Requirements:** The standards for documenting and presenting forensic findings.

The coded themes were then analyzed through the lens of quantum computing principles, such as superposition, entanglement, and the no-cloning theorem. This step involved a detailed examination of how these quantum phenomena could potentially disrupt or challenge the existing forensic processes outlined in the documents. For example, the no-cloning theorem's prohibition

on creating exact copies of unknown quantum states directly conflicts with the traditional forensic practice of duplicating evidence for analysis.

The findings from the thematic coding and the application of quantum principles were then interpreted and synthesized to identify potential vulnerabilities and areas where the current forensic guidelines might need to be adapted. This involved a critical evaluation of the existing frameworks and the development of recommendations for modifications or new approaches that could better address the challenges posed by quantum computing. For instance, the analysis might suggest that forensic tools need to be developed that can analyze quantum data without causing it to collapse or that new protocols for documenting the chain of custody of quantum evidence need to be established.

3.4.2 Analysis of Qualitative Interview Data

Given the qualitative nature of the interviews and the relatively small sample size (five interviewees), a thematic analysis approach was deemed the most appropriate (Braun & Clarke, 2012; Kiger & Varpio, 2020). The interview data were analyzed using MAXQDA, employing a combination of AI-assisted coding and researcher-led thematic analysis.

The analysis began with carefully reading the interview transcripts to gain an initial understanding of the data. This close reading emphasized identifying key ideas, topics, and patterns that arose organically from the responses. Given the open-ended questions and participants' specialized knowledge, this respected the nuanced nature of their insights.

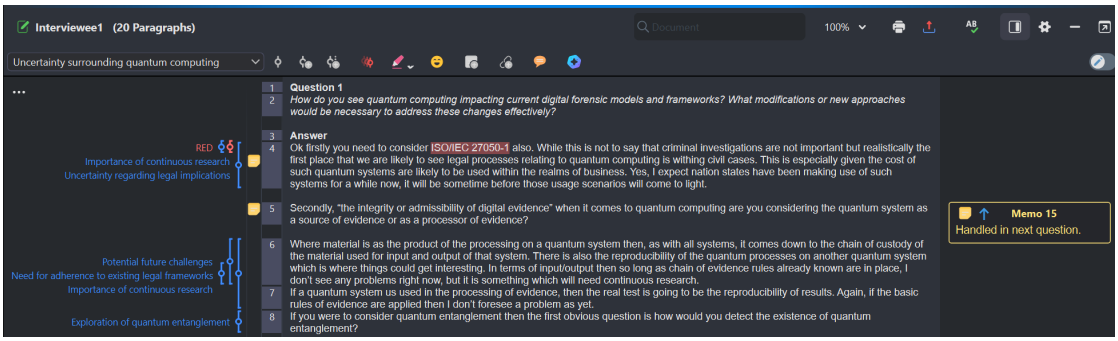

Figure 3.1: A screenshot of MAXQDA software in which the coding was done.

The AI features of MAXQDA were utilized to assist in the initial coding process, identifying potential codes and patterns in the data. However, the researcher maintained an active role in refining and finalizing the codes, ensuring their relevance and accuracy to the research objectives. This approach allowed for a balance between leveraging the efficiency of AI and the interpretive expertise of the researcher.

Themes were developed by grouping related ideas across the interviews, ensuring they accurately represented response patterns. To mitigate researcher bias, the thematic groupings were grounded directly in the participants' words. While the small sample size limits broad generalizations, this analysis offered valuable expert insights into potential future directions of digital forensics in a quantum computing landscape.

3.5 Validity and Reliability

This thesis incorporated several measures to ensure the validity and reliability of the findings. The mixed-methods approach, combining a document analysis with qualitative interviews, sought to triangulate data and enhance the robustness of the conclusions. The document analysis focused on universally recognized and widely adopted forensic standards, while the interview process involved a semi-structured guide and a purposive selection of participants with expertise in quantum computing and digital forensics. Reflexivity techniques, such as memoing, were employed to track interpretations and minimize researcher bias. Additionally, member checking was conducted by sharing preliminary findings with interviewees to verify the accuracy and resonance of the interpretations. These measures ensured that the research findings were robust, credible, and applicable to both theoretical advancements and practical applications in digital forensics and quantum computing.

This thesis also acknowledged several limitations that may affect the generalizability and applicability of its findings. The document analysis, while thorough, did not constitute a full systematic review, potentially overlooking some relevant studies. The qualitative interviews involved a small, non-random sample of participants, limiting the generalizability of their perspectives. The rapid advancements in quantum computing also necessitate ongoing research to keep the findings up-to-date. Future research should consider a more extensive and systematic document review, a larger and more diverse sample of interviewees, and empirical testing of proposed forensic model adaptations as quantum technologies become more accessible. To address the potential limitations of qualitative interviews, such as researcher bias or subjectivity in interpretations, triangulation with the document analysis findings was employed to enhance the validity and reliability of the results. Additionally, member checking was conducted, allowing interviewees to review and verify the accuracy of the interpretations derived from their responses.

3.6 Ethical Aspects

Ethical considerations were central to this thesis. All interview participants provided informed consent, and their confidentiality was protected. The inclusion of two colleagues as interviewees was acknowledged as a potential conflict of interest. However, impartiality was maintained by applying the same selection criteria to all participants, emphasizing their expertise rather than their affiliations.

The thesis also recognized the broader ethical implications of quantum computing in digital forensics. The advanced capabilities of quantum computing could lead to more invasive forensic techniques, raising significant privacy concerns if not properly regulated. To address these issues, the thesis advocates for stringent ethical guidelines and robust oversight mechanisms to ensure the responsible use of quantum technologies in forensic investigations.

Additionally, the thesis acknowledges the risk of disparities in forensic capabilities between countries and organizations. Wealthier nations and well-funded entities might have easier access to advanced quantum technologies, potentially leading to imbalances in forensic capabilities and affecting the fairness of criminal investigations and prosecutions globally. To mitigate these disparities, the thesis suggests international collaboration and knowledge-sharing through global research partnerships, funding programs for developing countries, and open-access educational resources.

In conclusion, the thesis emphasizes the importance of integrating ethical considerations into developing and applying quantum computing in digital forensics. By establishing robust ethical guidelines, promoting international collaboration, and ensuring transparency, the forensic

community can harness the power of quantum technologies while safeguarding individual rights and promoting justice.

4 | Result

This chapter embarks on an analytical journey to assess the potential impact of quantum computing on the integrity of digital evidence within existing forensic processes. The core aim is to identify how quantum computing's unique capabilities for data alteration require re-thinking established methods for ensuring evidence integrity and admissibility. The analysis examines how foundational quantum principles of superposition, entanglement, and the No-Cloning Theorem could introduce novel challenges at each stage of forensic processes, from evidence collection to courtroom presentation.

4.1 Document Analysis

The analysis will focus on relevant literature and examine two widely used digital forensic processes: the NIST SP 800-86 and ISO/IEC 27037:2012. This theoretical assessment aims to identify potential challenges quantum systems pose to current practices, particularly concerning preserving digital evidence integrity within this evolving technological landscape. The goal is to propose adaptations that ensure these processes remain effective and help maintain the reliability of digital evidence.

While some overlap of the digital forensic processes examined within the NIST SP 800-86 and ISO/IEC 27037:2012 may exist, the aim is to identify the challenges and adaptations unique to the processes mentioned above that focus on safeguarding the integrity and admissibility of evidence potentially influenced by quantum techniques.

4.1.1 NIST SP 800-86

The *National Institute of Standards and Technology's Special Publication 800-86 (NIST SP 800-86): Guide to Integrating Forensic Techniques into Incident Response* provides a structured framework for digital forensics. It emphasizes a four-phase process: **Collection**, **Examination**, **Analysis**, and **Reporting** (Kent et al., 2006), as detailed in section 2.1.1.

The **Collection** phase, as outlined by Kent et al. (2006) in NIST SP 800-86, follows a three-step process:

1. Identifying Potential Sources: This involves recognizing and logging all locations where relevant digital evidence might reside. These locations typically include desktops, laptops, servers, external storage devices, volatile data residing in system memory, and potential external sources like network traffic logs or ISP records.

2. Developing a Data Acquisition Plan: Analysts prioritize potential sources based on three key factors:

- Likely Value: This involves estimating the potential relevance of a data source to the investigation. Analysts consider their understanding of the situation and experience to prioritize sources likely to contain crucial evidence.
- Volatility: Volatile data, such as RAM content, is lost when a system shuts down. The Collection phase emphasizes acquiring volatile data first due to its fleeting nature. Like hard drives, non-volatile data is prioritized based on its potential evidentiary value.
- Effort Required: This considers the resources needed to acquire data from different sources. Factors like analyst time, legal hurdles, and specialized equipment costs all play a role. The Collection phase aims to balance prioritizing valuable data and minimizing the effort required for acquisition.

3. Acquiring the Data: The data is acquired using forensic tools after establishing a plan. Analysts typically duplicate non-volatile data sources to create a copy, while volatile data is collected directly from the system. Data integrity is verified using message digest algorithms to ensure the copy matches the original.

The No-Cloning Theorem poses a significant challenge to how digital forensics assesses evidence sources and their potential value. In classical forensics, prioritization often favors sources deemed most likely to contain relevant evidence. However, observation can irreversibly alter the system's state in quantum systems, potentially compromising the information sought (Wootters & Zurek, 2009).

Unlike classical volatility, which centers on data loss due to external factors, quantum systems introduce another layer of complexity: the inherent instability of their states. Superpositions may collapse, and entanglement links can degrade, even without direct interaction (Horodecki et al., 2009). The fragility of quantum data, particularly the inherent instability of states and the potential for entanglement degradation, demands collection strategies that preserve its most fleeting aspects.

The concept of effort required for collection takes on a new dimension in the quantum context. For quantum evidence, "effort" must also encompass the potential impact of the collection process on the integrity of the evidence (Pirandola et al., 2020). Setting up specialized facilities, implementing entanglement-sensitive techniques, or using probabilistic models might require significant investment. NIST guidelines may need revision to include protocols for carefully assessing whether the potential disruption created by a collection method outweighs its potential benefits, factoring in both the fragile nature of quantum evidence and the investigative needs for a particular case.

In the second phase, **Examination**, the NIST SP 800-86 framework prioritizes extracting relevant information while maintaining the integrity of collected data (Kent et al., 2006). The boundaries between "observation" and "tampering" can become less defined in quantum systems (Alléaume et al., 2014). Distinguishing whether changes observed in a quantum system result from an incident, legitimate system behavior, or the examination process presents a significant challenge for digital forensics. Traditional forensic techniques could lose accuracy without reliably establishing a "pre-incident" baseline.

Another crucial challenge lies in the interconnectedness of quantum systems through entanglement. Analyzing one component of an entangled system can have cascading effects, collapsing states in connected parts and potentially destroying evidence beyond the immediate area of focus (Horodecki et al., 2009). This concept of isolating evidence contrasts with the classical forensic assumption embedded in NIST guidelines of examining evidence without impacting other data sources. The quantum realm may necessitate a holistic approach, where analysis decisions carefully consider the potential impact on a broader network of interconnected quantum evidence.

Furthermore, the NIST approach assumes the ability to overcome obstacles like encryption to uncover the underlying "true" data. For quantum systems, decryption might necessitate actions that simultaneously destroy other valuable aspects of the quantum evidence (Szikora & Lazányi, 2022). Analyzing quantum data introduces a fundamental trade-off within the framework, where the price of accessing specific information might be the irrevocable alteration of other potentially crucial quantum data.

In the third phase, **Analysis**, the NIST SP 800-86 emphasizes concluding by analyzing extracted data, often through correlation across multiple sources and comparison against known baselines (Kent et al., 2006). By collapsing superposition states, the analysis process inherently alters the quantum-derived evidence. The inherent fragility of quantum systems may mean that each analysis step changes the system, making comparisons to a pre-analysis "baseline" problematic. Furthermore, NIST's focus on correlation among sources assumes the ability to isolate data for analysis. Entanglement, however, can make isolation impossible. Analyzing one part of an entangled system could cause state collapse in connected systems, potentially compromising evidence beyond the immediate scope of the analysis (Bengtsson & Życzkowski, 2017).

The last phase, **Reporting**, prioritizes tailoring findings for the intended audience, providing actionable insights, and addressing potential alternative explanations. Quantum evidence poses unique challenges in this phase, as legal environments often favor presentations with certainty and the assumption of independently verifiable "copies." The probabilistic nature of quantum states challenges fully reconciling it with this expectation. Measurements of a quantum system could inherently yield slightly different outcomes, and the act of observation alters the evidence itself. Quantum measurement undermines the ability to represent the "original" system state at the incident's time.

Additionally, conveying the nuances of quantum concepts to non-experts like judges and juries presents a significant challenge. Explaining quantum evidence necessitates discussions of complex interactions, the theoretical basis for analysis techniques, and the inherent uncertainties involved.

The NIST SP 800-86 emphasis on addressing alternative explanations relies on comparing evidence to a known baseline or leveraging multiple forms of corroboration. Within the quantum realm, this becomes difficult. Establishing a definitive baseline may be impossible due to measurement effects. Entanglement can also complicate isolating the impact of a particular incident from a system's natural evolution or unintended alterations during the investigation.

4.1.2 ISO/IEC 27037:2012

The *International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27037:2012: Guidelines for identification, collection, acquisition and preservation of digital evidence* provides a standardized framework for handling digital evidence while safeguarding its integrity and admissibility. The rise of quantum computing introduces new complexities that could challenge established best practices within this framework. ISO/IEC 27037:2012 outlines four key sub-processes, namely: **Identification**, **Collection**, **Acquisition**, and **Preservation**.

ISO/IEC 27037:2012 classifies digital evidence as physical or logical. Quantum information, residing in qubit states influenced by their physical environment (like superconducting circuits or trapped ions (Arute et al., 2019; Cirac & Zoller, 1995)), appears primarily physical. However, due to superposition and entanglement, the information behaves like logical data; its state becomes fixed only upon observation. This duality complicates identification and handling strategies, as quantum systems may require investigators to simultaneously treat them as physical devices (quantum computers) and logical systems (state-dependent data).

The **Identification** process recognizes potential data sources, including storage and processing devices. Unfamiliarity with quantum processors, often operating in cryogenic environments (Wu et al., 2021), can hinder their identification as potential evidence sources.

The inherent volatility of quantum systems means quantum data can rapidly change or be lost entirely upon observation or interaction with the environment. Quantum states are exceptionally fragile (Zurek, 2009), and even minimal disturbances like thermal energy (heat) can introduce noise and errors. Maintaining cryogenic temperatures can help mitigate this, demonstrating that the volatility of quantum evidence vastly exceeds that of traditional digital systems. Adaptation strategies for prioritization and collection will likely be crucial. The identification phase should assess which systems likely contain the most fragile evidence when multiple quantum systems are involved. Determining volatility can be complex, as it might depend on the specific quantum state and how entanglement distributes information across systems (Erhard et al., 2020).

The prioritization process must factor in the potential for concealed quantum data arising from superposition and entanglement. These properties enable observable data in one quantum system to actively connect with potentially hidden data in other systems. This hidden data might only become accessible under specific conditions or through carefully chosen measurements. Identifying and securing this interconnected quantum evidence poses a significant challenge. In the face of techniques like quantum encryption, ensuring the integrity of such evidence will require innovative solutions (Alagic et al., 2016).

In the **Collection** phase of ISO/IEC 27037:2012, the core actions involve securing potential digital evidence sources and deciding whether to collect devices or acquire data in situ. The guideline acknowledges that devices may be powered on or powered off, requiring different approaches. Quantum devices, however, introduce a new dimension to these considerations. Unlike traditional devices, their state directly impacts the nature of the stored information (Bennett & DiVincenzo, 2000). Powering down a device or disrupting its operational setup for quantum systems could lead to the irreversible loss of volatile quantum data held within superpositions or entangled systems (similar to how information stored in Random Access Memory (RAM) disappears after powering down a traditional computer). This potential loss has significant implications for ensuring the integrity of evidence.

The Collection phase outlines procedures for documenting the acquisition approach and packaging devices for transport to a controlled environment. When dealing with quantum devices, these protocols must be revised to prioritize maintaining the integrity of the quantum evidence. Quantum systems often require highly specialized environments to preserve their operational states. New protocols are needed to prevent decoherence (Schlosshauer, 2019) or the loss of entanglement during physical movement. These protocols might involve specialized transportation containers or procedures to monitor and mitigate environmental disruptions.

The third phase, **Acquisition**, says potential digital evidence should be acquired "in the least intrusive manner." As previously discussed, traditional "non-intrusive" techniques might still be too invasive for a quantum system due to superposition, entanglement, and fragility. Potential adaptations include the development of simulations that predict how a system might respond to different acquisition methods (Georgescu et al., 2014). These simulations could guide investigators toward techniques predicted to have the most negligible impact. Another approach might involve indirect inference – extracting information about a quantum system without directly interacting with it (Ježek et al., 2003). Indirect inference could involve techniques that capture aspects of the system's environment to infer its state, potentially limiting the disruption caused by the investigation.

Furthermore, the ISO/IEC 27037:2012 relies on a "proven verification function" to ensure the digital evidence copy matches the original. Due to the No-Cloning Theorem, perfect copies of unknown quantum states are impossible (Wootters & Zurek, 2009). Therefore, verification

strategies must shift towards verifying only limited aspects of the quantum system that can be reliably copied or measured without significant alteration. Another approach may be using theoretical models and simulations to confirm that the acquired data is consistent with the predicted behavior of the original system, potentially providing a form of indirect verification.

The last phase, **Preservation**, highlights that digital evidence, once acquired, must be protected from tampering or spoliation. Storing quantum evidence in specialized environments and real-time monitoring could help detect alterations caused by deliberate or unintentional outside influences.

4.1.3 Comparison

The emergence of quantum computing necessitates a reevaluation of existing digital forensic frameworks, as outlined in NIST SP 800-86 and ISO/IEC 27037:2012. This section presents a comparative analysis, highlighting the unique challenges quantum systems pose at each stage and suggesting potential adaptations to ensure the integrity and admissibility of digital evidence.

Collection Phase

The collection phase, as detailed in NIST SP 800-86 and ISO/IEC 27037:2012, involves identifying, prioritizing, and acquiring potential sources of digital evidence. However, the quantum realm introduces challenges related to the dual nature of quantum information, the volatility of quantum states, and the potential impact of collection on evidence integrity. These nuances necessitate adaptations in how evidence is identified, prioritized, and handled. For a detailed comparison of the collection phase challenges and potential adaptations in both frameworks, refer to Table 4.1.

Examination and Analysis Phases

NIST SP 800-86 outlines examination and analysis as separate phases, while ISO/IEC 27037:2012 focuses on minimizing intrusion during acquisition. Quantum systems blur the lines between observation and tampering, making the traditional distinction between examination and analysis less clear-cut. The interconnectedness of quantum systems through entanglement also poses challenges in isolating evidence for analysis. A comprehensive comparison of these challenges and potential adaptations for both frameworks can be found in Table 4.2.

Preservation Phase

While NIST SP 800-86 doesn't explicitly address preservation, ISO/IEC 27037:2012 highlights the importance of protecting acquired evidence from tampering. Quantum evidence, with its susceptibility to environmental influences and state changes, demands specialized environments and real-time monitoring for preservation. Quantum cryptographic techniques may also play a role in securing data integrity without disrupting quantum states. For a comparative overview of the preservation challenges and potential adaptations, refer to Table 4.3.

4.2 Qualitative Interviews

This section explores the practical implications of integrating quantum computing principles into digital forensics through qualitative interviews with experts in the field. The thesis adopts a thematic analysis approach to delve into how the unique characteristics of quantum computing, such as quantum superposition and entanglement, may revolutionize or disrupt traditional digital

Aspect	NIST SP 800-86	ISO/IEC 27037:2012	Quantum Challenges
Identification	Focuses on recognizing potential evidence sources, including both volatile and non-volatile data. Prioritization is based on the value, volatility, and effort required for acquisition.	Emphasizes the distinction between physical and logical evidence, outlining procedures for identifying and documenting potential sources of digital evidence.	Quantum information challenges the binary classification of evidence, requiring consideration of its unique dual nature as both physical (hardware) and logical (state-dependent data).
Acquisition & Handling	Details a plan for acquiring data, emphasizing the creation of forensically sound copies and the preservation of volatile data.	Outlines procedures for securing potential evidence sources, deciding on in-situ acquisition vs. device collection, and documenting the approach taken.	Quantum systems' volatility and entanglement necessitate adaptations to minimize disruption and preserve delicate quantum states during acquisition.
Additional Challenges	The No-Cloning Theorem complicates assessing evidence value and prioritizing sources. Quantum volatility (instability and entanglement degradation) necessitates collection strategies that preserve the most fleeting aspects. The effort required expands to include the potential impact on evidence integrity.	The state of a quantum device directly impacts the nature of stored information. Powering down or disrupting the setup could lead to irreversible data loss. New protocols are needed to preserve quantum states during transport and storage.	

Table 4.1: Comparison of NIST SP 800-86 and ISO/IEC 27037:2012 in the Collection Phase

Aspect	NIST SP 800-86	ISO/IEC 27037:2012	Quantum Challenges
Examination	Prioritizes extracting relevant information while maintaining data integrity.	Emphasizes acquiring digital evidence "in the least intrusive manner possible."	Quantum systems blur the line between observation and tampering. Traditional techniques may lack accuracy without a reliable pre-incident baseline. Entanglement poses challenges in isolating evidence for analysis.
Analysis	Focuses on drawing conclusions by analyzing extracted data, often through correlation and comparison with baselines. Assumes the ability to overcome obstacles like encryption.	Does not explicitly address the analysis phase, but principles of minimal intrusion and evidence integrity remain relevant.	The act of analysis alters quantum evidence due to state collapse. Correlation across entangled systems can be problematic due to potential for unintended state changes. Decryption might destroy other evidence.
Reporting	Prioritizes tailoring findings for the intended audience, providing actionable insights, and addressing alternative explanations. Relies on comparisons to a known baseline and corroboration from multiple sources.	Not explicitly addressed, but the preservation of evidence integrity is crucial for ensuring the admissibility of findings in legal proceedings.	Quantum measurement makes it difficult to represent the "original" quantum state. Explaining quantum concepts to non-experts is a challenge. Establishing baselines and isolating incident impacts can be difficult due to entanglement.

Table 4.2: Comparison of the NIST SP 800-86 and ISO/IEC 27037:2012 in the Examination and Analysis Phases

Aspect	NIST SP 800-86	ISO/IEC 27037:2012	Quantum Challenges
Preservation	Not explicitly addressed as a separate phase.	Emphasizes protecting digital evidence from tampering or spoliation after acquisition.	Quantum evidence requires specialized environments and real-time monitoring to prevent alterations due to its susceptibility to environmental influences and state changes.
Additional Notes			Quantum cryptographic techniques, such as quantum key distribution (QKD), may be necessary to secure data integrity without disrupting quantum states.

Table 4.3: Comparison of NIST SP 800-86 and ISO/IEC 27037:2012 in the Preservation Phase

forensic processes. Insights from industry experts provided a foundational understanding to guide the development of adaptations and considerations within digital forensic frameworks to accommodate the emerging quantum computing landscape.

4.2.1 Analysis of Interviews

The following subsections delve into the individual perspectives of the experts interviewed, highlighting their unique insights and experiences in navigating the evolving landscape of quantum computing and digital forensics.

Digital Forensics Academic (Netherlands)

The digital forensics academic from the Netherlands offered an insightful perspective on the integration of quantum computing with digital forensics. This academic highlighted the potential implications of quantum cryptographic methods and advanced data analysis techniques. They compared the advent of quantum computing to the transformative impact of DNA analysis in forensics, which revolutionized the ability to resolve cold cases. This analogy underscores the potential for quantum technologies to enhance digital forensics by enabling the resolution of cases previously deemed unsolvable due to limitations in existing methods.

Despite their optimism, the academic expressed a measured outlook on integrating quantum computing into forensics. They emphasized that while the tools and techniques may evolve, digital forensics' core principles and methodologies would largely remain applicable. This viewpoint aligns with technological evolution rather than a complete overhaul, suggesting that existing forensic frameworks can adapt to accommodate quantum advancements with targeted modifications.

A significant challenge noted by the academic is the judicial acceptance of quantum-derived evidence. They anticipated initial skepticism and resistance from the legal community until the reliability and validity of such evidence are thoroughly established. To address this, they advocated for clear explanations and comprehensive validation processes to aid in the admissibility of quantum evidence in legal contexts. This approach ensures that the forensic community can confidently present quantum-derived evidence bolstered by robust scientific validation.

The academic also distinguished between using quantum tools for forensic analysis and addressing crimes involving quantum computing technologies. This distinction highlights the dual challenge faced by the forensic community: updating existing tools to leverage quantum capabilities and developing new frameworks to address potential quantum-enabled crimes. This dual focus ensures that the forensic community is equipped to handle quantum technologies' opportunities and threats.

After the structured interview questions were completed, the conversation with the academic shifted toward the ethical implications of integrating quantum computing into digital forensics. This ad-hoc discussion provided valuable insights into the broader societal and ethical considerations accompanying technological advancements in this field.

The academic raised concerns about the potential for quantum computing to exacerbate existing ethical dilemmas in digital forensics, particularly around privacy and surveillance. They pointed out that the enhanced capabilities of quantum computing could enable more invasive forensic techniques, which can break advanced encryption methods and access highly sensitive personal data. This could lead to significant privacy violations if not carefully regulated and controlled.

They emphasized the need for stringent ethical guidelines and robust oversight mechanisms to ensure that the power of quantum computing is not misused. The academic advocated for developing international standards that clearly define the acceptable use of quantum technologies in forensic investigations. Such standards should prioritize protecting individual rights and ensure forensic practices align with fundamental ethical principles.

Additionally, the academic highlighted the potential for quantum computing to create disparities in forensic capabilities between different countries and organizations. Wealthier nations and well-funded organizations might gain access to advanced quantum technologies, while others may need to catch up, leading to an imbalance in forensic capabilities. This disparity could affect the fairness and equity of criminal investigations and prosecutions globally.

To address these concerns, the academic suggested fostering international collaboration and knowledge-sharing to democratize access to quantum forensic technologies. They proposed initiatives such as global research partnerships, funding programs for developing countries, and open-access educational resources to ensure that the benefits of quantum computing in digital forensics are distributed more equitably.

Moreover, the academic discussed the importance of transparency and accountability in using quantum technologies for forensic purposes. They argued that forensic practitioners and researchers should be transparent about the capabilities and limitations of quantum tools and the potential ethical risks involved. Public awareness and dialogue about these technologies can help build trust and ensure their development and use are guided by societal values and ethical considerations.

In conclusion, the ad-hoc discussion with the digital forensics academic underscored the necessity of integrating ethical considerations into the development and application of quantum computing in digital forensics. By establishing robust ethical guidelines, promoting international collaboration, and ensuring transparency, the forensic community can harness the power of quantum technologies while safeguarding individual rights and promoting justice. This holistic approach aligns with the academic's perspective on the careful and measured integration of

quantum computing into digital forensics.

Incident Response Expert (Finland)

Drawing from their experience as a senior incident responder, this interviewee provided insights into the practical realities of digital forensics and incident response. They detailed the primary artifacts (memory, disk, and network data) commonly used in forensic investigations, noting their inherent volatility and discussing how quantum computing might influence their integrity.

They highlighted the volatile nature of quantum memory and its potential implications for evidence integrity. They discussed how superposition and entanglement could alter the state of quantum memory, presenting challenges for maintaining the accuracy and reliability of digital evidence. They noted the expected inclusion of error detection and correction mechanisms in quantum systems, which are crucial for their stability and functionality.

They referenced the UK Post Office Horizon scandal (Race & Jones, 2024) to underline the importance of data integrity in legal contexts. This case involved faulty accounting software that led to wrongful prosecutions and significant financial loss, illustrating the severe consequences of data integrity issues.

They advocated for transitioning from traditional "dead box" forensics to live system forensics, acknowledging modern digital systems' growing complexity and dynamism, including those utilizing quantum computing. They suggested that targeted evidence collection, mainly focusing on the state of virtual machines or containers, could more effectively address the unique challenges posed by quantum technologies.

They also expressed concerns about hash collisions and the potential for quantum computing to compromise hashed data's integrity, which could impact the reliability of digital evidence and the security of cryptographic systems.

Overall, their interview represents a pragmatic and forward-thinking perspective, emphasizing the digital forensics community's need to evolve its methodologies and tools in response to rapid advancements in quantum computing. Their focus on data integrity, live system forensics, and the potential vulnerabilities of cryptographic techniques offers critical insights for researchers, practitioners, and policymakers as they navigate the complexities of the quantum era.

Forensic Investigator (U.K.)

The forensic investigator from the U.K. provided practical insights into the adaptations required for forensic methodologies in the context of quantum computing. They emphasized the necessity for forensic investigators to understand the principles of quantum mechanics and their implications for digital forensics. This understanding is crucial for effectively handling quantum data and mitigating the challenges posed by quantum technologies.

The investigator highlighted the potential for quantum computing to disrupt traditional evidence handling processes. They stressed the importance of continuous education and training for forensic professionals to stay abreast of technological advancements. This proactive approach ensures that forensic professionals are equipped with the knowledge and skills to address the evolving challenges of the quantum era.

They also pointed out the need for developing new forensic tools and techniques capable of handling quantum data. Collaboration between forensic experts, quantum physicists, and technologists is essential for creating robust forensic methodologies that ensure the integrity and admissibility of digital evidence in the quantum era.

After completing the structured interview questions, the discussion with the forensic investigator naturally shifted towards the cross-jurisdictional challenges posed by quantum forensics.

This ad-hoc conversation illuminated several critical issues that arise when forensic investigations involve quantum technologies across different legal and geographical jurisdictions.

The investigator emphasized that one of the significant challenges in digital forensics is the variation in legal standards and procedures across different jurisdictions. With the advent of quantum computing, these discrepancies could become even more pronounced. Quantum data, due to its highly technical nature and the complexities involved in its handling, may be subject to varying interpretations and legal requirements in different countries.

The investigator highlighted the importance of harmonizing international legal frameworks to address the unique challenges posed by quantum forensics. They suggested that international bodies, such as INTERPOL and the International Association of Computer Investigative Specialists (IACIS), could play a pivotal role in establishing standardized guidelines and best practices for handling quantum data. These guidelines would help ensure that evidence collected in one jurisdiction is admissible and reliable in another, thereby facilitating cross-border investigations.

They also discussed the potential for quantum computing to exacerbate issues related to data sovereignty and jurisdiction. Quantum data can be easily entangled and distributed across multiple locations, making it difficult to determine the precise jurisdiction in which the data resides. This situation complicates legal processes, such as obtaining warrants and subpoenas, and raises questions about which country's laws should apply to the collection and analysis of quantum evidence.

The investigator pointed out that mutual legal assistance treaties (MLATs) and other international agreements would need to be updated to address these complexities. These treaties should include provisions for the specific challenges posed by quantum data, such as the need for rapid response mechanisms to prevent the loss of volatile quantum information and the establishment of secure channels for sharing quantum evidence between jurisdictions.

Moreover, the investigator emphasized the need for enhanced collaboration and communication between forensic professionals in different countries. They suggested creating international task forces and working groups dedicated to quantum forensics. These groups could facilitate the exchange of knowledge and best practices, provide training and resources, and coordinate joint investigations involving quantum technologies.

Another significant point raised during the discussion was the potential impact of differing levels of technological advancement between countries. The investigator noted that while some countries might quickly adopt and integrate quantum technologies into their forensic practices, others might lag due to resource constraints or lack of expertise. This disparity could lead to challenges in ensuring the consistency and reliability of forensic investigations on a global scale.

To mitigate these issues, the investigator advocated for international funding and support programs to help less technologically advanced countries build their quantum forensic capabilities. These programs could include training initiatives, access to cutting-edge quantum forensic tools, and collaborative research projects aimed at developing cost-effective solutions for quantum forensics.

In conclusion, the ad-hoc discussion with the forensic investigator from the U.K. underscored the significant cross-jurisdictional challenges posed by quantum forensics. Harmonizing international legal frameworks, updating international agreements, and enhancing global collaboration are essential steps to address these challenges. By fostering a cooperative and inclusive approach, the forensic community can ensure that the advancements in quantum computing are leveraged to enhance the effectiveness and fairness of forensic investigations worldwide.

Digital Forensics Expert (Sweden)

The digital forensics expert from Sweden provided insights into the practical challenges and necessary adaptations in the field of digital forensics when dealing with quantum computing technologies. They emphasized the importance of maintaining the integrity of digital evidence and discussed the potential for quantum computing to introduce new vulnerabilities in forensic processes.

The expert highlighted the need for continuous research and development to create quantum-resistant forensic techniques that can effectively safeguard evidence integrity. This focus on R&D ensures that forensic methodologies evolve in tandem with advancements in quantum technologies, maintaining their relevance and effectiveness.

They also stressed the importance of collaboration between forensic experts and quantum physicists to develop innovative solutions addressing the unique challenges posed by quantum computing. This collaboration is crucial for bridging the gap between theoretical quantum principles and practical forensic applications.

After completing the structured interview questions, the discussion with the digital forensics expert naturally evolved to explore the role of automation and artificial intelligence (AI) in quantum forensics. This conversation revealed important considerations about how these technologies can be integrated to enhance forensic practices in the quantum era.

The expert emphasized that as quantum computing introduces greater complexity into digital forensics, the role of automation and AI will become increasingly critical. They pointed out that traditional forensic analysis, which relies heavily on manual processes, may be inadequate for handling the vast amounts of data and the intricate nature of quantum states. Automation and AI can help streamline forensic processes, making them more efficient and effective.

One of the key benefits of AI, as discussed by the expert, is its ability to identify patterns and anomalies within large datasets. Quantum forensics will likely involve analyzing massive amounts of quantum data, where patterns may not be immediately apparent to human investigators. AI algorithms can quickly sift through this data, flagging potential areas of interest and reducing the time required for analysis. This capability is particularly valuable given the transient nature of quantum states, where timely analysis is crucial.

The expert also highlighted the potential for AI to assist in developing quantum-resistant cryptographic techniques. AI can be used to simulate various attack scenarios on quantum cryptographic systems, helping researchers identify vulnerabilities and strengthen their defenses. This proactive approach can ensure that cryptographic methods remain robust against the capabilities of quantum computing.

Automation, on the other hand, can significantly enhance the efficiency of forensic processes. Automated tools can handle the routine aspects of evidence collection, preservation, and analysis, freeing up human investigators to focus on more complex tasks that require critical thinking and expertise. The expert noted that automation could also help ensure consistency and accuracy in forensic procedures, reducing the risk of human error.

However, the expert cautioned that the integration of AI and automation into quantum forensics must be approached carefully. They raised concerns about the potential for AI algorithms to introduce biases into forensic analysis. If not properly managed, these biases could affect the fairness and impartiality of forensic investigations. To mitigate this risk, the expert advocated for the development of transparent and explainable AI systems. These systems should provide clear insights into how they reach their conclusions, enabling forensic practitioners to understand and validate the results.

Furthermore, the expert discussed the need for ongoing training and education for forensic professionals to effectively utilize AI and automation tools. As these technologies evolve, it is

essential for practitioners to stay current with the latest advancements and understand how to integrate them into their workflows. This continuous learning will ensure that forensic professionals can leverage the full potential of AI and automation while maintaining the highest standards of evidence integrity and reliability.

In conclusion, the ad-hoc discussion with the digital forensics expert from Sweden underscored the transformative potential of automation and AI in the field of quantum forensics. By streamlining processes, enhancing pattern recognition, and strengthening cryptographic defenses, these technologies can significantly improve the efficiency and effectiveness of forensic investigations. However, careful implementation and ongoing education are crucial to ensure that these advancements are integrated in a way that upholds the principles of fairness, transparency, and accuracy in digital forensics.

Quantum Physicist (U.S.)

The quantum physicist from the U.S. provided a deep understanding of quantum principles and their potential impact on digital forensic processes. They discussed the fundamental differences between classical and quantum computing and the unique challenges posed by quantum data.

The physicist highlighted the principles of superposition, entanglement, and the no-cloning theorem, discussing how these quantum phenomena could disrupt not only traditional forensic methodologies, but computing in general as we know it. They emphasized the need for forensic investigators to understand these principles to effectively handle quantum data.

As the physicist was not too well aware of the digital forensics questions outlines in Appendix A, the conversation transitioned to the topic of quantum gates and other relevant quantum phenomena that provided valuable insights into the implications for digital forensics.

The physicist began by explaining the concept of quantum gates (Williams, 2011), which are the building blocks of quantum circuits, analogous to classical logic gates in conventional computing. Quantum gates manipulate qubits through operations that leverage the principles of quantum mechanics, such as superposition and entanglement. They described how quantum gates can perform complex calculations that would be infeasible for classical computers, making them powerful tools in various computational tasks.

One of the key types of quantum gates discussed was the Hadamard gate (Shepherd, 2006), which creates superposition states. By applying the Hadamard gate to a qubit, it can be placed in a superposition of both 0 and 1 simultaneously, a fundamental capability that underpins the parallelism of quantum computing. The physicist explained how understanding and utilizing such gates is crucial for any application involving quantum data, including forensics.

The physicist also highlighted the significance of the CNOT (Controlled NOT) gate, which is essential for creating entanglement between qubits. The CNOT gate operates on two qubits, entangling their states such that the state of one qubit directly influences the state of the other, regardless of the distance between them. This entanglement is a powerful resource in quantum computing but also introduces challenges for digital forensics, as entangled states must be carefully managed to avoid unintentional alterations during investigations.

Further, they discussed the role of phase shift gates, which change the relative phase between qubit states, an operation that can be critical in certain quantum algorithms. Phase shift gates, like the S and T gates, adjust the quantum state in ways that classical gates cannot, providing unique computational advantages that could be leveraged in forensic analysis if properly understood and applied.

The physicist emphasized the importance of coherence and decoherence in quantum systems. Coherence refers to the property of qubits to maintain their quantum state over time, which is essential for reliable quantum computations. However, decoherence, caused by interactions

with the environment, leads to the loss of quantum information, posing a significant challenge for maintaining the integrity of quantum data. Understanding and mitigating decoherence is crucial for preserving the reliability of quantum evidence in forensic applications.

They also introduced the concept of quantum error correction, a necessary technique to protect quantum information from errors due to decoherence and other quantum noise. Quantum error correction involves encoding quantum information in a way that allows errors to be detected and corrected without directly measuring the qubits, thus preserving their quantum state. This is particularly relevant for forensic applications where maintaining the original state of quantum evidence is critical.

Another topic of discussion was the use of quantum simulators, which can model complex quantum systems that are otherwise difficult to study experimentally. Quantum simulators could be used to test forensic methodologies in controlled environments, allowing researchers to explore how quantum systems behave under various conditions and develop techniques to handle quantum evidence more effectively.

In conclusion, the ad-hoc discussion with the quantum physicist from the U.S. underscored the fundamental relevance of quantum gates and other quantum phenomena to digital forensics. By understanding and applying the principles of quantum gates, superposition, entanglement, coherence, decoherence, and quantum error correction, the forensic community can better navigate the challenges and opportunities presented by quantum computing. This knowledge is essential for developing robust forensic methodologies that can effectively handle the complexities of quantum data, ensuring the integrity and reliability of digital evidence in the quantum era.

4.2.2 Thematic Summary

The interviews reveal a shared understanding among experts that quantum computing will profoundly transform the field of digital forensics. While acknowledging the potential of quantum computing to revolutionize data analysis and decryption, they also underscore the need for thoughtful adaptation and cautious integration.

Key themes that emerged from the interviews include:

1. **Evolution of Forensic Frameworks:** All experts agree that current forensic standards and practices must evolve to address the unique challenges and opportunities presented by quantum computing. This includes adapting chain of custody protocols, ensuring the reproducibility of results, and developing new tools and techniques tailored for quantum environments.

2. **Data Integrity and Evidence Admissibility:** The experts express concerns about quantum computing's potential impact on data integrity, especially due to the volatility of quantum memory. They stress the importance of maintaining the reliability and admissibility of digital evidence in legal proceedings.

3. **Shift Towards Live-System Forensics:** A consensus emerges among the experts that a shift towards live-system forensic approaches may be necessary to effectively investigate the dynamic nature of quantum computing environments. This would involve moving away from traditional "dead box" analysis towards more dynamic and targeted evidence collection methods.

4. **Legal and Ethical Considerations:** The experts highlight the need for careful consideration of the legal and ethical implications of quantum computing in digital forensics. This includes addressing privacy concerns, data protection, and the potential for misuse of quantum technologies.

5. **Proactive Research and Education:** The experts emphasize the importance of proactive research and education within the digital forensics community to stay ahead of the curve. This includes developing quantum-aware methodologies, investing in educational programs, and fostering collaboration between researchers and practitioners.

The insights gathered from the interviews underscore the need for ongoing adaptation, innovation, and collaboration to address the challenges posed by quantum computing and future-proof digital forensics. The emphasis on data integrity, methodological adaptation, cryptographic resilience, and multidisciplinary collaboration highlights the critical areas for further research and development in the field.

5 | Discussion

The introduction of quantum computing signals a paradigm shift in digital forensics, presenting profound challenges to the integrity and admissibility of digital evidence. This chapter synthesizes the previous sections, examining how quantum properties like superposition and entanglement directly impact the reliability and trustworthiness of evidence collected and analyzed using established methodologies. The ability of quantum computing to alter data seamlessly undermines core processes within digital forensics. This seamless data alteration necessitates fundamentally re-evaluating the techniques to secure, analyze, and preserve digital evidence.

This discussion analyzes how traditional frameworks, particularly the NIST SP 800-86 and ISO/IEC 27037:2012, may need to evolve to address the unprecedented challenges arising from quantum systems. The focus will be on specific quantum characteristics—such as the No-Cloning Theorem, which prevents conventional data duplication and verification—that disrupt standard forensic practices. These challenges highlight an urgent need for practical forensic adaptations to ensure digital evidence integrity in the face of rapid technological advancements.

Furthermore, the implications of these quantum-induced challenges extend into revised training, policy-making, and the execution of forensic processes. This chapter bridges the gap between quantum computing's theoretical disruptions and the tangible adaptations required to protect digital evidence's reliability and legal standing. The following sections explore the specific challenges posed by quantum computing, propose strategic modifications to forensic practices, and discuss broader implications for policy and digital forensics.

5.1 Analysis of Quantum-Specific Challenges

Quantum computing introduces several challenges threatening the integrity of digital evidence collected and analyzed using traditional forensic methods. The core principles of quantum mechanics, such as superposition, entanglement, and the no-cloning theorem, directly impact the reliability of evidence collected and its ability to withstand legal scrutiny. Superposition, where quantum bits (qubits) exist in multiple states simultaneously until measured, complicates determining the "original" state of evidence at the time of an incident. Observation or measurement can irreversibly change quantum data, making it difficult to establish an uncompromised baseline against which to assess alterations.

Entanglement further compromises evidence integrity. This phenomenon links the state of qubits across distances such that changes to one can instantaneously alter others. Analyzing a single entangled qubit may inadvertently modify data on connected devices, potentially obfuscating the investigation's scope and impacting evidence on multiple systems. This interconnectedness undermines the standard forensic assumption that investigators can isolate evidence for examination without influencing other data sources.

The no-cloning theorem prohibits creating identical copies of unknown quantum states. This

theorem directly challenges the cornerstone of digital forensics—the ability to duplicate evidence, ensuring the original remains unaltered for verification or re-examination. Forensic analysts must develop new data verification and validation approaches when exact, independent copies are impossible.

Adapting to the challenges posed by quantum computing necessitates technological innovation and shifts in the conceptual frameworks and procedural standards focused on preserving evidence integrity. Significant barriers include a need for quantum-aware forensic tools and expertise, quantum technology evolving faster than standardization efforts, and the inherent complexity of quantum data systems. Additionally, the existing legal frameworks governing digital evidence may not adequately address the nuances of quantum alterations, requiring policy revisions and legal discussions to ensure the continued admissibility of digital evidence in the quantum era.

5.2 Proposed Adaptations to Forensic Methodologies

The quantum-specific challenges identified earlier demand adaptations in forensic methodologies to counteract threats to digital evidence integrity. This adaptation process encompasses technological innovations, revised methods, and a comprehensive approach to training and education to maintain the reliability and admissibility of digital evidence in the quantum era.

5.2.1 Potential Adaptations of NIST SP 800-86

Adapting the NIST SP 800-86 **Collection** phase for quantum computing necessitates a move away from maximizing information gain and towards minimizing information loss. Due to the No-Cloning Theorem, traditional assessments focused on copying potential sources of evidence become less relevant in the quantum realm. Since any observation alters quantum information (Nielsen & Chuang, 2010), the primary goal becomes maximizing the integrity of preserved quantum information. Instead of direct duplication, the focus might shift toward theoretical simulations that predict how a quantum system will react to different measurement techniques. While these simulations might not fully capture the system's state, they could guide investigators toward choices that prioritize preserving the most crucial aspects of the quantum evidence for the given investigation.

Quantum systems could necessitate a rethinking of volatility. "Quantum-safe" storage may be required to preserve the fragile coherence and entanglement relationships of collected evidence (Preskill, 1998). The development of quantum-safe storage introduces an active element to evidence preservation. Real-time analysis tools integrated with collection could help extract information before superposition states collapse or entanglement degrades.

Cost/benefit analysis must incorporate the potential impact of the collection process itself on the integrity of quantum evidence. Addressing these concerns requires tools to assess the predicted disruption caused by a specific collection technique, quantifying the possibility of superposition collapse and the spread of entanglement effects. The adapted NIST framework might prioritize less invasive techniques in sensitive cases where maximum preservation of the original quantum state is critical.

Beyond technical adaptations, the Collection phase will require significant shifts in training and infrastructure to ensure digital evidence integrity. Collaboration between digital forensics experts and quantum physicists becomes essential. Training programs must focus on understanding quantum principles and developing minimally disruptive collection techniques to limit alterations to quantum evidence (Ekert, 1991). Additionally, investments in "quantum-aware" forensic facilities are crucial. These facilities should minimize environmental interactions and provide

controlled settings vital to examining quantum evidence. Finally, proactive legal discussions must address how to document and ensure the integrity of evidence when the original state is inherently uncertain, and each interaction introduces changes (Aaronson, 2005).

The second phase, **Examination**, might need to adapt and focus on developing a suite of "least destructive" analysis tools tailored to quantum systems. Prioritizing techniques that minimize the number of collapsed superpositions or disrupted entangled connections could become central to the adapted process.

Furthermore, determining whether changes observed in a quantum system result from an incident, legitimate system behavior, or the investigation itself presents a fundamental challenge (Alléaume et al., 2014). Techniques for determining whether system changes are due to an incident or investigative actions will be crucial. For example, employing quantum machine learning techniques that operate probabilistically without requiring complete state measurement could help identify anomalies while minimizing evidence disruption (Holevo, 2011; Liu & Rebentrost, 2018; Schuld et al., 2015). Theoretical simulations might hold another possible answer by constructing simulations of a system's likely "pre-incident" state, which could offer a comparison point for analysis, potentially aiding in attributing changes while protecting evidence integrity.

The interconnected nature of quantum systems driven by entanglement could pose a significant challenge to ensuring digital evidence integrity. A holistic approach becomes necessary, where investigators must carefully consider the potential impact of examination steps on the broader network of interconnected quantum evidence (Horodecki et al., 2009). Developing specialized forensic tools that operate probabilistically could be vital, as these tools would minimize uncertainty propagation during analysis.

Moreover, the fragility of quantum states may force difficult trade-offs. While the NIST framework assumes that the Examination phase "may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption, and access control mechanisms," investigators may irreversibly alter other valuable evidence when attempting such actions with quantum systems (Szikora & Lazányi, 2022). Developing protocols for determining when it is preferable to leave quantum data undisturbed, extracting only fragments of information obtainable without further compromising the system, could become a core component of adapted investigative models.

In the **Analysis** phase, Kent et al. (2006) prioritizes concluding correlation and comparison against established baselines. In quantum systems, superposition makes the concept of a single "true" baseline problematic. As previously discussed, analyzing the evidence could alter it (Nielsen & Chuang, 2010). Therefore, adaptation strategies should prioritize understanding and documenting the impact of each analysis choice on the broader quantum system's state.

The fragility of quantum states could even introduce trade-offs during Analysis. Since superposition allows a single quantum system to hold multiple potential outcomes, investigators might need to choose between obtaining specific information (collapsing other potential states) or forgoing that data to preserve the possibility of uncovering different insights later. Adaptations to the NIST framework might include developing analysis protocols that guide investigators in weighing these trade-offs. These protocols should emphasize justifying choices in a way that safeguards the integrity of the investigation and the digital evidence itself.

Entanglement further complicates the analysis phase (Bengtsson & Życzkowski, 2017). The ability to isolate and correlate evidence, as emphasized in classic frameworks, becomes less feasible when analyzing entangled systems, and analyzing one aspect risks unintended alterations in connected parts of the entangled network. Adaptations could focus on developing tools to track how analysis choices propagate through these networks. Additionally, integrating quantum error-correction techniques could help mitigate alterations caused by investigative tools, aiming to preserve the integrity of the overall system during analysis (Calderbank & Shor, 1996).

Quantum error correction, a technique designed to protect quantum information from errors due to decoherence and other quantum noise (Devitt et al., 2013), could be instrumental in preserving the integrity of digital evidence during the analysis phase. By encoding quantum information redundantly across multiple qubits, quantum error correction can detect and correct errors without directly measuring the qubits, thus avoiding the collapse of their quantum states. This approach could be particularly valuable in forensic investigations where maintaining the original state of quantum evidence is paramount.

A core challenge in the **Reporting** phase stems from the mismatch between legal expectations of certainty and the inherent uncertainty of quantum evidence. Since quantum states cannot be perfectly cloned or definitively measured without introducing change, the evidence presented will carry a degree of uncertainty. Successful adaptation likely necessitates proactive collaboration between quantum experts and legal bodies to establish new admissibility standards (Yeboah-Ofori & Brown, 2020). Developing methods to quantify the uncertainties associated with quantum evidence and establish reliability thresholds for its legal presentation may be crucial for its admissibility in court.

The Reporting phase presents a challenge in effectively communicating quantum concepts in the courtroom. Innovative visualization techniques or analogies could help judges and juries understand the probabilistic nature of quantum evidence without demanding specialized knowledge. Additionally, emphasizing the rigorous theoretical basis of investigative techniques and justifying each procedural choice can establish confidence in the conclusions' reliability, even when absolute certainty about the evidence is unattainable.

5.2.2 Potential Adaptations of ISO/IEC 27037:2012

In adapting ISO/IEC 27037:2012 for quantum computing, specifically during the **Identification** phase, distinct challenges arise due to the unique nature of quantum information systems. Identifying quantum systems potentially containing relevant digital evidence will demand the development of specialized protocols and potentially new tools. Investigators must design protocols that minimize interactions that could destabilize fragile quantum states or unintentionally modify them through observation.

The inherent volatility and potential for entanglement mean that identification strategies must acknowledge the unique behavior of quantum systems. Developing methods to assess the stability and fragility of a quantum state rapidly can help investigators prioritize evidence handling and minimize the risk of state collapse (Suter & Álvarez, 2016). Additionally, recognizing entanglement as a core feature of quantum systems will necessitate a more holistic approach to evidence assessment. Identifying one part of a system might highlight the potential existence of related, interconnected data and guide investigative efforts accordingly.

To address the challenges posed by quantum data's fragility and interconnected nature, investigators might need to rethink how they categorize such data within existing digital forensic models. Creating new categories that distinguish between highly volatile quantum data and more stable forms could contribute to developing more nuanced forensic procedures and ensure that the most at-risk data is prioritized and handled carefully.

The development of specialized tools for the Identification phase becomes essential for interacting with quantum systems in a manner that minimizes the risk of alteration. These tools might utilize techniques adapted from quantum research, such as non-demolition measurements, tailored for forensic purposes.

Addressing the **Collection** phase within the ISO/IEC 27037:2012 framework requires careful consideration of the unique properties of quantum systems. The fragility of quantum information, its potential volatility, and the interconnectedness introduced by entanglement necessitate adapting

existing methodologies and technical tools to ensure the integrity of collected evidence.

One such adaptation could be minimizing the time between acquiring quantum evidence and placing it in a controlled environment. Developing specialized portable units to maintain the conditions necessary to preserve coherence and protect entanglement links (Streltsov et al., 2015) could be a key solution for minimizing the time between acquiring quantum evidence and placing it in a controlled environment. These units might utilize cryogenic cooling, vibration isolation, or other techniques necessary to protect the integrity of the specific quantum system involved.

Furthermore, developing in-situ acquisition techniques that minimize disruption to the quantum system is essential. Developing specialized tools for non-destructive interaction with quantum systems could utilize techniques like quantum non-demolition (QND) measurements in quantum optics systems (Grangier et al., 1998). A QND measurement allows for extracting information about a quantum system's observable (a property like position, momentum, or photon number) without destroying the information contained in that observable. Instead of directly measuring the quantum system, one measures the changes imprinted on the light beam. These changes encode information about the observable. The emphasis would be on acquiring information or creating partial duplicates in ways that minimize the impact on the overall quantum state of the evidence, thus protecting the evidence's integrity.

However, some researchers try to minimize disruptions in quantum information by designing topological quantum computers, which aim to encode information in special materials whose properties make them inherently resistant to errors (Nayak et al., 2008). The idea is that disturbances have a hard time causing lasting damage to the encoded quantum information. This field is still relatively young, but it represents a promising path toward fault-tolerant quantum computation, which could aid in protecting the integrity of quantum digital evidence.

Additionally, the ability to quickly assess the environmental factors that might impact the integrity of quantum evidence is essential. Tools that measure electromagnetic interference (Olariu & Popescu, 1985), temperature fluctuations (Ourabah & Tribeche, 2017), or other potential sources of instability could inform necessary precautions or adjustments to collection procedures.

The third phase, **Acquisition**, follows many adaptations as its NIST SP 800-86 counterpart, Analysis. Quantum systems are sensitive to interaction and fundamentally resist traditional data acquisition methods because of quantum mechanics' intrinsic properties. In order to adapt, it is essential to refine the acquisition process in ways that acknowledge these properties without causing significant disruption.

First, one could consider enhancing indirect inference techniques and their applications. For instance, quantum tomography (O'Donnell & Wright, 2016), which reconstructs quantum states without directly measuring them, could help preserve the quantum system's state during the acquisition phase, addressing the principle of minimal intrusion cited in ISO/IEC 27037:2012.

Additionally, the No-Cloning Theorem might necessitate establishing alternative verification methods, as it prevents the creation of identical quantum state copies (Wootters & Zurek, 1982). One possible adaptation could be the utilization of quantum witness states (Eisert et al., 2007; Ollivier et al., 2004), which provide a sort of "fingerprint" of the quantum state without requiring a complete state duplication. This approach could align with the standard's requirement for a proven verification function by providing a method to verify the integrity of the quantum information collected without fully replicating it.

Lastly, the **Preservation** phase. Given that quantum systems are highly susceptible to environmental influences and observation-induced state changes, it is essential to create an ultra-secure environment to preserve quantum evidence. The isolation of quantum data should extend beyond physical security to include quantum cryptographic techniques that ensure data integrity without disrupting the quantum system's state. Preserving quantum evidence could involve innovative uses of quantum key distribution (QKD) to encrypt and authenticate data,

providing a dual function of security and minimal interaction (Alléaume et al., 2014; Broadbent & Schaffner, 2016; Wei et al., 2023).

The design of real-time monitoring systems for quantum evidence must focus on detecting and preventing tampering or environmental interference (Sasaki et al., 2014; Williams et al., 2016). Such systems could employ quantum sensors sensitive to minor physical changes (Degen et al., 2017), enabling immediate response to potential threats to data integrity. These sensors must operate under the principle of minimal quantum measurement to avoid collapsing the system's quantum state unnecessarily. The development of quantum-proof seals (Williams et al., 2016) could also be beneficial for detecting tampering of digital evidence materials. These seals leverage the fragility of quantum states and the principles of quantum entanglement. Any attempt to intercept or modify the quantum states involved in the seal would fundamentally alter their properties, leading to detectable changes that signal tampering.

Additionally, preserving quantum coherence and entanglement requires the development of novel storage technologies that can maintain these quantum properties over extended periods. Advances in quantum memory technologies that use optically trapped atoms (Chuu et al., 2008; Specht et al., 2011) or ion traps (Bruzewicz et al., 2019; Harty et al., 2014; Kielpinski et al., 2001), which have shown promise in experimental settings, could play a key role in preserving quantum coherence and entanglement.

Integrating these technologies requires a framework that allows for the constant evolution of storage and monitoring techniques as quantum technology advances. This adaptability is crucial given the rapid pace of quantum research and the emerging understanding of quantum phenomena, which may necessitate frequent updates to preservation strategies and tools.

Overall, the adaptations to the Preservation phase in the quantum context should focus on securing quantum evidence against both physical and quantum-specific threats, maintaining the integrity and coherence of quantum states, and ensuring that these states are preserved with minimal observation or interaction, thus adhering to the quantum principles outlined in existing quantum computing research.

5.2.3 Discussion of Interviewee Answers

The qualitative interviews conducted in section 4.2.1 provided significant insights into the practical implications of quantum computing on digital forensics. Interviewees highlighted several critical aspects, including the challenge of maintaining the integrity of digital evidence in quantum environments and the need for forensic tools to evolve in response to quantum capabilities. Common themes from these interviews included concerns about the speed and complexity of quantum computations, which could potentially outstrip current forensic methodologies.

The interview findings resonate with the theoretical frameworks discussed in chapters 2 and 3, where the transformative potential of quantum computing is articulated. For instance, the concept of quantum entanglement, as discussed in the literature, poses unique challenges for digital forensics, a concern echoed by our interviewees who stressed the difficulty in maintaining a chain of custody. This linkage between theoretical quantum mechanics and practical forensic concerns underscores the urgency for adaptations in forensic practices, a point similarly raised by recent publications in the field (see sections 2.1 and 4.1 for literature references).

The interviewees, whose identities have been kept confidential for privacy reasons, provided diverse perspectives that reflect the multifaceted nature of the challenges posed by quantum computing. Each interviewee brought unique insights based on their background and expertise:

1. **Digital Forensics Academic (Netherlands):** This academic emphasized the need for ongoing research to bridge the gap between theoretical quantum principles and practical forensic applications. They highlighted the importance of interdisciplinary collaboration

between quantum physicists and forensic experts to develop methodologies that can handle the peculiarities of quantum evidence. Additionally, the academic stressed the ethical implications of quantum forensics, advocating for international standards to ensure the responsible use of quantum technologies in investigations.

2. **Incident Response Expert (Finland):** This expert highlighted the volatile nature of quantum memory and its potential implications for evidence integrity. They noted that quantum systems' error detection and correction mechanisms are crucial for maintaining stability. Drawing parallels to the UK Post Office Horizon scandal, they emphasized the severe consequences of data integrity issues and the need for reliable quantum forensic tools. They also advocated for a shift towards live-system forensics to effectively investigate dynamic quantum environments.

3. **Forensic Investigator (U.K.):** The forensic investigator pointed out the necessity for continuous education and training for forensic professionals to keep pace with technological advancements. They highlighted the potential for quantum computing to disrupt traditional evidence handling processes and stressed the importance of developing new tools and techniques capable of managing quantum data. During an ad-hoc discussion, they emphasized the cross-jurisdictional challenges posed by quantum forensics, advocating for international collaboration to harmonize legal frameworks and enhance global forensic capabilities.

4. **Digital Forensics Expert (Sweden):** This expert focused on the practical challenges and necessary adaptations in the field. They emphasized the importance of maintaining evidence integrity and discussed the role of automation and artificial intelligence (AI) in enhancing forensic practices. They pointed out that AI could help identify patterns in large datasets and assist in developing quantum-resistant cryptographic techniques. The expert also stressed the importance of transparent and explainable AI systems to ensure fairness and accountability in forensic investigations.

5. **Quantum Physicist (U.S.):** The physicist provided a deep understanding of quantum principles and their potential impact on digital forensics. They discussed how quantum phenomena such as superposition, entanglement, and quantum gates could be leveraged to develop new forensic methodologies. The physicist highlighted the importance of quantum error correction and the potential of quantum simulators to test forensic techniques. They also underscored the need for forensic professionals to understand the fundamentals of quantum mechanics to effectively handle quantum data.

Based on the interview insights, several recommendations can be made for practice and policy in digital forensics:

- **Educational Programs:** Develop and integrate quantum computing fundamentals into the educational programs for forensic professionals. This will ensure that practitioners are equipped with the necessary knowledge and skills to handle quantum data and address the unique challenges posed by quantum technologies.

- **Tool Development:** Invest in research and development of forensic tools that can operate within quantum computing environments. This includes developing quantum-resistant cryptographic techniques and automation tools to enhance the efficiency and accuracy of forensic processes.

- **Policy Updates:** Update existing policies and standards to include guidelines for handling and analyzing quantum-based digital evidence. This should also involve establishing

international standards to ensure the responsible use of quantum technologies in forensic investigations.

- **Interdisciplinary Collaboration:** Foster collaboration between forensic experts, quantum physicists, and technologists to develop innovative solutions for quantum forensics. This interdisciplinary approach is crucial for bridging the gap between theoretical quantum principles and practical forensic applications.

By implementing these recommendations, the field of digital forensics can proactively address the challenges posed by quantum computing. Adopting quantum-aware methodologies will protect the integrity and admissibility of digital evidence, ensuring that forensic practices remain robust and effective in the quantum era.

5.2.4 Summary

It is evident the development of quantum-resistant forensic tools is crucial. These tools should include quantum non-demolition (QND) measurement devices (Grangier et al., 1998) that can interact with quantum systems without disrupting their states, thereby allowing for the observation of these systems without causing state collapse (Eckert et al., 2008). Additionally, innovative storage solutions that can maintain the quantum state of data over time are necessary (Preskill, 1998). These solutions must protect against both physical degradation and quantum decoherence, ensuring that quantum data remains stable and accessible for analysis when required. The use of advancements in quantum cryptography could further enhance the security of digital evidence, with quantum key distribution (QKD) systems providing a secure communication channel that is theoretically immune to eavesdropping (Broadbent & Schaffner, 2016; Mehic et al., 2020).

A noteworthy example of practical adaptation in the field comes from the work of Closser and Bou-Harb (2022), who demonstrated a live digital forensics approach on quantum mechanical computers. Their methodology centered around the manipulation and reversal of quantum computer gates (Cai et al., 2023; Miguel-Ramiro et al., 2023) to collect forensic evidence without causing the quantum state to collapse. This approach challenges previous notions that live forensics on quantum systems were unfeasible and highlights the potential for reversible quantum gates to maintain the integrity of quantum states during forensic investigations. Their work illustrates the type of innovative thinking required to develop forensic methodologies that are compatible with the nuanced dynamics of quantum computing.

Methodological adaptations are required to handle the unique properties of quantum data. New data collection protocols should explicitly address handling superposition and entanglement to minimize inadvertent alteration during acquisition. The field must move beyond traditional verification techniques, which rely on the ability to duplicate data, and possibly shift toward partial cloning or weak measurement approaches that reveal limited yet useful information without risking complete state change. Additionally, developing analysis techniques tailored to the probabilistic nature of quantum information would allow forensic analysts to derive meaningful insights while safeguarding evidence integrity.

Training and education must evolve. Quantum computing fundamentals should be integrated into the forensic science curriculum, providing both theoretical knowledge and practical skills. Ongoing training programs for existing forensic professionals are vital to maintaining updated knowledge in the face of rapid quantum computing advancements. These programs should prioritize the latest tools and methodologies in quantum digital forensics. Finally, fostering interdisciplinary collaboration between computer scientists, quantum physicists, and forensic experts will help bridge the gap between theoretical quantum principles and practical forensic applications.

By implementing these adaptations, the field of digital forensics can proactively address challenges posed by quantum computing. Adopting quantum-aware methodologies will protect the integrity and admissibility of digital evidence, ensuring that forensic practices remain robust and effective in the quantum era.

5.3 Ethical and Societal Aspects

The integration of quantum computing into digital forensics raises significant ethical and societal implications that warrant careful consideration. The enhanced capabilities of quantum technologies could lead to more invasive forensic techniques, potentially infringing upon privacy rights if not adequately regulated. Striking a balance between leveraging quantum advancements for investigative purposes and safeguarding individual privacy is crucial. Robust ethical guidelines and stringent oversight mechanisms must be established to ensure the responsible and ethical use of quantum computing in digital forensics.

Furthermore, the democratization of quantum technologies is essential to prevent disparities in forensic capabilities between different nations and organizations. Ensuring equitable access to quantum forensic tools and knowledge is vital for upholding justice and fairness in investigations globally. International collaboration and knowledge-sharing initiatives can play a pivotal role in mitigating these disparities.

The potential societal impact of quantum forensics is vast. By enhancing the ability to analyze and interpret digital evidence, quantum computing could improve the accuracy and efficiency of investigations, leading to more just outcomes in legal proceedings. However, the misuse of quantum technologies could also have detrimental consequences, such as enabling mass surveillance or facilitating cybercrimes.

6 | Conclusion

This thesis has explored the profound implications of quantum computing on the field of digital forensics, revealing a landscape where traditional methodologies face significant challenges in preserving the integrity and admissibility of digital evidence. As quantum computing advances, it introduces capabilities that fundamentally challenge the foundations of digital forensic practices, notably through phenomena such as superposition and entanglement and constraints like the No-Cloning Theorem. These quantum properties necessitate a re-evaluation and adaptation of established forensic procedures to ensure the reliability and trustworthiness of digital evidence in the quantum era.

Through a comprehensive document analysis of recognized forensic guidelines, namely NIST SP 800-86 and ISO/IEC 27037:2012, this research has identified key vulnerabilities in current practices when confronted with quantum technologies. The analysis reveals that traditional methods, which rely on duplicating data for analysis without altering the original, are rendered obsolete in a quantum context where any measurement can irrevocably alter the state of quantum data. This necessitates developing new forensic techniques that can infer the pre-measurement state of quantum systems or employ non-destructive analysis methods. The qualitative interviews with experts in quantum computing and digital forensics further emphasized the need for a paradigm shift in forensic methodologies, advocating for the development of quantum-resistant forensic tools, adapting chain of custody protocols, and ensuring the reproducibility of results in quantum environments.

The findings of this research point towards a future where digital forensics must embrace a more dynamic and adaptive approach to address the challenges posed by quantum computing. This includes developing new tools and techniques tailored for quantum environments, establishing robust ethical guidelines, and fostering interdisciplinary collaboration between quantum physicists, forensic experts, and legal professionals. By proactively adapting to these quantum-induced complexities, the field of digital forensics can ensure that the integrity and reliability of digital evidence are maintained, upholding the principles of justice and fairness in the quantum era.

As quantum computing continues to advance at an unprecedented pace, the urgency for these adaptations becomes increasingly apparent. The future of digital forensics lies in its ability to evolve alongside quantum technologies, ensuring that the pursuit of justice remains steadfast in the face of technological disruption. This thesis serves as a call to action for the forensic community to embrace the challenges and opportunities presented by quantum computing, paving the way for a new era of quantum-aware forensic practices that can effectively navigate the complexities of the digital landscape.

6.1 Limitations and Future Work

This thesis acknowledges its inherent limitations due to the nascent stage of quantum technologies and the evolving nature of digital forensics. The primary limitation lies in the conceptual nature of the research, as practical applications of quantum computing in digital forensics are still largely theoretical. The speculative nature of some conclusions necessitates caution in their interpretation, especially given the rapidly changing technological landscape.

6.1.1 Limitations

This research is primarily conceptual due to the nascent stage of quantum technologies, where practical applications in digital forensics remain primarily theoretical. The speculative nature of some conclusions necessitates caution in interpreting findings within the rapidly evolving technological landscape. This thesis is confined to analyzing digital forensic guidelines primarily from NIST SP 800-86 and ISO/IEC 27037:2012. While providing a robust framework, these guidelines do not cover all potential scenarios or the newer quantum-specific challenges that may emerge as the technology evolves.

Furthermore, insights derived from expert interviews, though invaluable, were limited in number and could reflect subjective biases. The limited empirical testing of the proposed forensic adaptations due to the unavailability of accessible quantum computing environments also poses a significant limitation. This restricts the ability to validate the efficacy and practicality of these recommendations in real-world settings.

Acknowledging these limitations underscores the necessity for continuous research and adaptation of forensic methodologies. As the quantum computing landscape matures, future research can play a pivotal role in refining and validating forensic practices to ensure they remain practical and relevant.

6.1.2 Future Work

Future research should prioritize empirical studies to test and refine the proposed adaptations in forensic methodologies as quantum computing technology becomes more accessible. These studies are crucial for assessing the practical application and effectiveness of these adaptations in preserving evidence integrity and admissibility. Additionally, a broader analysis encompassing a wider range of digital forensic guidelines and standards would help develop a more comprehensive set of adaptations suitable for various quantum environments.

An interdisciplinary approach incorporating insights from computer science, quantum physics, and legal studies would foster a more holistic understanding of how quantum computing impacts digital forensics. Collaborative research across these disciplines is essential to address the multifaceted challenges posed by quantum technologies. Moreover, researchers should closely monitor advancements in quantum computing to continually update and refine forensic methodologies, ensuring that forensic practices remain relevant and effective in safeguarding digital evidence. This proactive focus on adapting and evolving digital forensic methodologies will prepare the field to seamlessly integrate quantum computing into digital forensic practices, maintaining evidence integrity and legal admissibility in the quantum era.

References

Aaronson, S. (2005). Limitations of quantum advice and one-way communication. *Theory of Computing*, *1*(1), 1–28. https://doi.org/10.4086/toc.2005.v001a001

Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. *Journal of the American College of Clinical Pharmacy (JACCP)*, *4*(10), 1358–1367. https://doi.org/10.1002/jac5.1441

Alagic, G., Broadbent, A., Fefferman, B., Gagliardoni, T., Schaffner, C., & St. Jules, M. (2016, November). Computational security of quantum encryption. In A. C. Nascimento & P. Barreto (Eds.), *Information theoretic security* (pp. 47–71). Springer International Publishing. https://doi.org/10.1007/978-3-319-49175-2_3

Alghamdi, M. I. (2021, December). Digital forensics in cyber security—recent trends, threats, and opportunities. In M. Sarfraz (Ed.), *Cybersecurity threats with new perspectives*. IntechOpen. https://doi.org/10.5772/intechopen.94452

Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Länger, T., Lütkenhaus, N., Monyk, C., Painchault, P., Peev, M., Poppe, A., Pornin, T., Rarity, J., Renner, R., Ribordy, G., Riguidel, M., ... Zeilinger, A. (2014). Using quantum key distribution for cryptographic purposes: A survey. *Theoretical Computer Science*, *560*, 62–81. https://doi.org/10.1016/j.tcs.2014.09.018

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., ... Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

Bassi, A., Lochan, K., Satin, S., Singh, T. P., & Ulbricht, H. (2013). Models of wave-function collapse, underlying theories, and experimental tests. *Reviews of Modern Physics*, *85*(2), 471–527. https://doi.org/10.1103/revmodphys.85.471

Bengtsson, I., & Życzkowski, K. (2017, August). *Geometry of quantum states: An introduction to quantum entanglement* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781139207010

Bennett, C. H., & DiVincenzo, D. P. (2000). Quantum information and computation. *Nature*, *404*(6775), 247–255. https://doi.org/10.1038/35005001

Bhatia, V., & Ramkumar, K. R. (2020). An efficient quantum computing technique for cracking rsa using shor's algorithm. *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, 89–94. https://doi.org/10.1109/ICCCA49541.2020.9250806

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Braun, V., & Clarke, V. (2012). Thematic analysis. American Psychological Association. https://doi.org/10.1037/13620-004

Broadbent, A., & Schaffner, C. (2016). Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, *78*(1), 351–382. https://doi.org/10.1007/s10623-015-0157-4

Bruzewicz, C. D., Chiaverini, J., McConnell, R., & Sage, J. M. (2019). Trapped-ion quantum computing: Progress and challenges. *Applied Physics Reviews*, *6*(2), 021314. https://doi.org/10.1063/1.5088164

Buckley, P., Peat, F. D., Bohm, Dirac, Heisenberg, Pattee, Penrose, Prigogine, Rosen, Rosenfeld, Somorjai, Weizsäcker, & Wheeler. (1979, December). *A question of physics: Conversations in physics and biology*. University of Toronto Press.

Cai, Z., Luan, C. .-., Ou, L., Tu, H., Yin, Z., Zhang, J. .-., & Kim, K. (2023). Entangling gates for trapped-ion quantum computation and quantum simulation. *Journal of the Korean Physical Society*, *82*(9), 882–900. https://doi.org/10.1007/s40042-023-00772-3

Calderbank, A. R., & Shor, P. W. (1996). Good quantum error-correcting codes exist. *Physical Review A*, *54*(2), 1098–1105. https://doi.org/10.1103/PhysRevA.54.1098

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–448. https://doi.org/10.3233/jcs-2003-11308

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: Complex or simple? research case examples. *Journal of Research in Nursing*, *25*(8), 652–661. https://doi.org/10.1177/1744987120927206

Cao, Y., Romero, J., Olson, J. P., Degroote, M., Johnson, P. D., Kieferová, M., Kivlichan, I. D., Menke, T., Peropadre, B., Sawaya, N. P. D., Sim, S., Veis, L., & Aspuru-Guzik, A. (2019). Quantum chemistry in the age of quantum computing. *Chemical Reviews*, *119*(19), 10856–10915. https://doi.org/10.1021/acs.chemrev.8b00803

Chan, R. (2019, January). Ibm unveils the world's first quantum computer that businesses can actually use to solve previously impossible problems. Retrieved April 21, 2024, from https://www.businessinsider.com/ibm-unveils-ibm-q-system-one-the-first-commercial-quantum-computer-2019-1

Chuu, C.-S., Strassel, T., Zhao, B., Koch, M., Chen, Y.-A., Chen, S., Yuan, Z.-S., Schmiedmayer, J., & Pan, J.-W. (2008). Quantum memory with optically trapped atoms. *Physical Review Letters*, *101*(12), 120501. https://doi.org/10.1103/PhysRevLett.101.120501

Cirac, J. I., & Zoller, P. (1995). Quantum computations with cold trapped ions. *Physical Review Letters*, *74*(20), 4091–4094. https://doi.org/10.1103/PhysRevLett.74.4091

Closser, D., & Bou-Harb, E. (2022). A live digital forensics approach for quantum mechanical computers. *Forensic Science International: Digital Investigation*, *40*, 301341. https://doi.org/10.1016/j.fsidi.2022.301341

Creswell, J. W., & Poth, C. N. (2024, January). *Qualitative inquiry and research design: Choosing among five approaches* (5th ed.). SAGE Publications, Inc.

de Braekt, R. I., Le-Khac, N.-A., Farina, J., Scanlon, M., & Kechadi, T. (2016). Increasing digital investigator availability through efficient workflow management and automation. *2016 4th International Symposium on Digital Forensic and Security (ISDFS)*, 68–73. https://doi.org/10.1109/ISDFS.2016.7473520

Degen, C. L., Reinhard, F., & Cappellaro, P. (2017). Quantum sensing. *Reviews of Modern Physics*, *89*(3), 035002. https://doi.org/10.1103/RevModPhys.89.035002

Devitt, S. J., Munro, W. J., & Nemoto, K. (2013). Quantum error correction for beginners. *Reports on Progress in Physics*, *76*(7), 076001. https://doi.org/10.1088/0034-4885/76/7/076001

Devoret, M. H., & Schoelkopf, R. J. (2013). Superconducting circuits for quantum information: An outlook. *Science*, *339*(6124), 1169–1174. https://doi.org/10.1126/science.1231930

Dral, P. O. (2020). Quantum chemistry in the age of machine learning. *The Journal of Physical Chemistry Letters*, *11*(6), 2336–2347. https://doi.org/10.1021/acs.jpclett.9b03664

Eckert, K., Romero-Isart, O., Rodriguez, M., Lewenstein, M., Polzik, E. S., & Sanpera, A. (2008). Quantum non-demolition detection of strongly correlated systems. *Nature Physics*, *4*(1), 50–54. https://doi.org/10.1038/nphys776

Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, *47*(10), 777–780. https://doi.org/10.1103/physrev.47.777

Eisert, J., Brandão, F. G. S. L., & Audenaert, K. M. R. (2007). Quantitative entanglement witnesses. *New Journal of Physics*, *9*(3), 46. https://doi.org/10.1088/1367-2630/9/3/046

Ekert, A. K. (1991). Quantum cryptography based on bell's theorem. *Physical Review Letters*, *67*(6), 661–663. https://doi.org/10.1103/physrevlett.67.661

Erhard, M., Krenn, M., & Zeilinger, A. (2020). Advances in high-dimensional quantum entanglement. *Nature Reviews Physics*, *2*, 365–381. https://doi.org/10.1038/s42254-020-0193-5

Ganapathy, A. (2021). Quantum computing in high frequency trading and fraud detection. *Engineering International*, *9*(2), 61–72. https://doi.org/10.18034/ei.v9i2.549

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*(Supplement), S64–S73. https://doi.org/10.1016/j.diin.2010.05.009

Georgescu, I. M., Ashhab, S., & Nori, F. (2014). Quantum simulation. *Reviews of Modern Physics*, *86*(1), 153–185. https://doi.org/10.1103/RevModPhys.86.153

Golubov, A. A., Kupriyanov, M. Y., & Il'ichev, E. (2004). The current-phase relation in josephson junctions. *Reviews of Modern Physics*, *76*(2), 411–469. https://doi.org/10.1103/RevModPhys.76.411

Grangier, P., Levenson, J. A., & Poizat, J.-P. (1998). Quantum non-demolition measurements in optics. *Nature*, *396*(6711), 537–542. https://doi.org/10.1038/25059

Griffiths, D. J., & Schroeter, D. F. (2018, August). *Introduction to quantum mechanics* (3rd ed.). Cambridge University Press. https://doi.org/10.1017/9781316995433

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, 212–219. https://doi.org/10.1145/237814.237866

Häffner, H., Roos, C., & Blatt, R. (2008). Quantum computing with trapped ions (J. Eichler, Ed.). *Physics Reports*, *469*(4), 155–203. https://doi.org/10.1016/j.physrep.2008.09.003

Harty, T. P., Allcock, D. T. C., Ballance, C. J., Guidoni, L., Janacek, H. A., Linke, N. M., Stacey, D. N., & Lucas, D. M. (2014). High-fidelity preparation, gates, memory, and readout of a trapped-ion quantum bit. *Physical Review Letters*, *113*(22), 220501. https://doi.org/10.1103/PhysRevLett.113.220501

Holevo, A. (2011, May). *Probabilistic and statistical aspects of quantum theory* (1st ed.). Edizioni della Normale Pisa. https://doi.org/10.1007/978-88-7642-378-9

Horodecki, R., Horodecki, P., Horodecki, M., & Horodecki, K. (2009). Quantum entanglement. *Reviews of Modern Physics*, *81*(2), 865–942. https://doi.org/10.1103/RevModPhys.81.865

Ježek, M., Fiurášek, J., & Hradil, Z. (2003). Quantum inference of states and processes. *Physical Review A*, *68*(1), 012305. https://doi.org/10.1103/PhysRevA.68.012305

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. https://doi.org/10.1111/jan.13031

Karie, N. M., & Venter, H. S. (2015). Taxonomy of challenges for digital forensics. *Journal of Forensic Sciences*, *60*(4), 885–893. https://doi.org/10.1111/1556-4029.12809

Kävrestad, J., Birath, M., & Clarke, N. (2024, March). What is digital forensics? In *Fundamentals of digital forensics: A guide to theory, research and applications* (pp. 3–7). Springer International Publishing. https://doi.org/10.1007/978-3-031-53649-6_1

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006, August). Guide to integrating forensic techniques into incident response. https://doi.org/10.6028/NIST.SP.800-86

Kielpinski, D., Meyer, V., Rowe, M. A., Sackett, C. A., Itano, W. M., Monroe, C., & Wineland, D. J. (2001). A decoherence-free quantum memory using trapped ions. *Science*, *291*(5506), 1013–1015. https://doi.org/10.1126/science.1057357

Kiger, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: Amee guide no. 131. *Medical Teacher*, *42*(8), 846–854. https://doi.org/10.1080/0142159X.2020.1755030

Koroniotis, N., Moustafa, N., & Sitnikova, E. (2019). Forensics and deep learning mechanisms for botnets in internet of things: A survey of challenges and solutions. *IEEE Access*, *7*, 61764–61785. https://doi.org/10.1109/ACCESS.2019.2916717

Kuzyk, M. G. (2019). Quantum no-cloning theorem and entanglement. *American Journal of Physics*, *87*(5), 325–327. https://doi.org/10.1119/1.5093815

Li, S., & Liu, P. (2020). Detection and forensics of encryption behavior of storage file and network transmission data. *IEEE Access*, *8*, 145833–145842. https://doi.org/10.1109/ACCESS.2020.3015080

Liu, N., & Rebentrost, P. (2018). Quantum machine learning for quantum anomaly detection. *Physical Review A*, *97*(4), 042315. https://doi.org/10.1103/PhysRevA.97.042315

Lyle, J. R., Guttman, B., Butler, J. M., Sauerwein, K., Reed, C., & Lloyd, C. E. (2022, May). Digital investigation techniques: A nist scientific foundation review. https://doi.org/10.6028/nist.ir.8354-draft

Maletin, N. V., Dremov, V. V., & Klebanov, I. I. (2023). On the possibility of using quantum annealers to solve problems of computational materials science. *Laser Physics Letters*, *20*(11), 115205. https://doi.org/10.1088/1612-202X/acfd8e

Maras, M.-H. (2014, February). *Computer forensics: Cybercriminals, laws, and evidence* (2nd ed.). Jones; Bartlett Publishers, Inc.

Marella, S. T., & Parisa, H. S. K. (2022, February). Introduction to quantum computing. In *Quantum computing and communications*. IntechOpen. https://doi.org/10.5772/intechopen.94103

Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C., & Voznak, M. (2020). Quantum key distribution: A networking perspective. *ACM Computing Surveys*, *53*(5), 1–41. https://doi.org/10.1145/3402192

Miguel-Ramiro, J., Shi, Z., Dellantonio, L., Chan, A., Muschik, C. A., & Dür, W. (2023). Enhancing quantum computation via superposition of quantum gates. *Physical Review A*, *108*(6), 062604. https://doi.org/10.1103/PhysRevA.108.062604

Nayak, C., Simon, S. H., Stern, A., Freedman, M., & Das Sarma, S. (2008). Non-abelian anyons and topological quantum computation. *Reviews of Modern Physics*, *80*(3), 1083–1159. https://doi.org/10.1103/RevModPhys.80.1083

Nielsen, M. A., & Chuang, I. L. (2010, December). *Quantum computation and quantum information: 10th anniversary edition*. Cambridge University Press. https://doi.org/10.1017/cbo9780511976667

O'Donnell, R., & Wright, J. (2016). Efficient quantum tomography. *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, 899–912. https://doi.org/10.1145/2897518.2897544

Olariu, S., & Popescu, I. I. (1985). The quantum effects of electromagnetic fluxes. *Reviews of Modern Physics*, *57*(2), 339–436. https://doi.org/10.1103/RevModPhys.57.339

Ollivier, H., Poulin, D., & Zurek, W. H. (2004). Objective properties from subjective quantum states: Environment as a witness. *Physical Review Letters*, *93*(22), 220401. https://doi.org/10.1103/PhysRevLett.93.220401

Ourabah, K., & Tribeche, M. (2017). Quantum entanglement and temperature fluctuations. *Physical Review E*, *95*(4), 042111. https://doi.org/10.1103/PhysRevE.95.042111

Pang, S., & Wu, S. (2010). Unambiguously determining the orthogonality of multiple quantum states. *Physical Review A*, *82*(4), 042311. https://doi.org/10.1103/PhysRevA.82.042311

Park, J. L. (1970). The concept of transition in quantum mechanics. *Foundations of Physics*, *1*(1), 23–33. https://doi.org/10.1007/bf00708652

Pichai, S. (2019, October). What our quantum computing milestone means. Retrieved May 31, 2024, from https://blog.google/technology/ai/what-our-quantum-computing-milestone-means/

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shamsul Shaari, J., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., & Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, *12*(4), 1012–1236. https://doi.org/10.1364/aop.361502

Prayudi, Y., & Sn, A. (2015). Digital chain of custody: State of the art. *International Journal of Computer Applications*, *114*(5), 1–9. https://doi.org/10.5120/19971-1856

Preskill, J. (1998). Reliable quantum computers. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, *454*(1969), 385–410. https://doi.org/10.1098/rspa.1998.0167

Race, M., & Jones, L. (2024, January). Post office scandal: The ordinary lives devastated by a faulty it system. Retrieved May 5, 2024, from https://www.bbc.com/news/business-67956962

Raghavan, S. (2013). Digital forensic research: Current state of the art. *CSI Transactions on ICT*, *1*(1), 91–114. https://doi.org/10.1007/s40012-012-0008-7

Ramadhan, R. A., Rachmat Setiawan, P., & Hariyadi, D. (2022). Digital forensic investigation for non-volatile memory architecture by hybrid evaluation based on iso/iec 27037:2012 and nist sp800-86 framework. *IT Journal Research and Development*, *6*(2), 162–168. https://doi.org/10.25299/itjrd.2022.8968

Rovelli, C. (1996). Relational quantum mechanics. *International Journal of Theoretical Physics*, *35*(8), 1637–1678. https://doi.org/10.1007/BF02302261

Sasaki, T., Yamamoto, Y., & Koashi, M. (2014). Practical quantum key distribution protocol without monitoring signal disturbance. *Nature*, *509*(7501), 475–478. https://doi.org/10.1038/nature13303

Schlosshauer, M. (2019). Quantum decoherence (A. Buchleitner, Ed.). *Physics Reports*, *831*, 1–57. https://doi.org/10.1016/j.physrep.2019.10.001

Schrödinger, E. (1935). Die gegenwärtige situation in der quantenmechanik. *Die Naturwissenschaften*, *23*(48), 807–812. https://doi.org/10.1007/bf01491891

Schuld, M., Sinayskiy, I., & Petruccione, F. (2015). An introduction to quantum machine learning. *Contemporary Physics*, *56*(2), 172–185. https://doi.org/10.1080/00107514.2014.964942

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization*, *21*(1), 1–16. https://doi.org/10.1016/j.infoandorg.2010.11.001

Shah, M., Saleem, S., & Zulqarnain, R. (2017). Protecting digital evidence integrity and preserving chain of custody. *The Journal of Digital Forensics, Security and Law*, *12*(12). https://doi.org/10.15394/jdfsl.2017.1478

Sharma, M., Choudhary, V., Bhatia, R. S., Malik, S., Raina, A., & Khandelwal, H. (2021). Leveraging the power of quantum computing for breaking rsa encryption. *Cyber-Physical Systems*, *7*(2), 73–92. https://doi.org/10.1080/23335777.2020.1811384

Shen, L. Y. L. (1972). Superconductivity of tantalum, niobium and lanthanum studied by electron tunneling: Problems of surface contamination. *AIP Conference Proceedings*, *4*(1), 31–44. https://doi.org/10.1063/1.2946195

Shepherd, D. J. (2006). On the role of hadamard gates in quantum circuits. *Quantum Information Processing*, *5*(3), 161–177. https://doi.org/10.1007/s11128-006-0023-4

Shestakova, T. P. (2020). Is the copenhagen interpretation inapplicable to quantum cosmology? *Universe*, *6*(9), 128. https://doi.org/10.3390/universe6090128

Shor, P. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134. https://doi.org/10.1109/sfcs.1994.365700

Shrimangale, V. (2024, January). Google's sycamore: Exploring the power of google's quantum computer. Retrieved April 24, 2024, from https://medium.com/@shrimangalevallabh789/googles-sycamore-exploring-the-power-of-google-s-quantum-computer-266374339d54

Sikos, L. F. (2021). Ai in digital forensics: Ontology engineering for cybercrime investigations. *WIREs Forensic Science*, *3*(3), e1394. https://doi.org/10.1002/wfs2.1394

Specht, H. P., Nölleke, C., Reiserer, A., Uphoff, M., Figueroa, E., Ritter, S., & Rempe, G. (2011). A single-atom quantum memory. *Nature*, *473*(7346), 190–193. https://doi.org/10.1038/nature09997

Stackpole, B. (2024, January). Quantum computing: What leaders need to know now. Retrieved May 28, 2024, from https://mitsloan.mit.edu/ideas-made-to-matter/quantum-computing-what-leaders-need-to-know-now

Streltsov, A., Singh, U., Dhar, H. S., Bera, M. N., & Adesso, G. (2015). Measuring quantum coherence with entanglement. *Physical Review Letters*, *115*(2), 020403. https://doi.org/10.1103/PhysRevLett.115.020403

Suter, D., & Álvarez, G. A. (2016). Colloquium: Protecting quantum information against environmental noise. *Reviews of Modern Physics*, *88*(4), 041001. https://doi.org/10.1103/RevModPhys.88.041001

Szikora, P., & Lazányi, K. (2022, September). The end of encryption? – the era of quantum computers. In T. A. Kovács, Z. Nyikes, & I. Fürstner (Eds.), *Security-related advanced technologies in critical infrastructure protection* (pp. 61–72). Springer Dordrecht. https://doi.org/10.1007/978-94-024-2174-3_5

Taddei, M. M., Escher, B. M., Davidovich, L., & de Matos Filho, R. L. (2013). Quantum speed limit for physical processes. *Physical Review Letters*, *110*(5). https://doi.org/10.1103/physrevlett.110.050402

Tavares, F. (2019, October). Google and nasa achieve quantum supremacy. Retrieved May 31, 2024, from https://www.nasa.gov/technology/computing/google-and-nasa-achieve-quantum-supremacy/

Valjarevic, A., & Venter, H. S. (2015). A comprehensive and harmonized digital forensic investigation process model. *Journal of Forensic Sciences*, *60*(6), 1467–1483. https://doi.org/10.1111/1556-4029.12823

Wang, J., Sciarrino, F., Laing, A., & Thompson, M. G. (2019). Integrated photonic quantum technologies. *Nature Photonics*, *14*(5), 273–284. https://doi.org/10.1038/s41566-019-0532-1

Wei, S., Huang, P., Wang, S., Wang, T., & Zeng, G. (2023). High-precision data acquisition for free-space continuous-variable quantum key distribution. *Optics Express*, *31*(5), 7383–7397. https://doi.org/10.1364/oe.483375

Weilbach, W. T., & Motara, Y. M. (2019). Applying distributed ledger technology to digital evidence integrity. *SAIEE Africa Research Journal*, *110*(2), 77–93. https://doi.org/10.23919/SAIEE.2019.8732798

Wholey, J. S., Hatry, H. P., & Newcomer, K. E. (2015, August). Conducting semi-structured interviews. In *Handbook of practical program evaluation* (4th ed., pp. 492–506). John Wiley & Sons.

Williams, B. P., Britt, K. A., & Humble, T. S. (2016). Tamper-indicating quantum seal. *Physical Review Applied*, *5*(1), 014001. https://doi.org/10.1103/PhysRevApplied.5.014001

Williams, C. P. (2011). Quantum gates. In *Explorations in quantum computing* (pp. 51–122). Springer London. https://doi.org/10.1007/978-1-84628-887-6_2

Wong, H. Y. (2023). *Introduction to quantum computing: From a layperson to a programmer in 30 steps* (2nd ed.). Springer Cham. https://doi.org/10.1007/978-3-031-36985-8

Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, *299*(5886), 802–803. https://doi.org/10.1038/299802a0

Wootters, W. K., & Zurek, W. H. (2009). The no-cloning theorem. *Physics Today*, *62*(2), 76–77. https://doi.org/10.1063/1.3086114

Wu, Y., Bao, W.-S., Cao, S., Chen, F., Chen, M.-C., Chen, X., Chung, T.-H., Deng, H., Du, Y., Fan, D., Gong, M., Guo, C., Guo, C., Guo, S., Han, L., Hong, L., Huang, H.-L., Huo, Y.-H., Li, L., ... Pan, J.-W. (2021). Strong quantum computational advantage using a superconducting quantum processor. *Physical Review Letters*, *127*(18), 180501. https://doi.org/10.1103/PhysRevLett.127.180501

Yeboah-Ofori, A., & Brown, A. D. (2020). Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence. *Journal of Forensic, Legal & Investigative Sciences*, *6*(1), 1–8. https://doi.org/10.24966/flis-733x/100045

Zhang, H. (2023). On the copenhagen interpretation and its alternative theories. *Theoretical and Natural Science*, *2*(1), 182–187. https://doi.org/10.54254/2753-8818/2/20220134

Zurek, W. H. (2009). Quantum darwinism. *Nature Physics*, *5*(3), 181–188. https://doi.org/10.1038/nphys1202

A | Appendix

This appendix includes the series of guiding questions intended for the semi-formal interviews with the interviewees presented in section 3.3.1.

1. "How do you see quantum computing impacting current digital forensic models and frameworks? What modifications or new approaches would be necessary to address these changes effectively?"

2. "Considering the rapid advancement in quantum technologies, what proactive steps should the digital forensics community take now to prepare for these changes? How should educational programs and policies evolve to incorporate quantum-aware methodologies?"

3. "In what ways might quantum computing affect the integrity, admissibility, and reliability of digital evidence? What measures should be implemented to ensure these aspects are maintained in quantum environments?"

4. "What key features should future digital forensic frameworks include to adequately address the challenges posed by quantum computing?"

5. "How should researchers approach the theoretical and practical aspects of adapting forensic models to incorporate quantum computing capabilities?"

6. "What policy and ethical considerations should guide the development and implementation of digital forensic practices in quantum computing environments?"