Rune Kenneth Bauge

Risks and Quality Control in Norwegian Police's Digital Forensics Process:

The Digital Forensics Examiner's Tightrope Walk

Master's thesis in Information Security
Supervisor: Lasse Øverlier
Co-supervisor: Nina Sunde
June 2023

Created by Bing Image creator - by DALL-E

NTNU
Norwegian University of
Science and Technology

Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Rune Kenneth Bauge

Risks and Quality Control in Norwegian Police's Digital Forensics Process:

The Digital Forensics Examiner's Tightrope Walk

Master’s thesis in Information Security
Supervisor: Lasse Øverlier
Co-supervisor: Nina Sunde
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Abstract

There has been an increase in the number of digital trace sources in recent times, putting digital forensic science under pressure. Factors such as rising caseloads and a shortage of specialists have resulted in the involvement of practitioners with inadequate understanding and training in the field of digital forensic processes. Simultaneously, there is a growing focus on quality assurance and quality control related to the tasks performed in this process.

The research question that this study is based on is: To what extent is quality control utilized in the digital investigation process within the Norwegian police, and what is its possible impact on reputation, legal safeguards, and trust?

To address this question, both quantitative and qualitative data collection methods were employed, including surveys and interviews. The analysis of qualitative data was conducted using thematic analysis.

The study revealed that there is limited implementation of quality control for reports documenting the work conducted, except for basic grammar and coherence checks. Time and staffing were identified as the main obstacles to the implementation of effective quality control systems. Furthermore, it became evident that many specialized tasks are currently performed by individuals without expertise in digital forensics and without a system in place to ensure the quality of their work.

The findings of the study raise concerns regarding the management of digital forensic science as a discipline within the Norwegian Police and the risk of miscarriages of justice.

Keywords:

Quality Control, Digital Forensics, Digital Forensics Process, Digital Competence, Legal Safeguards, Peer-Review, Risk, Digital Forensics Roles

Sammendrag

Det har vært en økning i antall digitale sporkilder i den senere tid, og dette har satt digital kriminalteknikk under press. Faktorer som økende saksmengder og få spesialister har ført til at flere utøvere uten tilstrekkelig forståelse og opplæring i faget deltar i de digitale kriminaltekniske prosessene. Samtidig er det et økende fokus på kvalitetssikring og kvalitetskontroll knyttet til oppgavene som utføres i denne prosessen.

Forskningsspørsmålet som denne oppgaven baserer seg på er: I hvilken grad blir kvalitetskontroll benyttet i den digitale etterforskningsprosessen innenfor norsk politi, og hva er dens mulige innvirkning på omdømme, rettssikkerhet og tillit?

For å besvare dette spørsmålet ble det gjennomført både kvantitativ og kvalitativ datainnsamling, bestående av spørreundersøkelser og intervjuer. Analysen av de kvalitative dataene ble utført ved hjelp av tematisk analyse.

Studien avdekket at det i liten grad gjennomføres kvalitetskontroll av rapporter som dokumenterer arbeidet som blir utført, bortsett fra enkel grammatikksjekk og meningskontroll. Tid og bemanning ble identifisert som de største hindringene for implementeringen av gode systemer for kvalitetskontroll. Videre ble det klart at mange spesialistoppgaver i dag blir utført av personer som ikke er spesialister på dataetterforskning, uten at det finnes et system som sikrer kvaliteten på arbeidet som utføres.

Funnene i studien gir grunn til bekymring når det gjelder forvaltningen av digital kriminalteknikk som fagområde, samt rettsikkerheten til de involverte partene.

Nøkkelord:

Kvalitetskontroll, Digital Kriminalteknikk, Digital Kriminalteknisk Prosess, Digital Kompetanse, Peer-Review, Rettssikkerhet, Risiko, Roller Innen Digital Kriminalteknikk

Acknowledgements

I would like to express my sincere gratitude to the Norwegian University of Science and Technology for providing me with an intellectually stimulating and challenging academic environment. Commencing this endeavor during the COVID-19 pandemic introduced a distinctive array of experiences and challenges, ultimately enriching my academic path.

I am immensely grateful to my supervisors, Nina Sunde and Lasse Øverlier, for their invaluable professional guidance and unwavering support. Their expertise and mentorship have played a vital role in shaping this work.

I would also like to express my gratitude to my manager, Skjalg Øverås Lied, for his support and collaboration throughout the past year. And to my section manager, Odd Arve Solvåg, I am sincerely thankful for your support, positive attitude, and willingness to help. "No" was never a word in your vocabulary. Additionally, I extend my profound appreciation to my colleagues at DPA in Western Police District, who have shouldered extra responsibilities during my absence. I am dedicated to making it up to you.

I would like to express my appreciation to Håkon Eide for his meticulous proofreading and valuable insights, which greatly improved the quality of this work.

Bjarte Moe, to whom I owe gratitude for even working in the field of digital forensics. I had not considered a career in the Police before you encouraged me to apply. Your training and guidance when I began my journey as a DF examiner have been invaluable in shaping my skills and values.

A special acknowledgment goes to the interview participants from the six police districts who generously shared their experiences, as well as to all the other 60 colleagues who took the time to participate in my survey. Your input was invaluable to the success of this research.

To Silje, my deepest gratitude goes to you for your unwavering love and support. Throughout this entire process, you have been my constant source of encouragement, allowing me to focus on this research while taking care of other aspects of our daily life. Together, we can conquer any challenge. I love you to infinity and beyond!

To my parents, who have always supported and facilitated my path, believed in me, and cheered me on.

Lastly, I want to express my gratitude to the rest of my family, with special mention to my son Adrian, for their understanding and patience during my complete absence throughout the past year. Your unwavering support has been invaluable to me.

Contents

Figures

Tables

Acronyms

DF Digital Forensics. x, xi, xiii, 1–5, 7–19, 21–28, 30–32, 36–47, 54–81, 83, 84

DFM Digital Forensics Managers. 54–72, 74–80

FEFE Joint unit for prevention, intelligence, and investigation (Norwegian: Felles enhet for forebyggende, etterretning of etterforskning. 57

GDE Geographical District Unit (Norwegian: Geografisk Driftsenhet). 57, 67

NCFI Nordic Computer Forensic Investigator. 23, 36, 37

NPUC Norwegian Police University College (Politihøgskolen). 8, 15, 16, 22, 37, 38, 74

NTNU Norges teknisk-naturvitenskapelige universitet. 26, 36

PIT Politiets IT-enhet (PIT)(English: The Polices IT unit). 65, 76

QC Quality Control. ix–xi, xiii, 3, 4, 7, 13, 17, 21–25, 28, 30–32, 35, 38–54, 56, 67, 68, 71, 73, 76–80, 83, 84, 87

Chapter 1

Introduction

The exponential growth of digital evidence in criminal investigations has created a significant capacity challenge for the Norwegian Police. Most investigations now involve at least one digital device alongside one or more internet-related sources of evidence, resulting in an increasingly complex Digital Forensics (DF) process. Despite this complexity, there is a growing trend in Norwegian law enforcement that tasks considered specialist only a few years ago are left to generalists, leading to untrained personnel being given significant responsibilities in the digital forensic process (Haraldseid, 2021; Andreassen & Andresen, 2020).

In addition to capacity challenges, there is increasing recognition of the need to ensure the quality of digital investigations carried out by the Norwegian Police. Several studies have investigated different aspects of quality in digital forensic work, including fallacies in evaluation (Erlandsen, 2019), quality assurance mechanisms (Jahren, 2020), an assessment of the reliability of DF investigations (Stoykova et al., 2022) and perceived competence during initial phases of investigations (Heitmann, 2019). The importance of addressing these capacity and quality challenges in a timely and effective manner was further emphasized by the Norwegian Office of the Auditor General, which criticized the Norwegian Police's ability to handle ICT-related crime and highlighted challenges related to competence at all levels (Riksrevisjonen, 2021).

1.1 Motivation

In my role as a DF examiner, I experience a daily struggle of trying to get those with less knowledge of the field to understand that within the field of DF, it is not as simple as pressing a few buttons in a program and expecting full answers. It poses a significant risk to all involved if one does not comprehend how the programs we employ work, their limitations, and their weaknesses.

I have an example from my early career training. While studying one of the tools I use daily, I acquired an image of the hard drive of one of my laptops that I had exclusively used when studying. I had bought it new from a local electronics store, and I remember removing the plastic from the laptop screen. When I had secured a forensic image of the laptop's hard drive, I analyzed it in the tool, checking, among other things, deleted activity and media files. I was surprised to find a series of pictures of a family I did not know amongst the media files, but I recognized the surroundings. A good portion of the images was explicit, showing the two adults in the photos in a small fishing boat on a fjord not far from where I live. As I mentioned, I had only used the laptop for schoolwork, programming, and writing assignments. The point is that I believed I knew the device's history... or so I thought. A plausible explanation for the presence of these images is that the laptop had probably been sold before and returned to the store within the 60-day open purchase offer. Still, I never got to verify this since the store had closed down. However, it made me understand the importance of validating one's findings and that one cannot equate what one finds with guilt.

Since the start, I have continuously pursued new studies and courses within the field of DF. I am constantly reminded of how little we know and how quickly our knowledge becomes outdated. At the same time, there has been a strong push from the organization around us to involve more people in tasks that have traditionally been specialist tasks without offering them adequate training. When you combine this with the level of comprehension that one encounter, the willingness to take on tasks and make judgments that one does not have the appropriate expertise to make, it frightens me.

It frightens me because, in my experience, we, as specialists, are rarely challenged regarding digital evidence. What could be the consequences for the Norwegian police's practice of DF if one cannot stand behind the conclusions and judgments in cases due to inadequate expertise or improper tool usage? It is easy to envision similar repercussions as the Call Data Records scandal in the Danish police, where over 10,000 criminal cases had to be reviewed to see if they had been affected by the discovered error (Lentz & Sunde, 2021, p.1).

I have been contacted on multiple occasions, either just before or during court proceedings, where it was discovered that the reports by investigators documenting the content analysis of digital evidence were inadequate or contained erroneous conclusions. As a result, new analyses were required to shed light on the case accurately.

1.2 Delimitations

There are several different practitioners involved in the work with digital evidence in a criminal investigation in the Norwegian police. To mention some examples, we have police patrols handling the physical seizures of digital evidence at the scene of the crime, investigators performing content analysis, and analysts conducting some data gathering from external sources, to name a few. However, this thesis is focused on the specialists employed in a digital forensic unit who have the main responsibility for the digital forensic work conducted in the investigations. This would typically be engineers and police specialists who have education and experience in the field of DF. Throughout this thesis, they are referred to as DF Examiners, and requirements for the role are described in detail in section 2.1.

1.3 Research Problem And Questions

The following research problem was defined for this thesis:

To what extent is Quality Control utilized in the digital forensics process within the Norwegian police, and what is its possible impact on reputation, legal safeguards, and trust?

The research problem arises from the lack of systematic quality assurance within DF highlighted by Jahren(2020) and the fallacies in the process of evaluating digital evidence identified by Erlandsen(2019).

In order to provide an answer to the research problem defined for this thesis, the following research questions were established. They will help identify the main objectives of the research, act as a guide for the investigation, and serve as the backbone of the thesis (Leedy & Ormrod, 2015, p.335). Specifically, the research questions aim to explore to what degree Quality Control (QC) is carried out within DF in the Norwegian police, how it is utilized, and what the role of the Digital Forensics (DF) examiner is within the DF process in the Norwegian Police.

1. What is the digital forensic examiner's role within the digital forensics process in the Norwegian police?
2. What is the extent of the digital forensic examiner's involvement and responsibilities within the digital forensics process of the Norwegian police?
3. To what extent is QC implemented and utilized within digital forensic investigations carried out by the Norwegian Police?
4. What are the perceptions of managers and employees in the Norwegian Police digital forensics units regarding the value and feasibility of implementing systematic QC measures to improve the quality and reliability of digital forensic investigations and to safeguard the rule of law?
5. What are the potential risks to the rule of law, reputation, and trust resulting from the management of digital forensics within the Norwegian Police?
6. How does the management of digital forensics in the Norwegian Police affect the quality of work within the digital forensics process?

Moreover, the study seeks to investigate how the management and QC processes affect the work within the DF process from a risk perspective. By answering these questions, the research aims to provide insights into potential risks to the rule of law, reputation, and trust resulting from the management of DF within the Norwegian police.

1.4 Understanding Of Key Concepts

This section will provide a brief introduction to key concepts and how they should be understood while reading this thesis. Other terms, such as "DF Examiner," have received broader coverage in chapter 2 and will not be discussed here.

Distinguishing digital forensics from digital investigations

Stoykova(2021, p.11) describes the difference between a digital investigation and digital forensic science as that the primary objective of a digital investigation is to fulfill information needs and test hypotheses related to the crime. In contrast, digital forensic science aims to ensure scientific validity regardless of jurisdiction.

Quality

Quality is a term that is used throughout the thesis that will have a slightly different meaning depending on the context it is used in. In this thesis, it will be used in relation to two different concepts, DF, and digital investigations.

Quality in relation to Digital Forensics

In DF, quality involves evaluating the validity and reliability of both human and tool/technology-based methods used, as well as the end result (Horsman & Sunde, 2020, pp.2). Quality can then be described as the adherence to established standards, guidelines, and best practices in DF, ensuring that all evidence collected, analyzed, and presented is reliable, valid, and legally admissible.

Quality in relation to a digital investigation

When referring to quality within an investigation, the Norwegian Director of Public Prosecutions has described the following understanding of quality.

Quality refers to meeting certain standards in the investigation and prosecution of crimes, which can be based on legal requirements, established procedures, and best practices. The quality markers in criminal proceedings include ensuring effective investigation, adequate resource utilization, high clearance rates, proper reaction, adherence to procedural requirements, sufficient efficiency, objectivity, attention to victim perspectives, trustworthiness, collaboration, appropriate editing, accessibility, and evidence retention. The quality requirement does not give way to any other requirement for the handling of criminal cases by the police and prosecution authorities. ('Nytt kvalitetsrundskriv – Riksadvokaten', n.d., p.5).

Quality management

Quality management refers to the leadership and management approach to quality. It involves establishing quality policies, goals, and processes to achieve these goals through quality planning, quality assurance, QC, and quality improvement (ISO9000, 2015, p.18).

Quality assurance

Quality assurance is a concept that focuses on building confidence that quality requirements will be fulfilled (ISO9000, 2015, p.18).

Quality Control

QC is a concept within quality management that focuses on fulfilling quality requirements (ISO9000, 2015, p.18).

Competence

Competence refers to a person's ability to apply the skills, training, education, and experience necessary to carry out their roles and responsibilities effectively. It is the responsibility of top management to provide employees with opportunities to develop the necessary competence (ISO9000, 2015, p.7).

Investigative review of seizures / Content analysis

These terms, while sometimes used interchangeably, describe the same fundamental action within the DF process: the investigator's review and assessment of the evidence contained in the processed data obtained from the seizure.

1.5 Thesis Outline

This thesis is structured as follows: In Chapter 2, the theoretical background and relevant research related to DF will be presented. In Chapter 3, the method applied in the thesis is outlined and discussed. In Chapter 4, the results from the survey and interviews will be analyzed and presented. In Chapter 5, the results will be discussed in relation to relevant theory while answering the research problem. In Chapter 6, conclusions and in Chapter 7, suggestions for future work will be presented.

Chapter 2

Background

In this chapter, I will provide the necessary background and context for my research on QC within the Norwegian DF process. I will elaborate on the main concepts that are used further in the thesis, such as risk assessment, QC, and DF, and the roles relevant to a digital investigation in Norway will be explored and presented.

Risk assessment plays a pivotal role in identifying and evaluating potential risks and hazards. By examining its principles and methodologies, I establish a foundation for understanding its significance in the context of DF within Norway. Additionally, I will give a brief introduction to the different roles relevant to a digital investigation within Norway and their official descriptions.

QC is crucial in ensuring the reliability and integrity of processes and data. I will discuss its importance in my study, focusing on how it impacts the accuracy and trustworthiness of DF practices, specifically within the Norwegian Police. Understanding the fundamental principles of DF is essential as QC within the Norwegian Police's DF units is examined.

Through the systematic exploration of these concepts, frameworks, and the associated role, my principal objective is to contribute to the comprehension and advancement of QC practices within the Norwegian DF process. Subsequent chapters will delve into empirical findings, analysis, and conclusions that augment the understanding of QC in Norwegian DF units.

A recent article by Horsman and Sunde(2022) highlighted the lack of studies describing DF risks associated with investigative practices. I will summarize previous research on the aforementioned areas, thereby highlighting the need for further knowledge where there are knowledge gaps.

2.1 Introduction To Roles Within Digital Policing In The Norwegian Police

In order to provide an understanding of the different roles described when discussing the participants within the DF process within the Norwegian Police, I will provide a brief introduction to the roles and how they are described by the National Police Directorate.

I will center on the current situation, and for a summary of the history and evolution of DF forensics within the Norwegian Police, I recommend reading Heitmann(Heitmann, 2019, pp.12-26).

The following roles are discussed in relation to the DF process. Some of them have official role descriptions and competence requirements, and other roles have no official descriptions, but the naming is commonly used within the Norwegian Police.

The Generalist (or Generalist in Norwegian)
The generalist is intended to be the main actor in the Norwegian police force. In performing their tasks, the generalist should have the competence to make comprehensive assessments, view their work in a broader societal context, and involve relevant specialized expertise and collaborators when necessary. In the field of investigation, the generalist is responsible for investigating cases (both tactically and technically) as the first unit at a crime scene, at a criminal division of a police station, or at a sheriff's office (Politidirektoratet, 2019, p.21).

Tactical investigator (or Taktisk etterforsker in Norwegian)
The tactical investigator conducts the tactical investigation in a specific criminal case (Politidirektoratet, 2019, p.19).

Specialist in investigation (or Spesialist etterforskning in Norwegian)
The specialist has primary tasks and specialized expertise within a specific field and is responsible for providing professional support in criminal investigations, as well as ensuring and contributing to high-quality investigations within their area of expertise (Politidirektoratet, 2019, p.21).

DF Examiner (or Dataetterforsker in Norwegian)
The DF examiner has the primary task of conducting digital forensic investigations, which includes identifying, securing, analyzing, and documenting electronic evidence that can shed light on and prove what has happened (Politidirektoratet, 2019, p.22).

This is the only official role within the Norwegian Police that there are defined requirements in relation to competence within DF. The requirement is that one should have the course from Norwegian Police University College (Politihøgskolen) (NPUC) Nordic Computer Forensic Investigators (NCFI) module 1 CC or equivalent in addition to at least three years of experience within the field.

The DF liaisons (or Fagkontakt in Norwegian)
The translation of the Norwegian role Fagkontakt, which in this thesis is referred to as DF liaison, can in other publications be referred to as, for example, "Professional contact." This role has not been given a formal description in the document "National role definitions with competency requirements v1.0" (Politidirektoratet, 2019). It was, however, mentioned in another document by the National Police Directorate named "Rammer og retningslinjer."

> The professional contacts are to be an advisor for own unit within digital evidence, be a professional contact between own unit and the function for digital police work, be the contact person and communicate new methods and new knowledge within digital investigation into their own unit (Heitmann, 2019, p.22, as cited in National Police Directorate)

In addition, it has not been defined any official competence requirements for the personnel given this role. To my knowledge, it exists in most of the Norwegian Police districts, but there might be differences in regard to what responsibilities are given to the personnel being assigned the role.

Çhief Investigator (or Politifaglig etterforskningsleder in Norwegian)
A Chief Investigator oversees investigations involving multiple personnel in individual cases. Collaboration with the prosecuting legal officer is crucial for effective leadership of the investigation. However, the prosecuting legal officer holds the authority to issue directives regarding the investigation's conduct in each case. The primary objective is to prioritize mechanisms that combat confirmation biases at both the group and individual levels. Moreover, the prosecuting authority must actively seek information that upholds objectivity. Efficient allocation of resources is vital, including the utilization of relevant specialist expertise when required (Politidirektoratet, 2019, p.17).

DF manager
Similar to the DF liaison, this role has not been given a formal description in the document "National role definitions with competency requirements v1.0 (Original Norwegian title: Nasjonale rolledefinisjoner med kompetansekrav v1.0" by the National Police Directorate. But unlike the DF liaison, it most probably would not be described either. This is the description I have used throughout this thesis in order to normalize the role of the managers of the DF units.

There is no common description for such a manager role within the Norwegian Police. You could expect to find Police roles such as Police Superintendent (or Politi Overbetjent in Norwegian), Assistant Chief of Police (or Politi Inspektør in Norwegian), but also as civilian roles such as chief engineer (or Sjefsingeniør in Norwegian). There are also differences in what level they are organized at in the different police districts; in some districts, they are sections, and in other districts, they are organized as units. Common for them is that they are responsible for the personnel and DF as a field of subject within the different police districts.

First responders The term "first responders" is not directly described, but it generally refers to the initial law enforcement officers who first encounter potential digital evidence. In the Norwegian police force, this would be equivalent to the officers on patrol duty (Heitmann, 2019, p.18; Flaglien, 2018, p.19).

There seems to be a lack of clear role descriptions, and this will be further examined in the context of risk and quality.

2.2 The Digital Forensic Process

The first Digital Forensics Research Workshop collectively defined the following definition for DF.

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations (Digital Forensics Research Workshop, 2001, p.16).

The term DF refers to the process of collecting, analyzing, and preserving digital evidence in a manner that is admissible in a court of law. It encompasses various specialized fields, such as network forensics, device forensics, vehicle, and Internet forensics, to mention some. Since digital evidence can be volatile and easily manipulated, it is essential to preserve the evidence using standardized forensic tools and methods. The primary objective of DF is to establish factual answers to legal problems, and DF practitioners normally follow strong standards for evidence processing, analysis, and conclusions (Årnes, 2017, pp.4-5).

Over the years, several different models have been developed to describe the DF process. These models employ various terminologies to describe the different process stages and show variations in the stages that authors have focused on.

A common aspect among all these models is their attempt to create a process description or framework for DF that aligns with the tasks mentioned in the definition of DF: preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation. They also incorporate other aspects, such as quality management and decision-making.

In the absence of a stand DF model for the Norwegian police, the model described by Flaglien(2018) was chosen as a reference model for the thesis' data collection. This model has the advantage of being relatively simple and relating to the investigative principles used in the Norwegian police. In my opinion, the strength of this model lies in its simplicity, as it allows for less time-consuming integration of interview subjects into the tasks associated with each phase. Additionally, the use of a previously employed model facilitates easier comparison of results and findings, particularly in areas of interest. However, a weakness of this model, as I see it, is that it doesn't visually account for any form of error mitigation.

There are other models available, apart from the one chosen for this study (Valjarevic & Venter, 2015; Casey, 2004; Carrier & Spafford, 2004) are a few examples of other models of the DF process. Some models provide more detailed descriptions of the DF process, offering further insights into different steps and iterations. Kohn et al.(2013) provides an account of various DF processes, including discussions on differences in terminology. Subsequently, an updated, detailed, and advanced model for the DF process is proposed. Another newer model proposed by Horsman and Sunde(2022) also considers risk management and error mitigation throughout the process.

As the model serves as the foundation for my research, I will provide a detailed description of the content of each phase as described by Flaglien and offer a summary of relevant research conducted within the Norwegian context that is directly relevant to the phases outlined in the model. The DF process is described as a 5-step iterative process where each phase can result in a repetition of the previous phases.

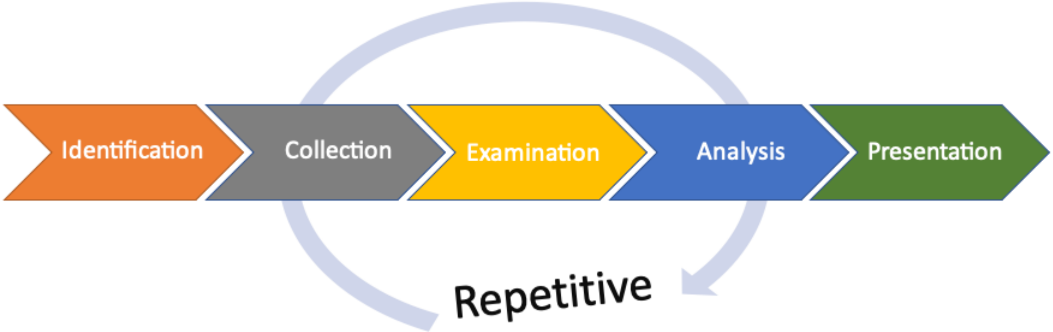


Figure 2.1: The DF process as described by (Flaglien, 2018, p.16)

Phase 1: Identification

A short description of this phase involves identifying digital sources that hold information that could be presented as evidence in a digital investigation (Flaglien, 2018).

The identification phase forms the basis for the entire digital investigation process, helping to determine what evidence or objects to look for and forming a hypothesis about what might have happened. Proper planning and preparation are essential for efficient and effective investigations. This includes having a trained team of investigators, access to resources, and an investigative infrastructure such as a lab and tools. Seizure of evidence must consider legal and ethical perspectives, and care must be taken to avoid compromising the seized evidence (Flaglien, 2018, pp.17-19).

Phase 2: Collection

This phase is defined by (Flaglien, 2018) as collecting data from digital devices to make a digital copy using forensically sound methods and techniques. In this thesis, the term *acquisition* is used to describe the task of copying data.

Forensically sound is a phrase often associated with work done in this phase of the DF process. Forensically soundness requires the forensic process used when acquiring the data to be judged reliable and appropriate. The practitioners at this stage of the process will need skills and competence to make them able to evaluate the forensic soundness of the acquisition method they choose when acquiring data from digital evidence (McKemmish, 2008, p.13).

The order of volatility is another concept that is an important part of this phase; it refers to the concept of gathering the most volatile data first, as it is likely to be changed or destroyed first. Different storage devices and media have varying data lifetimes, and data stored on disks are less volatile than data stored in memory (Flaglien, 2018, p.30).

Both the collection phase and the examination phase are in modern DF, heavily dependent on the use of tools to perform extractions or process extracted data for analysis.

Phase 3: Examination

The examination phase prepares collected data for analysis by restructuring, parsing, and preprocessing the raw data to ensure it is understandable for forensic investigators. Data and file carving techniques are often applied to identify specific patterns or signatures in file formats and extract files from the raw binary data (Flaglien, 2018, pp.33-39).

Phase 4: Analysis

This phase is defined by (Flaglien, 2018) as the processing of information that addresses the objective of the investigation to determine the facts about an event, the significance of the evidence, and the person(s) responsible. The analysis phase is a crucial component of DF, during which investigators determine the digital objects to be utilized as evidence in order to support or refute hypotheses related to a crime or incident. This phase involves the thorough analysis of data to establish factual information about an event and assess the significance of the evidence. Various techniques are employed for analysis, including the application of statistical methods, manual analysis, understanding of protocols and data formats, data mining, and timelining (Flaglien, 2018, pp.40-45).

Phase 5: Presentation

The presentation phase in DF entails documenting and presenting the results of the digital investigation to the prosecution, the court, or other pertinent audiences. The findings should be derived from an objective analysis of digital evidence. The final report should provide a summary of the investigation actions, including case information, evidence, visualizations, and findings. The documented chain of custody plays a critical role in preserving the integrity of the evidence. The presentation serves as the foundation for evaluating both the evidence and the methods employed during the investigation (Flaglien, 2018, pp.45-47).

To summarize, there is currently no standardized process model for DF work in the Norwegian police. Previous studies conducted by former Master's students have explored various aspects of the DF process. However, there is limited knowledge about the specific tasks involved in DF and the roles responsible for carrying them out.

2.3 Risk

As risk is a key aspect of my research question and a risk assessment was employed during the interviews to evaluate the Police's DF management, it is essential to introduce the specific concept of risk used in this study.

The risk involved in performing an activity lies in the potential consequences (events and effects) that can result in either a positive or negative outcome.

According to Aven and Thekdi, risk can be described as the consequence (C) of an activity and the associated uncertainties (U) (Aven & Thekdi, 2022, p.11). However, it is important to note that another definition of risk proposed by Aven and Thekdi focuses solely on the potential for undesirable consequences, which is not suitable for assessing the risk in this thesis.

When individuals perform a task, the outcome can be either successful or unsuccessful, and a decision to proceed with a task within an acceptable level of risk can lead to equally positive or negative results. This understanding aligns with the theory, which suggests that if a scientific method is used to define risk, it would be described as (C,U) (Aven & Thekdi, 2022, p.12).

2.3.1 Risk assessment methodology

A risk assessment is a process where one determines the threats that exist to a specific value and the associated risk value of that threat (Peltier, 2005, p.16). A successful risk assessment requires the participants to have an equal understanding of what values are to be reviewed, and a threat to this value would be an undesirable event that could impact the organization (Peltier, 2005, p.18).

From a management perspective, the risk is connected to the decision-making when considering tasks during the Digital Forensics (DF) process. Who does which activity, and what competence is needed to perform the action described? Risk is present at all stages of the DF process, and measures should be taken to mitigate the risks identified. (Horsman & Sunde, 2022) proposes a DF workflow model, which includes risk assessment as part of the workflow. Each step of the DF process has its own set of risks, which should be considered individually (Horsman & Sunde, 2022, p.174). Quantitative models describe risk using mathematical and statistical computations and would calculate a precise value representing the identified risk. This is a time-consuming process and would be outside this thesis's scope. But as pointed out by Horsman and Sunde(2022), a qualitative approach would be easier to use considering the complexity of DF work.

2.4 Quality Control And Peer-Review

When creating the survey and performing the interviews, the model for peer review and QC proposed in the papers by Horsman and Sunde(2020) and Sunde and Horsman(2021) was used as a starting point. This model for QC and peer review was introduced to managers and some employees at the DF units in a workshop conducted online led by Nina Sunde in the autumn of 2022, making it natural to rely on this as some of the survey participants had been introduced to it previously. This detailed model offers an opportunity to understand better the nature, extent, and practitioners involved in the current implementation of QC.

Horsman and Sunde(2020) describes the reliability of evidence in DF as crucial but challenging to achieve. Validity and reliability are essential for evidence quality, encompassing investigatory processes, practitioner interpretation, and accurate information conveyance. To enhance reliability, rigorous peer review procedures are needed, considering both technical (techniques, implementation, tool usage) and non-technical (knowledge, experience, subjectivity) error sources. Comprehensive review processes, standardized procedures, and checklists are crucial.

The Phase-oriented Advice and Review Structure (PARS) is proposed by Horsman and Sunde as a methodology for peer review, combining advice checkpoints and peer review for quality assessment and error detection. It evaluates error sources, critically evaluates peer review in DF, and offers the 'Peer Review Hierarchy' with seven levels. A structured and documentable peer review methodology is essential, including an advisory role and accountability throughout the investigation process.

Here is an overview of what each of the 7 phases in the PARS peer review process entails.

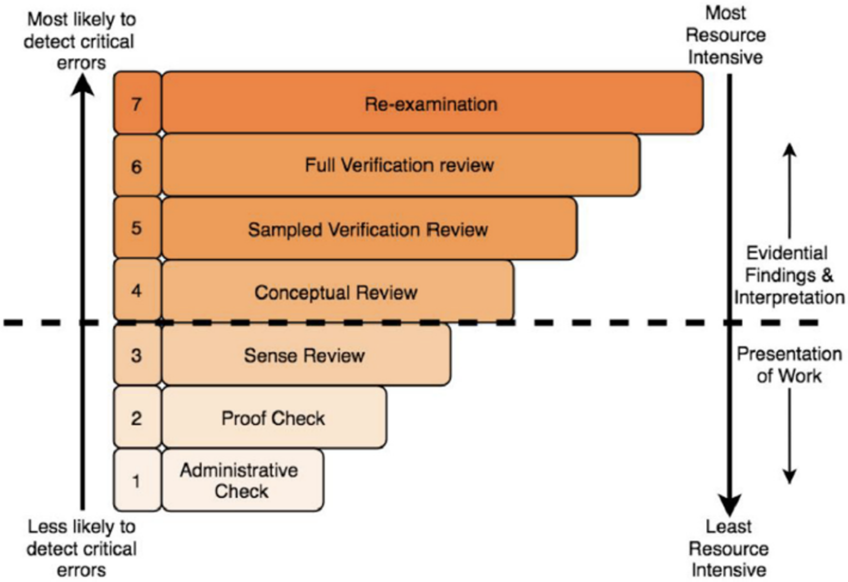

Most likely to detect critical errors
Less likely to detect critical errors
Most Resource Intensive
Least Resource Intensive
7 Re-examination
6 Full Verification review
5 Sampled Verification Review
4 Conceptual Review
3 Sense Review
2 Proof Check
1 Administrative Check
Evidential Findings & Interpretation
Presentation of Work

Figure 2.2: The "peer-review hierarchy" for DF (Horsman & Sunde, 2020, p.6)

Level 1: The 'administrative review' assesses whether the practitioner has fulfilled the required investigation, met the client's specifications, and accomplished the necessary tasks on the relevant exhibits. This review is typically a simple administrative process that can be implemented with minimal resources and time (Horsman & Sunde, 2020, pp.6-7).

Level 2: The 'Proof check' involves reviewing the report for spelling and grammatical errors. It is described as a low-labor approach that focuses on addressing grammar and spelling issues in the report (Horsman & Sunde, 2020, p.7).

Level 3: The 'Sense review' evaluates whether the report effectively presents the investigation findings in a clear and coherent manner. It focuses on ensuring the report makes sense as a piece of deliverable evidence, rather than evaluating the evidence itself. This review is a low-labor process that can be conducted with limited technical knowledge, as its primary goal is to ensure the report meets acceptable standards of clarity and organization (Horsman & Sunde, 2020, p.7).

Level 4: The 'Conceptual Review' is a thorough evaluation of the report's content, focusing on the scientific and logical foundation without verifying the findings. It examines the relationship between the evidence and conclusions, assessing the soundness of the report's conceptual aspects. Conducting a conceptual review can be resource-intensive and requires reviewers with expertise and experience equal to or greater than the principal examiner. It involves assessing evidence descriptions, interpretations, and the overall validity of the documented experimental design, methods, results, and conclusions. This level of peer review relies on professional and scientific expertise as it cannot replicate experimental methods or data (Horsman & Sunde, 2020, p.7).

Level 5: 'Sampled Verification Review' involves verifying selected findings using a different tool/method than the original examination. It helps scrutinize the practitioner's interpretation of data and identify non-technical errors. However, it may not detect technical errors before the dataset was generated. This review requires time and effort but is less burdensome than a full review and may be less robust as a peer review method (Horsman & Sunde, 2020, p.7).

Level 6: Full Verification Review involves verifying all reported results using a different tool/method than the original examination. It focuses on evaluating the practitioner's dataset and scrutinizing their interpretation of data. This process helps identify non-technical errors. However, it may lead to a slowdown in work turnover and potential bottlenecks, especially in smaller organizations with limited qualified staff for conducting verification reviews (Horsman & Sunde, 2020, p.7).

Level 7: Re-examination involves conducting a complete examination of the case by personnel who have no prior knowledge or involvement in the case. It is considered one of the most robust forms of peer review, but its implementation may be infeasible in the field of DF due to cost implications. The time and resources required for a second practitioner to examine and interpret the data make it too expensive for many organizations, leading to compromises in the review process compared to higher levels in the review hierarchy (Horsman & Sunde, 2020, p.8).

In their study, Sunde and Horsman(2021) discuss the implementation of the Phase-oriented Advice and Review Structure (PARS) model in the context of DF. The importance of peer review in the field is emphasized, and PARS is presented as a comprehensive approach to enhance the reliability of peer review. PARS consists of six stages, including peer advice, peer review, and dispute resolution. The challenges of implementing peer review for all cases are recognized, but the flexibility of PARS as a framework that can be gradually adopted is highlighted. Sunde and Horsman stresses the need for extensive knowledge in effectively reviewing digital evidence and emphasizes how PARS helps prevent errors and uphold the rule of law.

2.5 Relevant Research Conducted Within The Norwegian Context

In recent years, there has been a body of research conducted on the Norwegian Police, examining various aspects such as roles in the initial phases of digital investigations, content analysis from the perspective of investigators, challenges associated with comprehending digital evidence, and an assessment of quality assurance in digital forensics, among others. This section aims to provide a concise introduction to research conducted specifically within the Norwegian context.

The identification phase is considered a crucial part of the initial phase of a digital investigation since failure to identify a digital source could seriously impact the results of the investigation as a whole. Heitmann(2019) explored the Norwegian Police's capability to handle the initial phase of a digital investigation. Heitmann described the initial phase as part of the digital investigation that occurs until the evidence is acquired, which in the model used in this thesis would be the collection phase. The findings described in his thesis are that there are no specific requirements related to competence for police generalists who take part in a digital investigation and that police officers that graduated from NPUC before DF work became a part of the curriculum in the worst case scenario had no digital competence Heitmann, 2019, p.97.

In certain cases, Live Data Forensics is carried out in the early phase. **Live data forensics** involves the acquisition and analysis of data from a live system at the scene of a search (Andreassen & Andresen, 2020, p.37). It is a complex activity that requires personnel with proper training and encompasses various phases of the DF process (Andreassen & Andresen, 2020, pp.42, 86).

According to Andreassen and Andresen (2020), there is a lack of methods and best practices for performing live data forensics on mobile phones. Their study also revealed that some respondents, particularly students from NPUC, conducted live data forensics examinations without proper competence and adherence to methodology. This can result in the loss, alteration, or destruction of digital evidence, as well as potential errors of justice.

Haraldseid(2021) explores the analysis of digital evidence in police investigations, particularly when dealing with extensive amounts of seized data. It investigates how Norwegian investigators approach content analysis and emphasizes the need for a standardized procedure based on the investigative cycle. The study highlights the lack of research on the tactical phase of content analysis and calls for increased competence in handling digital evidence among law enforcement and prosecuting authorities.

Stoykova et al.(2022) analyzed reports from 21 randomly selected criminal cases in Norway involving digital evidence. The documentation of the digital forensic investigations was found to be insufficient, lacking consistency and compliance with methodology and standards. This made it difficult to assess the reliability of the digital evidence and establish its source. The use of screenshots and photographs for data acquisition was prevalent but not considered forensically sound. Omissions of important information about methods and tools further hindered the review and validation of the results.

In the evaluation of digital evidence by prosecutors, fallacies and errors of justice can occur due to a lack of knowledge and competence in DF (Erlandsen, 2019). Erlandsen study identified the challenges faced by prosecutors without specialized training in understanding and properly evaluating digital evidence. Concerns were raised regarding non-compliance with technical quality standards, highlighting the need for measures to address these issues and ensure accurate evaluations. The study suggests that an extraordinary focus on quality when writing reports describing digital evidence is crucial in compensating for the lack of training and competence among prosecutors (Erlandsen, 2019, p.76).

Jahren(2020) conducted a qualitative study that revealed a lack of involvement and quality management from managers in the field of DF among the participating police districts. The lack of involvement could be attributed to a lack of digital expertise among the leaders, which in turn led to individual DF examiners implementing quality assurance measures independently.

Moreover, the study indicated that management in DF demonstrated insufficient knowledge about the challenges within the field. Basic competence levels for DF examiners were deemed inadequate for ensuring the quality of digital forensic work. The limited training in tools was associated with poor economic conditions in the police districts, further exacerbating concerns related to the rule of law.

Sunde(2017) found that the combination of technological and investigative competence is often lacking in DF Examiners and investigators. Collaboration between DF examiners and investigators is crucial to prevent errors and optimize competency utilization. The absence of defined competency criteria and clear cooperation routines affects task communication, case prioritization, and timely involvement of the right competence. Additionally, large backlogs hinder the efficiency and quality of digital evidence investigations. She found that to address these challenges, detectives need sufficient technological and investigative competence while being aware of their limitations. Cooperation can be improved through routine descriptions, shared task management platforms, and a culture of challenging decisions. Organizational plans for competence development and strategic placement of DF examiners are also important. The study provided insights into non-technical sources of errors and suggested measures to enhance the quality and efficiency of digital evidence examination, thereby safeguarding the rule of law.

To summarize, there has been some research conducted in recent years on digital forensics in the Norwegian context, but there are still areas where knowledge is lacking. One such area is the role of leaders in digital forensics. The studies mentioned above focus on investigators, first responders, digital forensic technicians, and prosecution, but there is limited knowledge about the role of leaders.

Although it's limited scope, Jahren's qualitative study on QC practices in three Norwegian police districts provides valuable insights. The study revealed that QC was not performed systematically, and when conducted - it was initiated by the DF examiners themselves. The current study sets out to examine in greater detail to what extent and on which level the quality control is performed in practice by applying the PARS framework as a reference point. The study also applies a risk perspective to gain insights into the potential vulnerabilities associated with the current practices, the areas in need of improvement as well as the consequences associated with inadequate QC measures.

2.6 Relevant Research Related To Management Of Digital Forensics

In this section, I will review and present other relevant research, theories, and perspectives that may not have direct applicability to the Norwegian context but are nonetheless pertinent to the research problem addressed in this thesis.

Decentralization

When discussing how DF is managed as a field of subject, decentralization is a theme often discussed. Decentralization involves the involvement of various stakeholders in DF investigations, including not only dedicated DF examiners but also other practitioners. This decentralization might be driven by the need to address the growing workload and complexity of digital investigations. Casey(2019) describes that the decentralization of forensic science, particularly in DF, presents challenges. Limited knowledge among field personnel hinders their ability to handle the growing volume of data and technological advancements, increasing the risk of overlooking or misinterpreting digital traces. And that Police personnel lacking expertise in DF may not be aware of method limitations, resulting in errors and missed opportunities. Addressing these issues is crucial for improving the reliability of DF. The overwhelming volume of data further exacerbates these risks, neglecting potential sources of digital evidence and amplifying existing challenges in the field.

Casey et al.(2019) uses the Kodak Syndrome analogy to highlight the risks faced by forensic science laboratories that fail to adapt to decentralization. He argues that just as Kodak failed to restructure after inventing the digital camera, DF labs must recognize decentralization as a crisis and opportunity. Failure to undertake digital transformations risks obsolescence and loss of relevance.

Trust in tools

The preprocessing and automatic parsing of digital evidence during data preparation for analysis heavily relies on specialized software for interpreting digital content. However, it can be difficult to distinguish between tool usage errors and genuine tool errors. This underscores the importance of practitioners' training and competence in effectively utilizing these tools (Horsman, 2019).

Stoykova(2021) argues that examiner errors in digital forensic investigations can arise from inaccurate data examination, misinterpretation of tool results, and improper parameterization of tools. Detecting tool and method errors requires careful validation. Failing to identify limitations and errors can have serious consequences, potentially leading to the reopening of previous cases. Investigators focus on law enforcement objectives, while forensic scientists employ scientific methods and strive for impartiality. Reasoning about digital evidence, particularly when it involves data processing, involves inherent uncertainties and probabilistic inferences that require accurate examination. Furthermore, digital evidence always involves interpretation, either by the tool or the examiner.

Jones and Vidalis(2019) describes that commercially developed tools commonly used in digital forensic imaging and analysis lack independent testing, leading to concerns about their accuracy and reliability. Significant variations have been observed in the output of these tools across different versions and in comparison to alternative tools. To validate evidence, it is customary to employ dual tool verification. However, without knowledge of the underlying algorithms, there is a possibility that these tools may be self-validating, undermining the objectivity of the results. Moreover, the adoption of two tools per task increases costs and workloads for practitioners.

Standards, bias, and reporting

Several research studies have explored challenges in the practice of DF, particularly in the areas of reporting and bias. According to Casey(2018), the potential for bias among forensic experts exists, as they may present evidence in a manner that favors their clients. This poses a risk of employing inappropriate approaches that create an illusion of certainty without adequately assessing probabilities. To uphold the scientific integrity of forensic practices, it is crucial to discourage forensic practitioners from assuming an advocacy role and instead prioritize the evaluation and expression of findings based on the relative probabilities of evidence supporting various claims. Casey(2018, p.3) emphasizes the significance of transparently conveying digital forensic results, considering alternative claims, and expressing probabilities. Adhering to these principles ensures the accuracy and reliability of forensic practices and strengthens the confidence of decision-makers in digital forensic expert testimony.

Sunde and Dror (2021) describes a situation where the DF examiners' decisions are affected by bias, and their conclusions weren't consistent. The conclusion was that there was an immediate need for quality assurance mechanisms. Their analysis revealed that cognitive processes in DF are vulnerable to bias, raising concerns about the potential for human error in the field. To address this, they propose, the Hierarchy of Expert Performance framework as a tool for measuring performance and identifying susceptibility to bias.

Horsman(2021) emphasizes the importance of having common standards for constructing reports in the field of DF. And that standardization and guidance are crucial to ensure reliable and effective communication of examination results and to enhance the overall reliability of digital forensic evidence.

Differentiating between investigative activities, technical processes, and evidence evaluation is crucial for addressing quality-related issues in digital investigations. This distinction helps mitigate risks by emphasizing that individuals should not evaluate digital evidence beyond their technical expertise (Casey, 2016).

Tully et al.(2020) describes several concerns that were identified during a review of accreditation to ISO/IEC 17025 in England and Wales. These findings included issues such as a lack of systematic quality control and managers assessing employees' competence without possessing sufficient expertise to make accurate evaluations. Additionally, the importance of continuous competence building and the need for appropriate tools are emphasized. Their findings provide evidence for the necessity of robust systems that effectively uphold quality standards.

Chapter 3

Methodology

3.1 Introduction

This chapter outlines and justifies the research methodology employed in this thesis. Its primary objective is to give the reader a sufficient understanding of the methodology, including its strengths and limitations.

3.2 Research Methodology

When I started planning the thesis, it became clear that I needed insight into the attitude toward quality assurance and the extent to which it was carried out. I needed data from the practitioners themselves; a quantitative approach was selected. Since I also wanted to look into the management of DF from a risk perspective, I decided also to use a qualitative approach and interview managers within the DF units in the Norwegian Police.

The aim of the study was to utilize a quantitative approach to acquire information about the QC practices adopted by digital policing units within the Norwegian police, with sufficient data to enable generalization on the subject matter. To gain a more comprehensive understanding of the issues discussed, a qualitative methodology was employed. This approach constitutes a mixed-methods design, which may be comparable to an explanatory design (Leedy & Ormrod, 2015, p.331).

3.2.1 Background and bias

Since 2014, I have been employed as a DF examiner for the Western Police District in Norway. As the forensic community within the police is relatively small, most individuals are somewhat familiar with one another. Throughout my tenure, I have maintained a strong preoccupation with the quality of work performed within the field and have been transparent about this matter. My concerns regarding objectivity and bias when presenting digital evidence were amplified by my experiences as a witness in court.

Undertaking research where colleagues are among the study participants can present challenges. On the one hand, having prior knowledge of the organization's inner workings and an understanding of how work is organized within the unit being studied can be advantageous when creating the survey and planning the interviews. On the other hand, this familiarity also increases the potential for bias in the research findings.

My perception of how the work should be organized and what focus one should have regarding quality could make me have a narrower focus than it should when designing the survey and the interview guide. To minimize any potential issues related to confirmation bias, the interview and survey were initially tested on former colleagues who possessed knowledge of the field but were not part of the study population. After conducting the initial interview test, two questions were rephrased to enhance clarity and ensure consistent answers. The feedback on the survey indicated that some terminologies used were ambiguous and required further explanation to avoid confusion. Consequently, some questions were revised and clarified for better comprehension.

Another source of bias can be my personal acquaintance with some of the interview subjects. It is possible that the participants in the interview were aware of my attitudes toward the topic being discussed, which could have influenced their responses. Additionally, my preconceived attitudes toward the participants' opinions may have affected their ability to ask appropriate follow-up questions. To mitigate these potential sources of bias, I made a concerted effort to carefully analyze the data to prevent any biases from influencing the results. In cases where there was uncertainty, I asked the participants to confirm the accuracy of the content and to clarify their intended meanings.

3.2.2 Literature Review

When the decision was made to use a mixed methodology to answer my research questions, it became clear I had to seek more profound knowledge of several topics if I should be able to design a proper survey and interview guide. Since I wanted to address the issue of how the field of DF was managed with a risk perspective, I searched for relevant risk science theory in publications, books, and through discussions with a colleague that had recently delivered a thesis on the subject. And to get an overview of what was expected of the roles that participated in the different phases of the DF process, I used official documentation from the National Police Directorate and NPUC, in addition to looking for relevant published research. Quality assurance and QC concepts were also studied to get enough knowledge about what had already been done concerning these topics within the field of DF and how it would apply to my research.

3.2.3 Quantitative method - survey

A descriptive survey is a research method suitable when acquiring information such as characteristics, attitudes, and previous experiences from a group of people (Leedy & Ormrod, 2015, p.159). The approach used to get insight into what extent QC was performed was to design a descriptive survey as a questionnaire. The survey was administered using Nettskjema.no as a delivery platform, and it was composed of closed questions. The use of closed questions enabled the identification of constant variables for measurement purposes and simplified the process of responding for the participants. Some questions were given free-text fields allowing the respondents to comment on their answers. This could be considered a mix-methodology approach since using a free-text field allowing respondents to elaborate their answers can be regarded as qualitative data. The comments could give better insight into the quantitative data and, in some cases, even point toward new interpretations of the data collected (Harland & Holey, 2011). The survey was created and distributed in Norwegian; a version translated into English is included in Appendix section C.2.

Population and sample size

I opted to design a survey that would be disseminated among managers and employees who primarily handle digital forensics-related tasks. The survey was distributed to participants working in police districts and national units. In the Norwegian Police districts, these are organized under a common name, the Digital policing unit (Norwegian: Digitalt politiarbeid), but at different levels depending on the local police districts' organizational structure. As of 1.3.2023, approximately 185 individuals (N= 185) would be part of this population. With a small population, setting up criteria for whom to sample would not make sense. It was decided to sample the DF branch, what Leedy and Ormrod(2015, p.183) describes as purposive sampling.

Bias and potential sources of error

An error was detected in question 4 of the survey distributed to the respondents. This question was exclusively presented to individuals who had a civilian background. Consequently, information on the highest completed academic degree of respondents with a police background was lost due to this error. While this error did not impact the critical components of the survey, some analyses related to education could not be performed. The error remained unnoticed during the survey testing phase.

An issue with questions 6 and 7 in the survey is that I don't allow the respondents to answer with alternatives other than the ones I have listed. If I, for example, had used this to discuss a relationship between the level of education and QC, that would have been an issue and could have resulted in a skewed analysis. Question 6 was related to continuing professional development courses for civilians within investigations and was related to a requirement presented in Politidirektoratet(2019, p.23). Question 7 was related to the NCFI program. Both questions would have provided better data if a field where the respondent could provide an alternative option had been included.

Leedy and Ormrod(2015, p.186) describes several sources of bias that one need to consider in descriptive studies. Sampling bias could be present due to the delivery method used for the survey. I want to say everyone in the selected population had an equal opportunity to participate in the survey, and in theory, they did. A link to the survey and an approval form was distributed to all the managers of DF units in the Norwegian Police. I had contacted the managers before I sent out the invite and asked them if they could help distribute the survey in their units. A few respondents were contacted directly. This could provide at least three obstacles, affecting the responses and the sample size. I had no guarantee that all the managers would distribute the survey. The fact that they had to return a form agreeing to participate could make some potential respondents postpone or even avoid answering since it would be too much of a hassle. And last, even though I distributed it to all units that had employees that had DF as part of their primary task, there might be employees at these units that do not participate in DF work but still have answered the survey. This has to be considered when analyzing the data gathered through the survey.

Instrumental bias could also be present in how the questions are presented and maybe even in the scales used for some questions. The questions are formed to give insight into a very narrow topic, and different phrasing could provide another insight. It is important to be aware that I was the one that decided which questions to include and how to phrase them when analyzing the data (Leedy & Ormrod, 2015, p.187). Many of the questions in the survey are related to QC, and this is a topic that is often confused with quality assurance. I must therefore be open to the possibility that some have answered about quality assurance and not QC. An example of a potential error source related to how a question is perceived can be discussed for question 5 in the survey. The question in Norwegian was; "Hvor mange års erfaring har du innen fagområdet digitalt politiarbeid?". If this is translated directly into English, this would be, "How many years of experience do you have within digital policing?" or "How many years of experience do you have within the DF discipline?". The wording in the Norwegian question discloses one of the biases I am affected by as one of the practitioners within the field. "Digitalt politiarbeid (Digital policing)" is a name that was introduced with the last reform within the Norwegian Police; before that, the units were known under different names. Digital policing could have a broader meaning but includes DF; some respondents might have given answers related to when this name was established and not how long they have had DF as their primary task. One must also consider response bias. Quality assurance, QC, and the quality of the work that is done within DF units have been a topic of discussion for the last few years. And there are many opinions on the subject. It is important to be aware of the possibility that respondents have an agenda when answering the way they do. The main topic of the interview and the survey had recently been discussed at different organizational levels. Most participants could have theories about what this research project could result in. This is referred to as the Hawthorne effect in (Leedy & Ormrod, 2015, p.104). Researcher bias might also be present, but this will be discussed in subsection 3.2.1.

Survey topics and type of questions

The survey was divided into three different sections.

- Demographics
- Quality Control at the respondents' workplace
- Quality Control performed within the last 12 months

Demographics

Some demography-related questions were included to get better insight and to allow for a deeper analysis. The questions were formed to gain insight into education, experience, role, and if they worked at a police district or a national unit and were presented to the users in closed form. These could provide better knowledge about who is involved in QC, their experience level, and so on. These questions were kept to a minimum with privacy in mind. The demographic questions were designed to only ask for superficial information that could contribute to a better analysis afterward. This is to avoid asking questions that could lead to respondents being identified. The survey was intended to be anonymous, and the sample was limited, which made it extra important to focus on the respondents' privacy.

Quality Control procedures at the respondent's workplace

These questions were given as closed questions, but for questions 8 to 13, the respondents were allowed to comment or elaborate on their answers. The thought was that these free-text comments could provide better insight into the topics covered by the questions. Questions 8 through 13 were given as statements where the respondents were asked to which degree they agreed with the statement on an ordinal scale (Leedy & Ormrod, 2015, p.111). The following ordinal scale was used.

- Completely agree
- Partly agree
- Neutral
- Partly disagree
- Completely disagree

The questions were constructed to get data on existing practices within the respondents' unit. To what degree do the different DF units have documentation facilitating quality managment? Questions around that subject could give an impression of how the organization contributes to the work with quality assurance.

Role and frequency of Quality Control

Questions 14 to 18 were related to who is involved in the QC process at the units and if they had DF liaisons participating in the DF work that is done. There were some differences between the questions presented to managers and employees. Question 16 was only given to respondents who answered that they were managers. This was to understand how the managers participated in the units QC. Questions 17 and 18 were only given to respondents who responded that they worked in a police district; national units were excluded from that question since they don't have DF liaisons in their units. Question 18 was only given to respondents that answered yes to question 17.

Questions related to the amount of Quality Control performed

The questions in this section were given in a closed form. In this part, the respondents answering that they were managers were given statements where they were asked to quantify how many reports were subject to a QC on an ordinal scale (Leedy & Ormrod, 2015, p.111). The employees were asked to answer how many reports they had performed QC on within the last few months. The following ordinal scales were used.

The scale used for managers:

- All
- Most
- A few
- None

The scale used for employees:

- 0
- 1 - 5
- 6 - 9
- 10+

Managers and employees were asked to answer on a different scale because I wanted to measure how much QC the managers thought was done by their units and if there would be a notable difference between them and the groups' perception of what was done.

3.2.4 Qualitative method - interviews

Since part of the study question had phenomenological perspectives, DF in a risk perspective, better insight into the DF work process and the DF investigator role, a qualitative approach using research interviews was chosen. I chose to use a semistructured interview model since I wanted to be able to pursue respondents' answers with follow-up questions to get clarification (Leedy & Ormrod, 2015, p.160). Phenomneical studies try to describe people's perceptions and perspectives about a particular situation (Leedy & Ormrod, 2015, p.273).

Sampling

I decided that managers of DF units would be the source that would give the best insight into the research problem. Since I wanted to explore how the organization managed the field of DF, and questions like which roles take part in the DF process and what implications this could have on the field in terms of risk and quality, the managers should be the ones that would give most insight. The managers have professional responsibility for the area and have firsthand knowledge of how the work is organized within their respective units and police district.

I interviewed six managers of DF units from different police districts. The selection process of interview candidates was semi-random; I had a non-sorted list of the managers working in the different DF units and started from the top of the list, and stopped when I had six candidates that were willing to participate in the interviews. Since there are 12 police districts in addition to the national units, there are not many managers within the field of DF. And since a representative sample in a qualitative study should be a sample that represents the population(Leedy & Ormrod, 2015, p.279), this should be a large enough sample to represent the perspective of managers within the DF in the Norwegian police.

To save time, I contacted the managers directly, presented the study, and asked if they would participate. If they were willing, they were asked to sign a written agreement describing that they agreed to participate in the interviews, that I was allowed to handle their data, and that they could withdraw at any time.
After agreeing to participate, I kindly asked them to seek permission within their police district to participate.

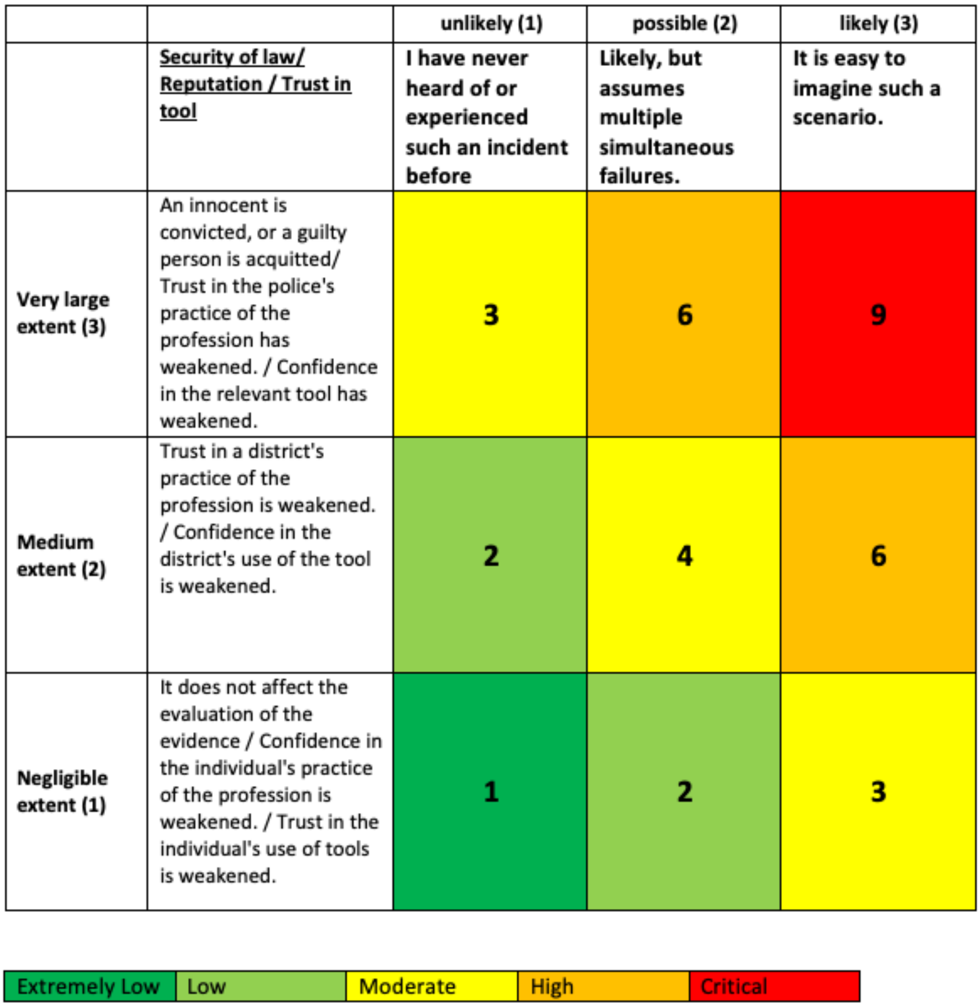
Semistructured interviews

I first decided that I wanted to do all the interviews face-to-face. But after considering factors such as cost and time I decided it would be better to do the interviews using the Zoom platform that was made available to me through NTNU licensing. I had met all the candidates on various occasions beforehand, so we had prior knowledge of each other. Using conference software such as Zoom and Teams is considered an appropriate method when one wants to conduct face-to-face interviews with candidates at different geographic locations. But the candidates need to be comfortable using the technology (Leedy & Ormrod, 2015, p.160). During the Covid-19 pandemic, Microsoft Teams were introduced, in the Norwegian Police, as a platform for meetings and video calls. I, therefore, felt confident that the participants were used to using that type of technology for meetings and face-to-face conversations. To ensure the viability of the proposed solution, I also sought the opinions of all the candidates, and they all agreed that it was a sound approach. The interviews lasted approximately one hour, and prior to the commencement of each session, participants were reminded not to share any confidential information during the interview. To initiate the interview, I sent an invitation to a password-protected Zoom meeting. Prior to the interview, I notified the participants that the session would be recorded and that the recordings would be saved in an encrypted environment.

I had created an interview guide that evolved around a risk assessment of the DF work performed on each phase of the DF process. This would lead to a semi-structured design since the outcome of the different risks identified by the candidates could lead to different follow-up questions seeking clarification when needed. The interview was tested on my manager, who was not one of the participants. All the candidates were given the same questions and in the same order. The first few questions seek knowledge into the candidates' perception of risk and who within their police district participates in the different phases of the DF process. To maintain consistency across all interviews, I established a common set of values to be used in the risk assessment. However, during the interviews, the candidates were given the opportunity to provide feedback and make adjustments to these values as needed. The following values were presented to the candidates:

1. Legal protection of those involved
2. Trust in the police's practice of digital forensics as a subject (reputation)
3. Confidence in the use of commercial tools and the interpretation of what is presented by these.

Next, I introduced the risk assessment model to be used and provided a brief overview of the concept. During this stage of the interview, my role was more of a facilitator, guiding the participants through the process and clarifying any uncertainties as needed. The following model was used for the risk assessment. The model is inspired by the Risk Analysis process described by Peltier(2005, pp.15-25).



		unlikely (1)	possible (2)	likely (3)
	Security of law/ Reputation / Trust in tool	I have never heard of or experienced such an incident before	Likely, but assumes multiple simultaneous failures.	It is easy to imagine such a scenario.
Very large extent (3)	An innocent is convicted, or a guilty person is acquitted/ Trust in the police's practice of the profession has weakened. / Confidence in the relevant tool has weakened.	3	6	9
Medium extent (2)	Trust in a district's practice of the profession is weakened. / Confidence in the district's use of the tool is weakened.	2	4	6
Negligible extent (1)	It does not affect the evaluation of the evidence / Confidence in the individual's practice of the profession is weakened. / Trust in the individual's use of tools is weakened.	1	2	3

Extremely Low	Low	Moderate	High	Critical

Figure 3.1: The form used for the risk assessment adapted from Peltier(2005, pp.20, 24).

The last part of the interview had different questions seeking more knowledge into attitudes toward QC and what the candidates see as the biggest challenges in the field of DF within the Norwegian police. Although not expected, the risk assessment yielded a significant amount of relevant information. This influenced some of the questions I had planned for the later part of the interview, as the information I was seeking had already been covered during the assessment.

Processing of data and analysis

The analysis was performed as a thematic analysis, inspired by the method described by Braun and Clarke(2006, p.6), and involves identifying, analyzing, and reporting themes or patterns within the source data. And the process described includes the following phases (Braun & Clarke, 2006).

- Phase 1: familiarising yourself with your data
- Phase 2: generating initial codes
- Phase 3: Searching for themes
- Phase 4: reviewing themes
- Phase 5: defining and naming themes
- Phase 6: producing the report

When dealing with data collected through interviews, verbatim transcription is a standard method for preparing the data for analysis. And can be described as reproducing spoken words into text (Davidson, 2009, p.1). But a stricter description would be that it is the translation of oral language into a written language. During this translation, data like body language, pauses, and hesitation might be lost (Brinkmann & Kvale, 2018, p.106-107).

Transcription of data can be a time-consuming activity, and there are tools available that could automate the process. I decided to do it manually since this could give me a better overview of my data, and the process could start the analysis process (Brinkmann & Kvale, 2018, p.110). There are no definite rules defining how a transcription should be performed, and how much non-verbal communication should be included in a transcription has been debated (Davidson, 2009, p.1). I chose not to include emotional aspects like coughs and sighs in the transcriptions but to only have a complete transcription of the verbal communication of the candidates.

I started working on transcriptions in parallel with the interviews, which was a wise decision. I learned a lot from transcribing my first interview and used this knowledge of my behavior during the interviews to improve the quality of the following interviews.

I transferred the transcribed interviews to Microsoft Excel, in which I did the coding and analysis. During this process, I read through the transcriptions and made small summaries of each answer to the different questions throughout the interview. By doing this, I got an overview of the data set and produced initial codes for themes within the data that were relevant to my research questions. Braun and Clarke(2006, p.18) describes an initial coding as data-driven or theory-driven. I will describe my initial coding as data-driven, driven by the data itself and not by looking for themes relevant to my research question. I chose this approach to mitigate bias during the coding of the data.

After the initial coding, I had a long list of codes. I cross-referenced the different codes in Excel and organized them into potential themes. During this phase, it became clear which parts of the data set were part of themes that would be of interest when answering my research problems and which parts could be left out. A process influenced by the description by Braun and Clarke(2006, p.19-22). During this process, as themes emerged, I reviewed the different themes. I checked them towards the raw material to ensure that the coding created coherent patterns and that the themes accurately represented the data. I then organized them under stricter naming conventions, creating the final analysis's basis.

These themes were:

- Quality & QC
- The participants of the DF process
- Risk from a DF perspective
- Trust
- Administration of digital forensics

Themes such as Quality, QC, participants of the DF process, and risk were introduced during the interviews. However, through the analysis of the data, additional themes, including the administration of DF and perceived trust, emerged. These themes provide important insights into the research questions, shedding light on key aspects of the investigated phenomenon.

3.3 Quality Assurance

When a research method is chosen, it is important to account for the validity of the approach. The data collected should accurately yield meaningful and credible results that answer the research problem. In quantitative research, one often divides this into terms of Internal and external validity. And the researcher can increase internal validity by taking precautions and using methods mitigating bias and other possible explanations for the results from their analysis. External validity can be described as the results' ability to be used for generalizations beyond the study itself. In qualitative research, however, it is not common to use the term validity but to use other terms like quality, credibility, and trustworthiness when accounting for the validity of their studies (Leedy & Ormrod, 2015, p.103-106).

The methods used in this research resemble more a quasi-mixed design than a fully mixed design. And this is noticeable in the results section, where each research method is presented in separate chapters and discussed on behalf of their data sets (Halcomb & Davidson, 2006, p.53).

In mixed-methodology designs, different approaches can be used to justify the research methods' validity. Halcomb and Davidson(2006, p.57) describes nine different legitimation types for research using mixed methods; Sample integration, inside-outside, Weakness minimization, sequential, conversion, paradigmatic mixing, commensurability, multiple validities, political.

One of the methods described as pertinent for mixed methodology is "multiple validities legitimation,» which describes validity as the sum of the included methods' validity. "Validities" for both the qualitative and the quantitative methods need to be addressed, and only if both methods yield high validity can one say the validity of the research method is good (Halcomb & Davidson, 2006, p.59).

3.3.1 Internal validity - survey

In order to improve the internal validity of the survey that was used in the quantitative phase of this thesis, I have used the following strategies; I have presented the sampling procedures in detail, and in that way, making it possible for the readers to verify if they were appropriate for the study and the research question. I have been transparent with my background and prior knowledge, and by doing that, I tried to help address issues related to researcher bias. Another issue that might be present in this kind of survey is known as the Hawthorne effect (Leedy & Ormrod, 2015, p.104). The month before the survey was sent to the possible respondents, Nina Sunde held a workshop presenting a model for QC Sunde and Horsman(2021), where several of the respondents participated, and this might have affected how the respondents related to the topics of the survey. The community it was distributed in is also relatively small. As a member of that community, I can not ignore the possibility that respondents could have answered what they thought I wanted them to respond.

3.3.2 External validity - survey

The external validity of quantitative research describes the extent to which the conclusions can be generalized to other contexts. A common strategy is to identify if the sample used for the method is representative of the population. The sampling procedure and population are described in section 3.2.3. Only when the sample is a valid representation of the population can it be used to draw conclusions for the population as a whole (Leedy & Ormrod, 2015, p.105).

The following formula was used to calculate the sample size needed (Etikan & Babtope, 2019).

$$n = \frac{N * X}{X + N - 1} \tag{3.1}$$

X is given by

$$X = \frac{\left(Z_\alpha / 2^2 * P(1-P)\right)}{MOE^2} \tag{3.2}$$

n=Sample size, p = proportion of sample, MOE = margin of error, N= population size

This results in the following requirements for the sample to be representative of the population.

Confidence level	95	90	95	90
Margin of error	5	5	10	10
Sample size	126	111	64	50

Table 3.1: Calculated minimum population size for N=185 (Etikan & Babtope, 2019)

There were 60 responses to the survey. Using the same formula would result in a confidence level of 95% with a 10,43% margin of error or a confidence level of 90% with an 8,78% margin of error. Drawing conclusions, within the context of Norwegian Polices DF units, based on these results should be possible but with medium to low confidence.

3.3.3 Validity - interviews

In order to vouch for the validity of the qualitative approach, I have used the following methods as described by Leedy and Ormrod(2015, p.106)

- Acknowledgment of personal bias
- Respondent validation
- Feedback from others

Acknowledgment of personal bias
I have disclosed my personal background and potential biases in relation to the research topic to enable the reader to identify any researcher bias. As a researcher with a background in the subject under investigation, I have made a concerted effort to maintain a broad perspective when analyzing data and interpreting findings. In this regard, I have undertaken additional efforts to seek out alternative explanations for the results to minimize any potential impact of my personal biases.
Respondent validation
All quotes included and used in his thesis were sent to the respective participants for validation and to get consent before they were used. This would also address a wrongful translation or loss of meaning when translating quotations from Norwegian to English.
Feedback from others
I have also tested my use of the methods and my analysis of the data on my supervisors and a colleague with experience from within the field. This has been a good way to get corrected inferences that are not linked well enough to the data.

Conclusions from the analysis of the interviews would not be suitable for generalization. But it could give a good indication into how DF is managed as a profession within the Norwegian Police from a risk perspective.

3.4 Ethical Considerations

When planning and designing the survey and the interview guides focus on the participant's right to privacy and voluntary participation was in focus. Both were distributed with information about their topic and a consent form to ensure that the participation was voluntary and informed (Leedy & Ormrod, 2015, p.121).

I have expressed concerns regarding the potential negative impacts that the insights from this study on risk and QC within the DF units might have on the reputation of the Norwegian Police. Additionally, focusing on these issues may expose the already heavily burdened group of DF examiners to further external pressures. However, at the same time, knowledge and insight into these topics is crucial from the perspective of safeguarding legal protection.

The survey was delivered in such a manner that the respondents would be completely anonymous if they chose to answer. It would not be possible to link the written consent and answers to the survey. Written permission doesn't automatically mean the person who sent the consent answered the survey.

Applications were sent to the Norwegian Agency for Shared Services in Education and Research (Sikt) for both the survey and the interviews. It is mandatory to seek approval from Sikt when doing surveys or interviews that might involve handling personal data.

Demographic questions used in the survey, when sampling such a small population as I did, could make it possible to identify individuals who had answered if they were not handled correctly. The approval for the survey and the interviews is available in appendix Appendix A.

Before distributing the survey, I contacted Anna Charlotte Amdal Neumayer at the National Police Directorate through a phone call to inquire about the necessary approvals for sending out the survey and conducting interviews. Ms. Neumayer informed me that I did not require their approval to conduct my research. Still, she emphasized the importance of ensuring that the interviewees were aware they were not exempt from their duty of confidentiality. To address this, the consent forms included information on confidentiality, and I also emphasized this point before the start of each interview.

Chapter 4

Results

In this chapter, I will first present the results of the analysis of the survey, followed by a presentation of the analysis of the interviews. The combined results and implications will be discussed in light of theory and related research in chapter 5.

4.1 Survey

In this section, the analysis of the data collected through the survey will be presented. The survey has been divided into several sections, including demographics, questions related to QC at the respondents' workplace, the role and frequency of QC, QC questions given to managers, and QC questions given to employees. Each section will be followed by a brief summary of the key findings. The analysis of these survey sections will provide valuable insights into the state of QC practices and perceptions within the surveyed population.

4.1.1 Demographics

The initial part of the survey consisted of seven questions that pertained to the respondents' demographic information. This was done to enable the comparison of attitudes toward QC among various respondent groups.

Demographic characteristics of respondents with police and civilian backgrounds

Variable *(N = 60)*	**Count**	**Percentage**
Situated:		
A police district/local unit	47	78 %
A national unit	13	22 %
Role:		
Manager	10	17 %
Employee	50	83 %
Background:		
Police with additional civil education	12	20 %
Civil	30	50 %
Police	18	30 %
Civil with bachelor's degree from the Police University College	0	0 %
Years of experience:		
0 - 2	11	18 %
3 - 5	10	17 %
6 - 8	19	32 %
10 +	20	33 %
NCFI modules completed:		
None	17	28 %
NCFI module 1 (core concepts in digital investigation and forensics)	9	15 %
NCFI module 2 (one or more modules)	19	32 %
NCFI module 3 (one or more modules)	11	18 %
Master's program – offered by The Norwegian Police University College and NTNU (MISEB)	4	7 %

Table 4.1: Demographics

Out of the 60 survey respondents, 47 worked in police districts, and 13 worked in national units. Of these, 10 were managers within a Digital Forensics (DF) unit at a police district or national unit.

Half of the respondents reported having a civilian background, which is not surprising given that DF is a specialized field that requires particular interest and/or education. We can also observe that of the respondents with a police background, 20% of them had an additional civil education.

A significant majority, 65%, of the respondents had more than six years of experience working in DF. This high percentage of experienced respondents suggests that there is low turnover in this field.

Nordic Computer Forensic Investigator (NCFI) is a study program that offers courses on three different levels of expertise teaching different areas of DF methodology. The program includes an introduction and different modules on levels one, two, and three. At the time this thesis was written, the official requirement was that one must have NCFI module 1 or equivalent to be able to work as a DF examiner (Politidirektoratet, 2019, pp.22-23). The required minimum level, NCFI module 1, was originally proposed by the Oslo police district as the level of competence needed to take on the role of DF liaison. And representatives from Norwegian Police University College (Politihøgskolen) (NPUC) argued that the requirement for taking on a role as DF examiner should be raised to NCFI module 2 or equivalent (Sunde & Bergum, 2019).

The survey revealed that 17 of the respondents had not completed any of the courses offered by the NCFI program, and out of these, six were in their first two years of employment within the field. However, the remaining 11 respondents had six years or more of experience as DF examiners.

The reasons why some respondents did not complete an NCFI module 1 or higher course were not investigated in greater detail. It is important to note that the survey did not provide respondents with the opportunity to specify alternative qualifications that could be considered equivalent to completing NCFI module 1 or higher.

Demographics from respondents with civil background only

As part of the survey, respondents who reported working in civilian positions were given additional questions to explore their educational background and professional development. Specifically, they were asked about their highest completed degrees and whether they had participated in any continuing professional development courses for civil personnel. As mentioned in the methodology chapter, it is important to note that question 4, which specifically pertained to the highest completed degrees, was only given to respondents with a civilian background. However, in retrospect, it would have been valuable to ask the same question to respondents with a police background and to gather more comprehensive data on the educational background of all respondents.

Variable ($N = 30$)	**Count**	**Percentage**
Highest academic degree:		
No degree	7	23 %
Bachelor's degree (BSc)	12	40 %
Master's degree (MSc)	11	37 %
Doctoral degree (PhD)	0	0 %
Continuing professional development courses:		
None	29	97 %
General introduction to criminal investigation – strategies and principles (7,5 ECTS)	0	0 %
General introduction to investigative methodologies (7,5ECTS)	0	0 %
Continuing professional development in criminal investigation (15 ECTS)	1	3 %

Table 4.2: Demographic questions only asked civilians

23% of those working in civilian positions reported that they had not obtained a degree.

In their publication, "Nasjonale retningslinjer for digital etterforskning" (Politidirektoratet, 2019), the Norwegian National Police Directorate outlines a requirement for individuals working as data investigators (DF examiner) to have completed at least the course "Begrenset politimyndighet - etterforskning" ("Limited police authority - investigation"). However, upon review of the Norwegian Police University College (Politihøgskolen) websites, no study program under that exact name could be found. It is possible that this course has been replaced with the courses "General Introduction to criminal investigation – strategies and Principles" and "General Introduction to investigative methodologies," which were approved by the Education Committee in November 2020.

The Office of the Auditor General's report on the evaluation of the police effort against computer-enabled crimes highlights the need for education in investigations for civilians working within the DF units (Riksrevisjonen, 2021).

The first two courses listed in Table 4.2 have only recently been approved by the Education Committee as of November 26, 2020. This may explain why relatively few respondents reported having completed these courses, as they may not have been widely available at the time of the survey.

Out of all respondents with a civilian background, only one reported having completed one of the Norwegian Police University College (Politihøgskolen) development courses aimed at increasing knowledge on how investigations are conducted in the Norwegian police. The respondent who had completed a development course had completed a course mainly targeting police personnel rather than civilian personnel.

4.1.2 Questions About Quality Control At The Respondents' Workplace

Questions 8 to 13 had a free-form text field attached to them, making it possible for the respondents to comment on their questions. Including free-form text fields in a survey can allow respondents to provide more detailed or nuanced feedback that may not have been captured by the fixed-response questions. The comments are used in the analysis of the results.

Question 8. In my unit, there is sufficient documentation available such as procedures, routines, and templates describing and facilitating Quality Control of digital forensic work performed at the unit.

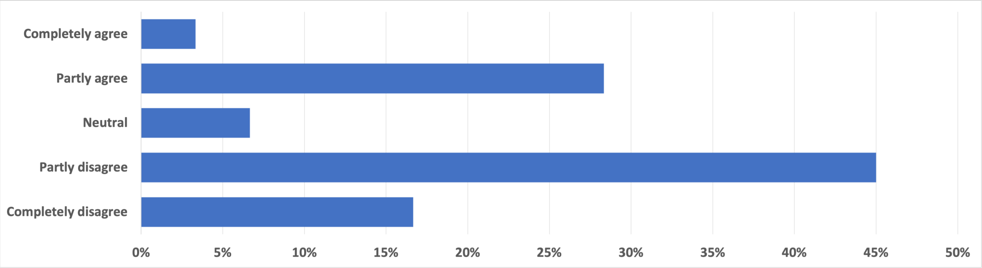


Figure 4.1: In my unit, there is sufficient documentation facilitating QC of DF work.

As many as 62% of the respondents answered that they completely disagree or partly disagree with having sufficient documentation available. Two respondents answered that they completely agreed when asked if their unit has sufficient documentation facilitating QC of DF work.

‘Missing procedures, routines, and templates. No structured QC.’ was a comment given to one of the answers that were representative of the answers given. The procedure, routines, and templates are not adequate, and QC is something that is not encouraged by the system but by the employees themselves. Another comment, ‘Lack of capacity to prepare/maintain documentation’, suggests that there is a capacity problem within the respondents’ unit and that the DF units that have some documentation available but lack the opportunity to follow up on the routines. Could that indicate that focus on quality gives way to casework? ‘It cannot be called a routine when it is up to each individual.’

My experience from working in DF unit in a police district is that there are no common national templates and routines that describe how this work should be done. When you do not have a common template or methodology for reports documenting DF work, perhaps not within your own unit, it becomes difficult to carry out any form of QC.

Question 9. In my unit, the reports undergo systematic Quality Control.

This question concerns reports resulting from the examination/analysis of the evidence file, which involves technical analysis and/or content analysis performed by an employee at a DF unit.

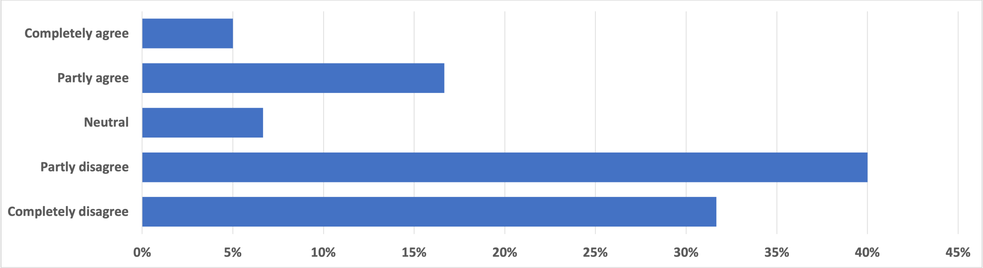


Figure 4.2: In my unit, the reports undergo systematic QC.

The survey results indicate that systematic QC is not implemented in the DF units, as 72% of respondents completely or partly disagree that reports undergo systematic QC. The comments suggest that the lack of quality management in the units is the reason for this and that QC is mostly initiated by employees themselves. ‘No structured QC, only on the initiative of each individual employee’.

40% partly disagree that the reports produced within their units undergo systematic QC, and it might be related to the question asking if the QC is systematic. A systematic control suggests that its part of a routine or workflow. And as one of the respondents put it, the QC done is "..not structured, person-dependent and no anchoring towards the management."

The survey results show that only a small proportion of participants (5%) completely agreed that reports within their unit undergo systematic QC, with a slightly larger proportion (17%) partially agreeing. These findings suggest that there may be variations in the level of systematic QC across different units. This is consistent with the comments provided by some respondents who indicated that, while there is a desire for systematic QC, the current process is not well-structured and largely relies on individual initiative. One respondent suggested that for short and simple reports, colleagues in the section take shortcuts and do not fully adhere to QC procedures. 'In principle, reports must be peer-reviewed by colleagues in the section. For short and simple reports, shortcuts are taken in everyday life.'

It is also worth noting that 7% of the respondents indicated a neutral stance on the matter.

Question 10. In our police district, we perform systematic Quality Control of the criminal detective's reports resulting from an investigative review of the evidence file.

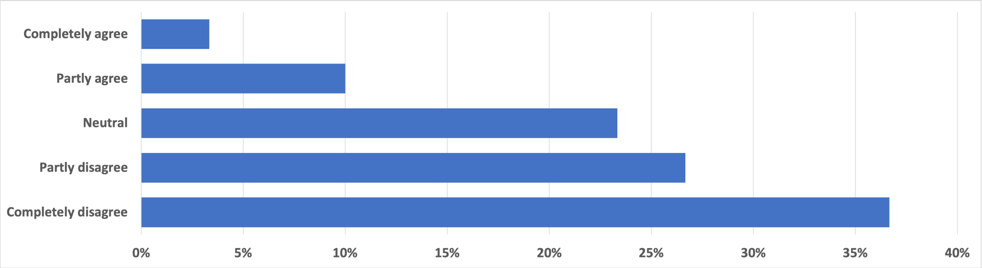


Figure 4.3: In our police district, we perform systematic QC of the criminal detective's reports resulting from an investigative review of the evidence file.

64% of the respondents either completely disagree or partly disagree that there is conducted QC of the criminal detectives' reports resulting from an investigative review of the evidence file. Only 3% of the respondents completely agree that they perform systematic QC of the criminal detective's reports resulting from an investigative review of the evidence file. This suggests that there is a lack of a system in place to ensure the quality of work done in the investigative review process.

In chapter subsection 4.2.1, there is given more insight into who is performing tasks on the different phases of the DF process in the Norwegian Police. More refined models for

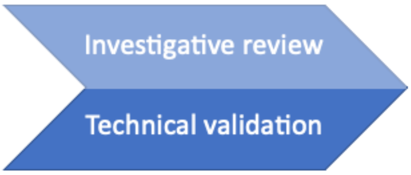


Figure 4.4: The analysis step in the DF process is here divided into two parallel steps.

the analysis steps in the DF process divide this step into two parallel process steps where they, to some degree, are co-dependent. If one fails to include one of the processes, the results presented will have less value. Criminal detectives are trained to validate their findings with judicial reasoning, and that is the focus of the reports produced during their investigative review of the evidence file. The other half of this process is the process of validating their findings. These findings suggest that there is no system in place to ensure the validity of police investigators' findings.

As one of the respondents comments, 'Only at the request of the investigator'. Could this suggest a system error? What happens with the digital evidence after the DF unit has completed the examination process and made the results available for the investigators so that they can perform a review?
'I am not certain; I work little with investigators who are not employed in my section.' is a comment that suggests that there is too little communication between the tactical and technical investigators.

The results also suggest that there is no system in place to ensure the quality of the work done in these processes. Some QC is performed, but it is up to the individuals themselves to initiate such control, and there is no system in place to ensure how such QC is conducted. In my experience, most investigative reviews of evidence files are performed by criminal detectives, and that they may ask for a technical report supporting their findings.

Question 11. At my unit, we have enough time to perform Quality Control of the casework.

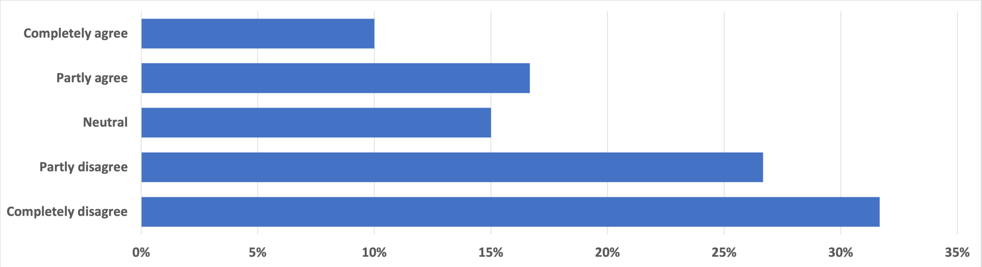


Figure 4.5: At my unit, we have enough time to perform QC of the casework.

57% claim to completely or partially disagree with having enough time to perform QC. This suggests that there may be time constraints or workload issues that prevent them from dedicating adequate time to perform QC. And 27% completely or partly agree with having enough time to perform QC. 15% answered neutrally, which could indicate that they are unsure or do not have a clear understanding of the time allocation for QC at their unit. It is noteworthy that 10% of the respondents completely agree with having enough time to perform QC, indicating that some units may have a better system in place than others.

This question seems to divide the respondents into two different groups. One group considers QC as something extra, a part of the process that is time-consuming and comes at the expense of their main tasks. 'If we had done this, the processing time for everything we do at DPA would be significantly longer.' This is a comment that suggests that the respondents don't consider QC as a part of the process. This leads to a perception that a new task is being imposed on them. One of the respondents comments this way on the question; "We have more than enough to carry out our own tasks. Occasional time is used on one's own initiative to ensure the quality (read spelling/rewording) of reports."

The other group has a common notion that can be represented by the comment, 'We always have time to do what we have to do depending on the situation.' This perspective suggests that if QC was considered to be a part of the workflow, the DF examiner would have had enough time to perform it as well. Other answers to this survey show that QC was done in the DF units, but it was not initiated by the system; it was initiated by individuals. This is a good indication that time is already spent to some degree on QC-related tasks. Could one get a more productive use of this time if it was used to a more systematic approach to QC?

'The focus is supposed to be on quality rather than quantity, but in reality, this is not quite the case.' Overall, this suggests that there is a need for more systematic approaches to QC in the DF units and that the implementation of such a system may require a shift in mindset towards QC as an essential part of the workflow rather than an extra task.

Question 12. Quality Control should be integrated into the work processes at DF units.

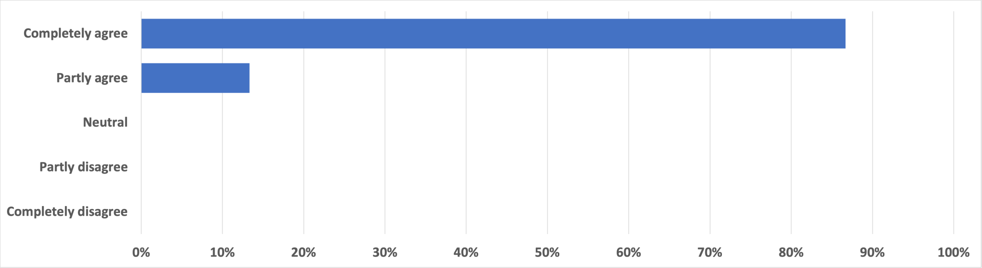


Figure 4.6: QC should be integrated into the work processes at DF units.

87% of the respondents completely or partly agree that QC should be integrated into the work processes at DF units. Only a minority of 13% partly agree with the statement, while none of the respondents completely or partly disagree or are neutral about it.

'I believe it is an important part of due process, which is currently almost non-existent. Ideally, it should be integrated, but resources will make this challenging.' Although all, to some degree, agree that QC should be integrated into the workflow, many comments on the lack of resources as one of the biggest obstacles. 'A court case can collapse if an investigation is found to be invalid/wrong. Ensuring that the reports we deliver maintain their quality is extremely important both for legal protection and for the success of a case in court.'. All the respondents, to some degree, agree that QC should be integrated into the overall process. A recent study by Sunde and Dror (2021, p. 9) concluded that it was an urgent need for quality assurance in DF. The conclusion was based upon findings that showed low reliability between the DF examiners in observations, interpretations, and conclusions.

Question 13. Quality Control of results prior to being used in a criminal investigation should be a natural part of the workflow in the police district.

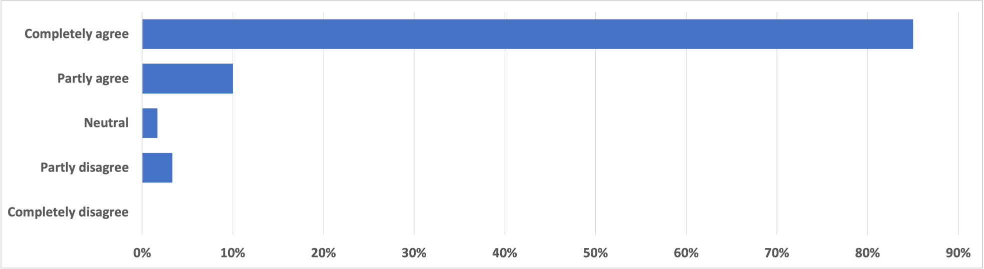


Figure 4.7: QC of results prior to being used in a criminal investigation should be a natural part of the workflow in the police district.

85% of the respondents completely agree that QC of results prior to being used in a criminal investigation should be a natural part of the workflow in the police district. 10% partly agree, while only a small minority of 3% partly disagree, and 2% are neutral on the matter.

Comments from respondents within these 5% suggest that concerns towards workload and time are the main reasons for not agreeing with this being part of the process.

> All reviews are, in one way or another, used as evidence in criminal cases, so the scope will be too large. But if the result/artifact is very central to the criminal case, this should be done. In addition to a selection of the other review reports and technical reports...

This comment provided by one of the respondents indicates an understanding and need for QC of findings before using them in an investigation but also suggests that this should only be done if the evidence is deemed "central" to the criminal case. This opens up another source of error in the investigation; who should decide if the findings are safe to use without validation? And what criteria should these decisions be based upon? My own experience is that there are no QC mechanisms in place and that it is up to us as DF examiners to ensure the quality of our reports.

> To safeguard due process, yes. In particular, due to the lack of a control mechanism (lack of knowledge on the part of other parties, which makes them unable to challenge findings/evidence) during legal proceedings.

A recurring theme among the comments is that one is concerned with having good enough quality so that legal protection is safeguarded. And that is most likely the reason for such a positive attitude towards QC amongst the respondents.

Summary of findings from questions 8 to 13

The majority of respondents, 72%, reported that reports at their unit did not undergo systematic quality control. The findings reveal that a majority of the respondents disagree with the availability of sufficient documentation, systematic QC of reports, and systematic

QC of criminal detectives' reports. There is a lack of a system in place to ensure the quality of work done in the investigative review process, and variations in the level of systematic QC across different units were observed. The comments suggest that the lack of quality management in the units is the reason for this and that QC is mostly initiated by employees themselves. The survey results indicate that there may be a capacity problem within some units, and the absence of a common national template or methodology for documenting DF work may lead to difficulties in carrying out any form of QC.

4.1.3 Role And Frequency Of Quality Control

Variable	Count	Percentage
Question 14. What is the role of those performing Quality Control at your unit? *(N = 17)*		
Manager at a digital forensics unit	7	41 %
Employee at digital forensics unit	9	53 %
Prosecution	1	6 %
other	0	0 %
Question 15. During the last 12 months, have you initiated Quality Control of your own reports? *(N = 60)*		
Yes	40	67 %
No	20	33 %
Question 16. During the last 12 months, have you performed Quality Control according to the scope of one or more of the Peer Review Hierarchy for DF levels? *(N = 10)*		
Yes	5	50 %
No	5	50 %
Question 17. In our police district, digital forensic work is performed by Digital Forensics liaisons. *(N = 47)*		
Yes	37	79 %
No	10	21 %
Question 18. In our district, the work performed by Digital Forensics liaisons or similar positions is subject to Quality Control. *(n = 37)*		
Yes	9	24 %
No	28	76 %

Table 4.3: Role and frequency of QC

A restriction was applied to Questions 14 and 16 in the survey, such that it was only presented to respondents who identified themselves as managers in response to Question 2. Question 14 allowed the respondents to select multiple answers. Question 17 in the survey was restricted to respondents who indicated that they work in a police district in response to Question 1. Similarly, Question 18 was only presented to those who answered affirmatively to Question 17.

Question 14. What is the role of those performing quality control at your unit?

According to the respondents that answered they were managers, the majority of those who perform QC are employees at DF units, with 53% of the respondents indicating this. However, a significant proportion of managers, 41%, also reported performing QC. The prosecution was a less common response, with only 6% of respondents indicating that they perform QC. No respondents chose "Other" as an option.

When deciding who should perform QC of work done by a specialist within a field such as DF, it is important that the person conducting the QC has the appropriate knowledge and skill set. An individual's employment status can not automatically qualify him for the role of controller. Members of the prosecution are skilled professionals within their area of expertise, but their expertise is the law and doing judicial decisions based on the evidence presented to them. Without training in validating the evidence, they will not necessarily realize that the evidence they were assessing did not prove what they thought it to do (Erlandsen, 2019, p.76). This argument would also be valid for other practitioners that don't have the necessary competence to perform QC on other practitioners' work.

Question 15. During the last 12 months, have you initiated Quality Control of your own reports?

67% of the respondents answered they have initiated QC of their own reports within the last 12 months. This suggests that the respondents are taking responsibility for ensuring the quality of their work, which is a positive indication of their commitment to producing reliable and accurate findings.

On the other hand, 33% of the respondents reported not initiating QC of their own reports within the same time frame. This raises concerns about the possibility of errors or inaccuracies in their reports.

As we could read from the comments to earlier questions, QC is something that is mainly initiated by the employees, even though they lack the systems support. So even if a systematic approach regulated by quality management was missing, some sort of QC was performed, but with the individual examiners having discretion over whether it was conducted or not and to which extent. When the units lack a systematic approach and a common standard for quality, it is still alarming that as many as 33% answered they have not initiated such a review by their own initiative.

Question 16. During the last 12 months, have you performed Quality Control according to the scope of one or more of the Peer Review Hierarchy for DF levels?

According to the managers who participated in the survey, the responses to the question about performing QC according to the Peer Review Hierarchy for DF levels were evenly split, with 50% answering "Yes" and 50% answering "No."

Question 17. In our police district, digital forensic work is performed by DF liaisons or similar positions.

79% of the respondent answered that in their police district, digital forensic work is performed by DF liaisons or similar positions. This suggests that there are other roles than the DF examiner performing digital forensic work in most police districts.

On the other hand, 21% of the respondents answered negatively, indicating that digital forensic work may not be consistently performed by DF liaisons or similar positions in all police districts. This may suggest a lack of standardization or inconsistency in the performance of digital forensic work across different police districts.

This is a role that is not defined by National role definitions with competence requirements for the investigative field. But the role exists, and since there is no national definition of competence required to have this role, the police districts can define what is needed to have the role of a DF liaison. In my experience, there are large differences between the police districts in this area. Some police districts do not have any official DF liaison at all, and others can have as many as 60 employees having this role. It is not within the scope of this thesis to give much insight into this role, but it is a role within the police that, in my experience, does a significant amount of DF work. In some cases, in all the stages of the DF process.

Question 18. In our district, the work performed by digital forensic liaisons or similar positions is subject to Quality Control.

76% of respondents did not perform QC on DF work done by digital forensic liaisons, while 24% did, indicating a low focus on QC outside of DF units.

As discussed under question 17, this is a role with no typical competence requirements attached to it. This is a participant doing work on various stages of the DF process. These responses indicate that there is no or limited quality management connected to the work that is done in relation to DF. The lack of QC raises concerns about the accuracy and reliability of the digital forensic work performed by DF liaisons or similar positions. Without proper QC procedures, errors or inaccuracies may go undetected, potentially leading to wrongful convictions or acquittals.

Summary of findings from questions 14-18

DF employees were the most common group performing QC, but managers also reported participating. 67% of respondents reported initiating QC of their own reports within the last 12 months, but 33% did not, which raises concerns about the possibility of errors or inaccuracies. 79% of respondents reported that digital forensic work is performed by DF liaisons or similar positions in their police district, but only 24% reported that the work performed by these liaisons is subject to QC. This suggests a lack of consistency in the implementation of QC procedures across different police districts.

4.1.4 Quality Control

In this section, the survey results related to the degree of QC performed at each level of the QC hierarchy as described by (Sunde & Horsman, 2021). This part of the survey had a separate set of alternatives for employees and managers. The questions presented to the managers were focused on QC within their respective teams. The employees were asked about the number of reviews they had conducted on each hierarchy level.

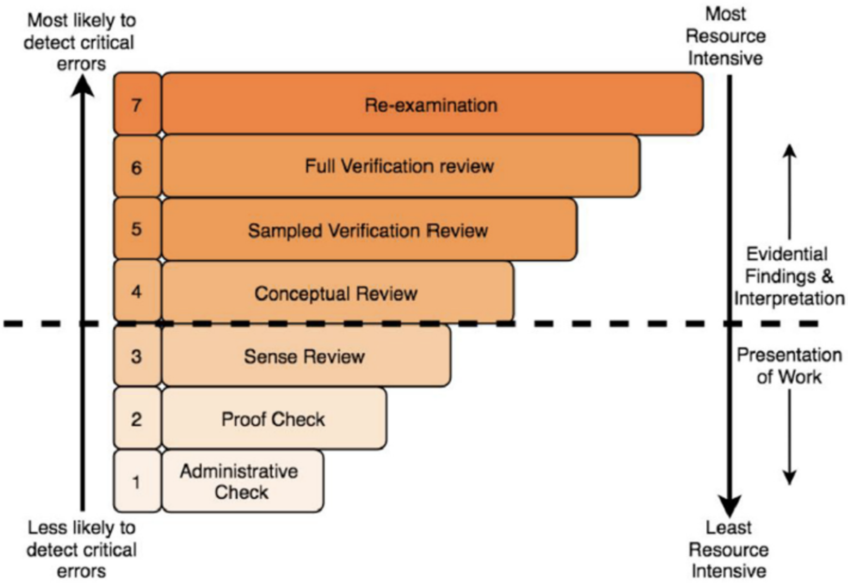

Most likely to detect critical errors
Most Resource Intensive
7 Re-examination
6 Full Verification review
5 Sampled Verification Review
4 Conceptual Review
Evidential Findings & Interpretation
Presentation of Work
3 Sense Review
2 Proof Check
1 Administrative Check
Less likely to detect critical errors
Least Resource Intensive

Figure 4.8: The "peer-review hierarchy" for Digital Forensics (Horsman & Sunde, 2020, p. 6)

The managers: Questions 19 to 25

After the survey data is presented in table form, questions 19 to 25 will be analyzed, followed by a short summary of the findings.

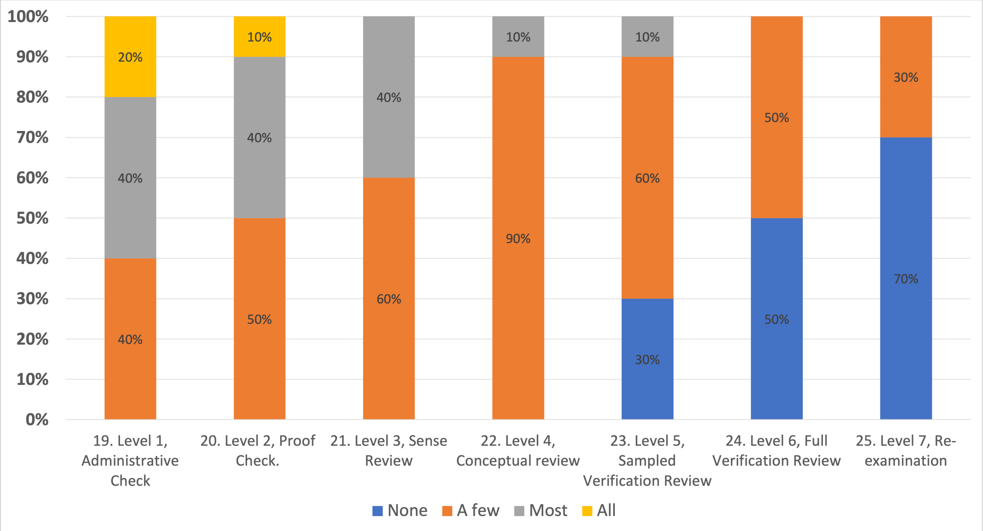


Figure 4.9: Volume of Reports Subjected to QC as Reported by Managers

19. At our unit, Quality Control of reports is performed at level 1, Administrative Check.

An Administrative Check entails controlling whether the investigation is performed in compliance with formal requirements and according to the agreed assignment – meaning, the agreed tasks have been performed on the seized devices.

Of the managers surveyed, 40% reported that a few reports underwent this level of QC, while another 40% reported that most reports were subject to it. Only 20% of managers reported that all reports underwent level 1 QC, and none reported that no reports underwent this level of QC.

These findings suggest that although QC is being performed at the Administrative Check level to some extent, it is not consistently applied to all reports.

20. At our unit, Quality Control of reports is performed at level 2, Proof Check.

A Proof Check involves assessing whether the report contains spelling or grammatical errors that should be corrected.

50% of the managers reported that only a few reports underwent Proof Check, while 40% reported that most reports underwent this level of QC. Only 10% of the managers reported that all reports underwent Proof Check, and none reported that no reports underwent this level of QC.

These findings suggest that although Proof Check is being performed to some extent, it is not consistently applied to all reports. The results could indicate that there may be areas for improvement in QC practices at the unit.

21. At our unit, Quality Control of reports is performed at level 3, Sense Review.

A Sense Review involves assessing whether the report author presents the result in a clear, understandable, and coherent manner for a reader without particular technical expertise.

60% of the managers reported that only a few reports underwent Sense Review, while 40% reported that most reports underwent this level of QC. None of the managers reported that all reports underwent Sense Review, and none reported that no reports underwent this level of QC.

These findings suggest that Sense Review is not being widely applied to all reports at the unit. The results could indicate that there may be a need for improved implementation of QC practices for Sense Review or that this level of QC may not be deemed necessary for all reports produced at the unit.

22. At our unit, Quality Control of reports is performed at level 4, Conceptual review.

Conceptual Review. A Conceptual Review is a thorough control of the report content describing the result of the investigation but does not include verification of findings/results. The focus is directed toward the scientific and logical foundation of the report. Assessing the relationship between the evidence and the conclusion is of key importance.

90% of the managers reported that only a few reports underwent Conceptual Review, while 10% reported that most reports underwent this level of QC. None of the managers reported that all reports underwent Conceptual Review, and none reported that no reports underwent this level of QC.

These findings suggest that Conceptual Review is not being widely applied to all reports at the unit, with the majority of reports being subjected to only limited QC at this level. The low level of implementation of Conceptual Review may indicate that this level of QC is not deemed practical for all reports produced at the unit or that there may be barriers to its implementation, such as a lack of resources or expertise.

23. At our unit, Quality Control is performed at level 5, Sampled Verification Review.

A Sampled Verification Review verifies selected findings from the report by using a different tool/method than used in the original examination. 60% of the managers reported that only a few reports underwent Sampled Verification Review, while 30% reported that none of the reports underwent this level of QC. Additionally, only 10% of managers reported that most reports underwent Sampled Verification Review, and none of them reported that all reports underwent this level of QC.

24. At our unit, Quality Control is performed at level 6, Full Verification Review.

A Full Verification Review involves verification of all reported results by using a different tool/method than used in the original examination.

50% of the managers reported that only a few reports underwent Full Verification Review, while the other 50% reported that none of the reports underwent this level of QC. None of the managers reported that most or all reports underwent Full Verification Review.

These findings suggest that Full Verification Review is not being widely applied to reports at the unit, with either no or limited QC at this level.

25. At our unit, Quality Control is performed at level 7, Re-examination.

A Re-examination means that the full examination is done a second time by personnel with no former knowledge of or involvement in the case. 70% of them reported that no reports undergo Re-examination, while 30% reported that only a few reports undergo this level of QC. None of the managers reported that most or all reports undergo Re-examination.

These findings suggest that Re-examination is not being widely applied to reports at the unit.

Summary of managers' responses to the amount of Quality Control being performed

QC of reports is being performed to some extent, but it is not consistently applied to all reports. Administrative Check is the most widely used level of QC, followed by Proof Check and Sense Review. Conceptual Review, Sampled Verification Review, Full Verification Review, and Re-examination are not being widely applied to reports at the unit. The low level of implementation of Conceptual Review may indicate that there may be barriers to its implementation, such as a lack of resources or expertise. Re-examination is not being widely applied to reports at the unit. Overall, the findings suggest that there may be a need for improved implementation of QC practices at the units to ensure consistent and comprehensive QC of all reports produced.

The employees: Questions 26 to 32

After the survey data is presented in table form, questions 26 to 32 will be analyzed to further investigate employee QC practices, followed by a short summary of findings.

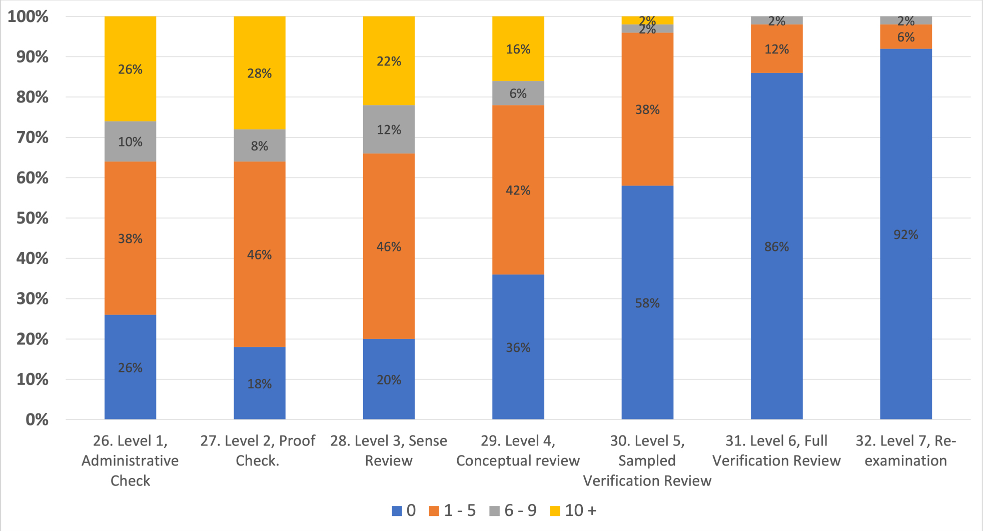


Figure 4.10: Number of Reports Subject to QC in the Last 12 Months, as Reported by Employees

26. To what extent have you performed Quality Control at level 1, Administrative Check during the last 12 months?

An Administrative Check entails controlling whether the investigation is performed in compliance with formal requirements and according to the agreed assignment – meaning, the agreed tasks have been performed on the seized devices.

26% reported that they did not perform any level 1 Administrative Check QC on any reports in the last 12 months. 38% reported performing QC on 1 to 5 reports, while 10% reported performing QC on 6 to 9 reports. Finally, 26% reported performing QC on 10 or more reports during the last 12 months.

This means that 74% of the respondents answered that they had performed at least one administrative check during the last 12 months, and as many as 26% of the respondents had performed administrative checks on more than ten reports.

27. To what extent have you performed Quality Control at level 2, Proof Check during the last 12 months?

A Proof Check involves assessing whether the report contains spelling or grammatical errors that should be corrected.

18% of the respondents did not perform any proof checks on reports during the last 12 months. 46% reported performing proof checks on 1 to 5 reports, while only 8% performed proof checks on 6 to 9 reports. The remaining 28% of respondents performed proof checks on 10 or more reports during the last 12 months.

The data suggests that a majority of employees performed at least some level of Proof Check QC during the last 12 months, with 82% of respondents reporting performing Proof Checks on 1 or more reports. However, the data also indicates that a significant portion of respondents (18%) did not perform any Proof Checks, suggesting a potential area for improvement in QC practices.

28. To what extent have you performed Quality Control at level 3, Sense Review during the last 12 months?

A Sense Review involves assessing whether the report author presents the result in a clear, understandable, and coherent manner for a reader without particular technical expertise.

20% of the respondents reported not performing any Sense Review QC on reports during the last 12 months. 46% of the respondents reported performing Sense Reviews on 1 to 5 reports, while 12% performed Sense Reviews on 6 to 9 reports. Finally, 22% of respondents performed Sense Reviews on 10 or more reports during the last 12 months.

The data indicates that while a majority of employees (80%) performed at least some level of Sense Review QC during the last 12 months, there is still room for improvement. Specifically, 20% of respondents did not perform any Sense Review QC, which could have implications for the overall quality of the reports being produced. Additionally, only a small percentage of respondents (12% and 22%) performed Sense Reviews on a higher number of reports.

29. To what extent have you performed Quality Control at level 4, Conceptual Review during the last 12 months?

Conceptual Review. A Conceptual Review is a thorough control of the report content describing the result of the investigation but does not include verification of findings/results. The focus is directed toward the scientific and logical foundation of the report. Assessing the relationship between the evidence and the conclusion is of key importance.

36% of the respondents did not perform any Conceptual Review QC on reports during the last 12 months. 42% of the respondents performed Conceptual Reviews on 1 to 5 reports, while only 6% performed Conceptual Reviews on 6 to 9 reports. Finally, 16% of the respondents performed Conceptual Reviews on ten or more reports during the last 12 months.

The data suggests that there is room for improvement in the area of Conceptual Review QC. 78% of the respondents performed Conceptual Reviews on five or fewer reports, with over 36% reporting that they did not perform any Conceptual Reviews. This indicates a potential gap in the level of control being applied to report content, which could impact the scientific and logical foundations of the reports. Furthermore, 22% performed Conceptual Reviews on higher numbers of reports, indicating potential variation in QC practices across employees.

30. To what extent have you performed Quality Control at level 5, Sampled Verification Review, during the last 12 months?

A Sampled Verification Review verifies selected findings from the report using a different tool/method than used in the original examination.

58% of the respondents did not perform any Sampled Verification Reviews on reports during the last 12 months. 38% of respondents performed Sampled Verification Reviews on 1 to 5 reports, while only 2% performed Sampled Verification Reviews on 6 to 9 reports.

The remaining 2% of respondents performed Sampled Verification Reviews on ten or more reports during the last 12 months.

The data suggests that there is a significant gap in the level of Sampled Verification Review QC being applied to reports. 58% did not perform any Sampled Verification Reviews, which could have implications for the accuracy and reliability of the findings in the reports. Additionally, only a small percentage of respondents performed Sampled Verification Reviews on higher numbers of reports, indicating that this level of QC may not be standard practice across the organization.

31. To what extent have you performed Quality Control at level 6, Full Verification Review during the last 12 months?

A Full Verification Review involves verification of all reported results by using a different tool/method than used in the original examination. 86% of the employees did not perform any Full Verification Review during the last 12 months, while only 12% performed Full Verification Reviews on 1 to 5 reports. 2% performed Full Verification Reviews on 6 to 9 reports, and none of the respondents performed Full Verification Reviews on ten or more reports during the last 12 months.

The data indicates that Full Verification Review QC is not widely practiced across the organization, with 86% of the respondents answering that they had not performed any Full Verification Review during the last 12 months.

32. To what extent have you performed Quality Control at level 7, Re-examination during the last 12 months?

A Re-examination means that the full examination is done a second time by personnel with no former knowledge of or involvement in the case.

92% of the respondents did not perform any Re-examination QC on reports during the last 12 months. 6% of the respondents performed Re-examination on 1 to 5 reports, while 2% performed Re-examination on 6 to 9 reports. None of the respondents performed Re-examination on ten or more reports during the last 12 months.

This data suggests that Re-examination QC is not widely practiced across the organization. With 92% of respondents indicating that they did not perform any Re-examination during the last 12 months

Summary of employees' responses to the number of Quality Controls conducted in the last 12 months

26% performed administrative checks on 10 or more reports during the last 12 months, while 74% performed at least one administrative check. 18% of employees did not perform any proof checks, 46% performed proof checks on 1 to 5 reports, and 28% performed proof checks on 10 or more reports during the last 12 months. 20% of employees did not perform any sense review, while 46% performed sense reviews on 1 to 5 reports. 36% of employees did not perform any conceptual review, while 42% performed conceptual reviews on 1 to 5 reports. 58% did not perform any sampled verification review, while 2% performed it on 6 to 9 reports. Full verification review and re-examination were not widely practiced across the organization, with 86% and 92% of the employees not performing them, respectively.

Overall, the data suggests that there is room for improvement in QC practices, particularly in the areas of proof checks, sense review, and conceptual review. Additionally, there may be variations in QC practices across employees, with some performing QC on a higher number of reports than others. The gaps in QC practices could have implications for the overall quality, accuracy, and reliability of the reports being produced.

4.2 Interview

All participants in this part of the study were managers of a DF unit. The participants included both men and women. To distinguish between the participants, I will refer to them as Digital Forensics Managers (DFM) and assign them numerical identifiers (e.g., DFM1, DFM2, and so on). To ensure confidentiality, I will use the pronoun "they" when referring to the statements made by each participant during the interviews. The analysis of the interviews resulted in the following main themes:

- Roles and risk within the digital forensic process
- Perception of risk
- Administration of Digital Forensics
- Attitudes towards Quality Control
- Perceived trust

The themes of roles and risk, perception of risk, administration of DF, attitudes towards QC, and perceived trust provide valuable insight into the digital forensic process and management of risk within the field. By exploring these themes, we can gain a better understanding of how digital forensic processes are managed, the perceived risks involved, and the attitudes toward QC and trust within the field.

4.2.1 Roles And Risk Within The Digital Forensics Process

All the participants were asked to identify who was doing what in relation to the different phases of the DF process as described in section 2.2. Another significant part of the interview consisted of a risk assessment of work done in the various phases of the DF process. Respondents were asked to assess risk against three predefined values, as explained in section 3.2.4.

I expected to find that the DF examiner had a dominant role in most phases of the process, either in the form of an advisory role or as a practitioner. And that some phases were supported by other participants like first responders, investigators, or DF liaisons. But the situation described by the DFMs was different. The role in practice appears to be mainly focused on the acquisition of data from seizures and facilitating the content analysis conducted by investigators.

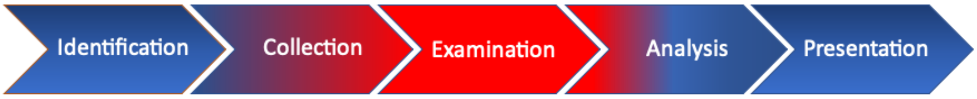


Figure 4.11: The red gradient area illustrates where the role of the DF examiner is most apparent in the DF process.

Competence was a term that was highlighted by the respondents when they described the risk in the different phases of the DF process. In this context, they discussed competence in relation to DF, not the overall competence. A situation was described where personnel that is highly competent within their own respective professions (e.g. investigators, prosecutors, judges) are given responsibilities in relation to DF work that they do not have sufficient training to do without risking inaccurate findings. Investigators are performing analysis of seized digital evidence without being given proper training, guidelines, or support. Investigators were involved in many of the different phases. During the analysis phase, they were set to find evidence, report on their own findings, and then decide if they needed to get their findings validated before presenting them to the prosecution.
Prosecutors and members of the court are presented with reports describing findings from such analysis without the opportunity to validate if the findings are accurate.

> *I know of cases where we have quite randomly stopped people from going to court and alleging that people have done something they absolutely did not do ...*

DFM2

Table 4.4 contains an identified risk from each phase of the DF process. The risks identified are a result of assessments made by the respondents.

Ph[1]	Risk	Effect	Existing measures	C[2]	P[3]	Risk
1	Not enough competence to correctly identify and handle digital evidence	Evidence is not found / The matter is not properly presented	Internal routines describing procedures	3	2	**6**
2	Lacking knowledge about the different acquisition methods	accidental loss of evidence / The matter is not properly presented	Continuous information campaign	3	3	**9**
3	Competence in using tools	Wrongful interpretation of evidence/evidence isn't presented for analysis	Workshops	3	3	**9**
4	Overall competence in the analysis of digital evidence	Misinterpretation of data /Misrepresentation of findings	Voluntary Quality Control	3	3	**9**
5	DF examiners are trusted as expert witnesses	Misunderstood / Not challenged	None	3	3	**9**

Table 4.4: Risk assessment of the DF process

[1] Phase in the DF process.

[2] Consequence

[3] Probability

Identification

The identification phase is mostly dominated by first responders, investigators, and DF liaisons. This also seems to be the issue for the identification phase during iterations of the DF process, DF examiner most often only participate in identifying new evidence sources if they have been asked to do so. The DFMs express a desire for early involvement. But they describe a need for routines that ensure early involvement. Another issue is that they are only available during regular working hours, which again means they do not get involved early in most cases.

> *Often it is an investigator at the GDE or FEFE who carries out a search and does, for example, seizures of physical units as evidence and brings them in. And in the bigger cases, if there are special considerations to account for, I send people from the technical side, or DPA investigators, to assist them.*

DFM5

When describing risk in the identification phase, a common theme was availability. The DF units availability outside office hours and the availability of personnel with adequate understanding and training in finding and identifying digital evidence. One of the DFM described it as challenging that it is others than those within the field themselves who assessed whether there was a need for someone with knowledge of DF in this phase. It could then become completely random how one related to digital evidence early in the investigation, and it could be difficult to correct this at a later stage. A mitigating measure described by the DFM was availability outside office hours. But this had not been prioritized in any of the respondents' police districts.

> *In my police district, there is no service outside regular business hours, so we rarely contacted or considered in the cases.*

DFM2

But the DF examiner is not completely absent; most of the DFMs say that they do participate in major cases or when it is suspected that there may be a question of high operational security in the form of encryption and the like, either by physical presence during the search or as support by telephone.

Collection

In the collection phase, the DFMs are clear that the DF environment carries out the acquisition. But it turns out that this mainly applies to traditional digital sources such as PCs, laptops, hard drives, and the like. Most have made equipment available for DF liaisons or investigators, who have a little extra training, allowing them to acquire data from sources such as mobile phones and tablets. This is not instead of services from the DF units but in addition to. Investigators or DF liaisons also solve most acquisitions from the Internet. DF examiners contribute in cases where tokens and special programs are used to carry out the acquisition from the internet.

Risks described by the DFM in his phase were related to tools, training, time, and lack of quality assurance systems within DF. Failure to choose the correct method to acquire the evidence was associated with training and cost. The different DFM described differences in which tools were made available for them and lack of training in the use of the tools they had access to. One DFM pointed out that the police districts could have significant differences regarding which tools they had access to. Economics is a decisive factor in determining which tools the different police districts have access to and whether they have access to courses on how to use them.

> *... when DPA is acquiring evidence from devices, I consider it a risk that we are completely at the mercy of the fact that we have tools that do things for us ...*

DFM2

All but one DFM had DF liaisons or investigators that were participating in the acquisition from evidence sources such as mobile phones and internet accounts. These were, in most cases, given access to one tool to complete the task, and the DFMs worried that they didn't have enough training to understand when they should use the tool provided and when to as for help. Another issue that was described was that in some situations, data from the devices were only captured with screenshots after doing a manual review of the seizure. And that in some cases, the seizure was delivered to the DF unit for acquisition after a manual review was performed. One of the DFMs thought this might be due to time constraints and a lack of understanding.

Two of the respondents described situations where a lack of quality assurance led to the wrong digital storage being acquired, which subsequently resulted in incorrect data being made available for investigator content analysis. The discovery of the error was entirely accidental.

> *What happened to us was that we imaged the disk of the forensic computer, which contained child abuse material. The disk we were supposed to image did not contain any child abuse material. The person in question could have risked being convicted of child abuse material we have "planted" ...*

DFM4

A risk that was pointed out was time and resources. That failure to identify the important evidence sources early enough could result in that one no longer having access to an evidence source, or it was remotely deleted. This was also somewhat linked to a low understanding related to where digital evidence could be located. A situation that was used as an example was that the opportunity to acquire the correct evidence was lost due to misunderstandings in relation to where the data was stored. The investigators had focused on the acquisition of the mobile phone and did not realize that the information that they were seeking was stored online on a social media service, and since so too much time was spent on acquiring data from the mobile phone and preparing this data for analysis, the access to the social media was lost. This situation was linked to low capacity within the DF units and the DF competence of the investigator writing the mandate.

> *The good old example is that a seized phone is put in a seizure room, and then what you are looking for is actually on the internet.*

DFM2

Examination

The examination phase is dominated by the DF examiners, and three risks stood out, and these were related to training, time, and examination of evidence acquired by others than those within the DF unit.

Investigators and DF liaisons that are given training in how to use mobile extraction software like XRY or UFED are also preparing the seized evidence for content analysis using the software suite included with the acquisition software and do not necessarily consider other tools that could be more suitable. This exposes a risk in the examination of evidence acquired by DF liaison and others; this evidence was mainly processed for analysis with the processing tool provided with the acquisition tool (e.g., Cellebrite Physical Analyzer or MSAB XAMN). The DFMs were afraid that evidence was not found during this process and that databases or other data structures that were not interpreted by the tools were not considered.

There was a consensus that there was too little focus on training in the tools that were used when preparing data for analysis. Too often, evidence was processed through one of the tools at hand, and little else was done to make data stored on the evidence available for the investigators' content analysis. And when this is combined with the fact that the DF examiner was not given training in how to use the tool and insight into how the data was processed, this was considered a risk by the DFMs. They describe that there is a big difference in the results provided by software like, for example, MSAB XAMN and Cellebrite Physical Analyzer, that data presented in one tool can be absent in another. Knowledge about what artifacts the different tools are able to analyze and when it is appropriate to use what tool when preparing seizures for content analysis is crucial when deciding which tools to use. One of the DFM describes that many of the cases were processed like part of assembly line production, that they only had enough time to properly assess the major cases or the ones that were considered technically challenging.

> *We only have resources for the most serious cases. We also work on the less serious ones, but then it becomes more like an assembly line. We whizz through, and "You are welcome." We do few checks there.*

DFM3

There is a focus on competence and skills within the DF units, but they lack the funding to provide the employees with training in the tools they are using on a daily basis. To compensate for not being able to provide the staff with professional training courses in tools, they organized workshops and attended free classes and webinars whenever they are available. One of the DFMs describes the situation as amateurish and says they feel ashamed of the situation, but explained there is a limit to what you can achieve without being allocated funds. They seemed affected and showed discomfort when talking about the issue.

> *We try to have workshops and take free tool classes, if you know what I mean. Webinars and such, it feels pretty amateurish.* ***So this is something I'm ashamed of, that we haven't made it work, but I'm at the mercy of someone coming with money, and that, eh, yes.***

DFM2

Analysis

The analysis of processed data is primarily conducted by investigators, with DF examiners only occasionally evaluating the investigators' findings. Typically, the data presented to investigators is the result of an automated process, where a DF examiner has used commercial tools such as Magnet Axiom or Griffeye Analyze DI to prepare the data for content analysis. During the analysis process, there are several risks to consider, such as tools that fail to interpret the data, tools that misinterpret data, reviewers who lack an understanding of digital evidence, and personnel who lack proficiency in using the tools.

According to one DFM, the process is comparable to an assembly line, driven by economic factors that have a positive impact on the capacity of the DF unit.

> *The content analysis is an entirely different matter; there, it is a bit more like "forensics as a service," a bit of the principle of an assembly line.*

DFM6

During the interviews, the DFMs expressed concerns about the competence level of investigators tasked with reviewing digital evidence seizures. They noted that there are no formal requirements for investigators to meet before conducting an analysis of digital evidence. While some DF units attempt to mandate training before granting tool access, there are no organization-wide requirements in place. The DFMs also highlighted the absence of common guidelines for conducting digital evidence analysis and a lack of systematic training for the tools used in the process. One DFM recounted experiencing pushback from investigator leaders when attempting to make minimum tool training mandatory. Training courses can be costly, and therefore, many DF units attempt to provide introductory sessions on the tools they utilize to offer a starting point for investigators. However, the DF examiners themselves are not always trained in the use of the tools.

> *Our investigators primarily do this with different backgrounds, skills, and training. And with different prerequisites to do a thorough and good enough job. Some, depending on the person in many ways, don't ask for help. They start going through, you know, and then they click around and search, pull in a few keywords, and no, there's a lot. I think there is a considerable risk of missing information here.*

DFM1

Some DFMs described differences in perceived competence between the different investigative environments. Investigators in the central units have a better understanding of DF and access to better training than investigators who work combined duty at smaller duty stations.

There is a slight difference between the investigative environments that are established and sound and those that have combined duty at the good old "sheriff's" offices that are now called police stations. They struggle more with it because they don't understand what they are handed over from us, so we occasionally have to assist them.

DFM3

When the analysis of the seizure is only based upon the results of parsing of data types that are known by the tools available, without any kind of verification to see if there are databases and other data structures that could hold pertinent data that are not parsed, then you introduce a risk that your investigative case is missing information. The big manufacturers of tools that are used by law enforcement are typically not based in Norway, and we can not trust these manufacturers to include parsing and analysis of applications that are developed in and for the Norwegian market. Most such applications are not automatically parsed by commercial tools but can still hold information that could provide pertinent information and potential evidence for use in criminal investigations. The DFMs used applications like Vipps and Skyss as examples of such applications that could hold communication and location data. One of the DFMs says they try to hold information meetings and attend paroles and such to get the information out in their organization, but they are too few to manage that and the DF tasks they are supposed to handle.

Presentation

The majority of analysis in DF is carried out by investigators and DF liaisons, with DF examiners involved only occasionally. This has resulted in a decrease in the number of reports produced by DF examiners regarding digital evidence findings.

Although we verify a lot, we write some reports but less than before, but that is because we have outsourced a lot of the work.

DFM6

The participants of the study have emphasized the significance of engaging DF examiners in the process of assessing the outcomes of investigators' discoveries. There was a worry that one had too little focus on controlling the results describing the results of reviews and analysis. After a report is delivered in the system, there is very little chance it will ever be challenged. And it is worrying that the investigators' reports after review were not subject to any control and that it was up to the investigator himself to request that findings be validated. None of the practitioners of tasks within DF are infallible; therefore, one needs a system that safeguards and ensures a certain quality that protects the legal protection for those involved.

At the same time, you see a considerable risk with the usual investigator doing a huge part of the work in those phases, especially in the review and presentation phase.

DFM1

During the interviews, examples were given that showed that most of the DFMs had experienced reports with wrongful descriptions of findings during analysis or that they had included wrongful conclusions that were detected days before they were supposed to be presented in court or during the court proceeding. And as they describe it, it was completely accidental that it was discovered; they don't really have a system to pick up such errors.

The issue of investigator competence in the analysis of digital evidence is a significant concern, as some investigators may make claims that exceed their expertise. In certain cases, it has been observed that reports from investigators contain claims that cannot be substantiated in court. Such lack of expertise can result in claims that cannot be supported by the evidence, and this can have serious implications for the outcome of a case.

When there are no quality standards or quality assurance systems, this is something that DFMs have experienced, and worry could easily happen again. As one of the DFMs said, "I can't say it won't happen because I've experienced it several times." It is important to have a system that safeguards and ensures a certain quality to protect legal protection for those involved in DF.

> *... when we check what they have written, we have to simply tell them: "Listen, you cannot write it like that because what you say there you cannot stand for in court."*

DFM5

It has been observed that requests for analysis of digital evidence in a case have been received in close proximity to the trial date, leaving limited time for comprehensive examinations and analysis. This time constraint poses a risk to the quality of the investigations, as the investigators may not have sufficient time to conduct thorough analysis before presenting their findings in court. Such requests for analysis should be submitted in a timely manner to ensure that the proper amount of time can be allocated for thorough investigations and analysis.

> *... the request has come so late that we haven't had time to do the necessary analysis before it goes to court.*

DFM1

4.2.2 Perception Of Risk

When examining risk in the context of DF, it is crucial to take into account participants' understanding and perception of the concept. Prior to conducting a risk assessment, the participants were asked to provide their own definitions of risk and their thoughts on potential risks associated with DF. One of the DFMs placed a particular emphasis on the possibility of negative outcomes or errors as a central aspect of risk. According to this DFM, risk involves the danger of things going wrong, such as missing important evidence or making other mistakes.

> *... how big is the chance that something will go right or wrong, but wrong in the first place.*

DFM1

Another DFM described the risk as the amount of chance one is willing to take to achieve a goal or complete a task. They explained that risk is inherent in DF and that understanding and managing it is essential to completing a job successfully. This perspective suggests that risk can be seen as a tradeoff between the level of uncertainty and the expected outcome of a task. In other words, the higher the risk, the greater the potential reward, but also the greater the potential for negative outcomes.

> *..risk. It is, in a way, how much chance you are willing to take, how much chance you are willing to take to achieve a goal.*

DFM5

Risk is the potential for something to go wrong, and in DF, perceived risk can be mitigated by prioritizing thoroughness and precision. This emphasis on meticulousness is highlighted by one DFM, as it minimizes or prevents potential risks. Given the potential consequences of errors in the DF process, it is crucial to implement risk mitigation measures. Mistakes can occur in various aspects of digital forensic work, which increases the risk to legal safeguards. This is a significant concern that requires a focused approach.

While quality assurance has always been important in DF, it has gained increased attention from researchers and practitioners in recent years due to the significant potential for errors in the field. As such errors can compromise legal safeguards, there is a growing need for greater emphasis on risk mitigation measures and a more thorough and accurate approach to all aspects of digital forensic work and research.

> *It is the risk to the legal safeguards, that perhaps primarily affects us to a considerable extent, so this is something that we have to focus on.*

DFM6

One of the DFMs expressed the weight of the responsibility they feel when it comes to managing risk in their work. They emphasized that risk assessment is an integral part of operative police work, and proper training is provided for it. In situations where the safety of the team or the quality of the task solution may be compromised, choices that prioritize safety and quality are always preferred over efficiency. This is similar to how it would be unacceptable for a patrol driver to take risks that could harm the team or the task's outcome. In contrast, the entire organizational structure surrounding operative police work is designed to prioritize risk mitigation and quality assurance, with measures such as yearly training, equipment focus, and dispatch center protocols. However, DFMs in digital policing feel there is no similar safety net in place to mitigate risk and ensure quality.

> *...in relation to digital forensic work, nobody in the police system cares about that except us working in the field.*

DFM2

The DFMs have reflected on the potential impact of inadequate training in DF tools such as Magnet Axiom and Cellebrite Physical Analyzer and how it may affect legal safeguards. Merely possessing a few academic credits in DF is not sufficient to operate these tools effectively and prevent the risk of missing vital information or presenting false evidence.

One DFM highlights the presence of risks throughout the entire DF work process, with the analysis or review of data from seizures identified as the phase where the risk for errors is most significant. During the review of seizures, the risk of errors is particularly significant, as individuals who lack an understanding of the data may be responsible for making decisions in the context of criminal law. This situation may arise when investigators lack the necessary expertise to assess the information properly and instead rely on their intuition or "gut assessments" when determining the appropriateness of the evidence. Such situations can lead to miscarriages of justice when the prosecution and courts rely on incorrect information or assessments. Consequently, there is an ongoing risk throughout the DF process, which underscores the need for comprehensive measures to minimize these risks.

> *... and then there is a risk when reviewing seizures, that is probably the biggest risk, where those who do not understand the data should be the ones who enter the criminal law into it.*

DFM4

4.2.3 Administration Of Digital Forensics

The development of DF within different police districts varies due to financial constraints and differences in investment priorities. The police districts vary in their capacity, with some having access to expensive tools but lacking personnel, while others do not have the resources to allocate to either personnel or tools. Due to budget limitations, few police districts prioritize training for tool usage. However, it is anticipated that a significant number of tasks will be executed outside the professional environment, with the expectation of being supported by the professional environment through training and guidance. The units lack the necessary resources to carry out the tasks assigned to them effectively. They also find it challenging to balance casework with other competing priorities, such as developing their own competencies and operating the required systems.

> *Perhaps understanding is the word. Knowledge on the part of the management, if one is not going to go into detail at the infrastructure level and such. But at least as I experience it, we work a lot with justifying the economics of it, training and equipment, and everything possible. And that you still don't see that there must be more than a handful of people in a district working with digital policing in 2023; that's very; I find it strange …*

DFM1

The addition of new tasks and requirements to DF units without proper reinforcement is leading to the outsourcing of tasks, according to some DFMs. One area that has been particularly affected is the review of seizures and documentation of analysis. While the unit still performs some verifications and report writing, these tasks have been reduced due to outsourcing.

> *We write fewer data technical reports now than we did a few years ago, but it is because that part of our tasks is being carried out by others.*

DFM6

Infrastructure

It has been observed that many DF examiners spend a significant amount of their time and resources ensuring that the IT systems supporting their work are secure and operational. This includes using DF examiners as system administrators, which negatively impacts the unit's ability to produce case-related work. Most of the DFMs believe that Politiets IT-enhet (PIT)(English: The Polices IT unit) (PIT), which is responsible for the IT infrastructure in all police districts, should centrally control this responsibility. There is a clear need for improved IT support from the police IT unit, as the units are currently expected to cover their own infrastructure needs. It is feared that this may lead to less efficient solutions and reduced overall security in the administration of the infrastructure.

> *It is very labor-intensive as things are today, where we internally have to manage and maintain a system for which PIT should strictly be responsible.*

DFM2

The responsibility for acquiring and managing the hardware and software required to support production and analysis in DF units falls on the police districts, which is a source of frustration for DFMs. In cases where resources are already limited, using personnel who are initially employed for DF-related tasks for operational tasks poses significant time constraints. In addition, this situation can lead to differences between the police districts since they may not all choose the same solutions.

> *Those who work as computer investigators or with DF should work with cases and not with keeping their systems up and running, networks and all such things*

DFM5

Training and development

The DFMs have stressed the importance of understanding how the tools that are used work. It is imperative for the examiners to ensure the accuracy of the tools and to verify the results via manual decoding or alternate techniques. Therefore, expertise in the operation and usage of the tools is essential. This training can enhance both the effectiveness and the general quality of the work carried out with the assistance of these tools.

One DFM says that in their unit, workshops are frequently held, usually every two months, as a regular part of their annual training, in which they share experiences. Additionally, they maintain an experience database that they strive to expand when someone discovers a new method, such as how to interpret data or how to conduct reverse engineering on, for example, a new messaging application. The documentation of such methods is shared with others in their unit.

> *... information sharing and expertise sharing are central concepts.*

DFM6

The DF units attempt to provide training for the tools they utilize; however, there is a restricted or absent supply of training from the national level for the most commonly used tools. Units that investigate cases of sexual abuse have been offered courses from the manufacturer of Griffeye Analyze DI, which has been advantageous. Furthermore, a best practice has been established at a national level for content analysis of seizures that contain this type of material. Apart from the training provided for investigating cases of sexual abuse, there is an overall lack of provision for training in tools. Additionally, there is a scarcity of common methodologies for content analysis and a standardized approach for documenting findings as evidence or the absence of evidence.

Perceived anchoring

The development and maintenance of technology-dependent areas such as DF heavily rely on institutional support. However, the organizations surrounding the DFMs lack such support, resulting in inadequate anchoring. Furthermore, there seems to be a mismatch between the national focus area and the lack of commitment and anchoring experienced in the police districts. This discrepancy was recently highlighted in a parole attended by one of the DFMs.

> *... most recently at a police chief's parole last week, where the police chief drew the broad lines from the company's strategy, where digital is very prominent and a high priority, and he excitedly spent a lot of time on it. Where they then moved on to local priorities for 2023, where it shines with its absence; it is not even mentioned in a subordinate clause. So it's like, well, where did it go? Where did it disappear? Were there any black holes on the road? It's kind of thought-provoking.*

DFM6

DFMs have made attempts to employ DF liaisons to alleviate the workload of professionals; however, the implementation of this strategy has proved to be challenging. The personnel designated for this role often have existing responsibilities, which results in the DF liaison role becoming a secondary or tertiary priority. Additionally, there are difficulties associated with developing and maintaining the necessary skills required to function in this role. The responsibilities delegated to DF liaisons vary between different police districts, and there are no uniform training plans or competence requirements. The absence of clear guidelines from national authorities regarding the role of DF liaisons is also a concern. Consequently, there is a demand for national training that addresses the various roles of DF liaisons.

> *The Digital Forensics liaison function has failed; it has been pulverized by GDE managers who have yet to give it priority.*

DFM3

One of the DFMs exemplifies how the DF liaisons role could have offloaded the DF units by describing that, in some cases, multiple investigators are involved in the content analysis of digital evidence with guidance from DF Examiners or DF liaisons if they have enough competence. However, when the investigators are DF liaisons, they typically should have the necessary expertise to perform the content analysis independently. In either case, a quality check should be performed afterward to ensure the accuracy and reliability of the analysis, and additional technical analysis should be conducted when necessary.

Unfortunately, the managers responsible for DF liaisons have shown minimal interest in following up and committing to this initiative, resulting in DFMs losing confidence in the feasibility of this approach.

4.2.4 Attitudes Towards Quality Control

The DFMs were initially positive towards QC of work performed in DF. There was little doubt that most saw this as necessary to increase the safety of those involved in the process, whether they be defendants, victims or digital forensic experts themselves. At the same time, it was perceived as a new task, and thus a task that was associated with uncertainty and concern. How would they be able to solve yet another task within the existing framework, which is already under pressure, and how would the casework be affected by the need to check the results before they are used as evidence in cases? It was pointed out by several that it would not be possible to implement such control within the available framework, and there was also concern about how it would be introduced - would the digital forensic community be relied on once again to effectuate this?

Challenges such as time and resources were identified as obstacles when discussing QC. It is clear that there are two competing demands: on the one hand, work must be delivered in as many cases as possible, and on the other hand, it must be ensured that the work delivered is of high quality. The DFMs provided several examples of errors made in the processes related to the treatment of digital evidence, where only chance had uncovered the error before it reached the legal system.

> *The problem is that we are small and that it takes time, and we already have a massive backlog of cases, so resources would have to be added. But I want a higher quality of our work and to be deeper into the cases. But we can't do everything.*

DFM1

Time and resource constraints were identified as significant challenges to implementing QC measures. DFMs faced a dual challenge: on the one hand, they needed to deliver work for as many cases as possible, and on the other hand, they needed to ensure that the work met appropriate standards.

> *We may have to cut the case portfolio on the less severe cases. Of course, that will free up capacity so we can carry it out, but at the expense of quite serious matters. And that, yes, most things are possible; it's just a matter of how much you want to sacrifice.*

DFM3

The DFMs provided several examples of errors made in the DF process, where it was only by chance that the error was discovered before it ended up in the legal system. These examples referred to errors in the interpretation of digital evidence, but there were also examples of errors related to the acquisition of data from seizures. These errors could have been avoided if adequate quality assurance and QC systems were in place.

> *For example, that they do not know the difference between cache files and saved images, and that they are unable to interpret the data, which results in them creating an incorrect image of the evidence.*

DFM4

Implementing appropriate measures to avoid incorrect investigations and erroneous conclusions is important, as these may lead to a miscarriage of justice. Such situations can result in scrutiny and investigations of the methods used, which may cause discomfort and negative consequences for the organization and its members. Therefore, suitable mechanisms, such as peer review and QC of reports, should be employed to mitigate the risk of such situations. These measures ensure that investigations are carried out based on sound scientific principles, reducing the likelihood of errors and subsequent negative outcomes.

4.2.5 Perceived Trust

There are concerns regarding others' understanding of the content in reports describing digital forensic work. Several of the Digital Forensic Managers (DFMs) describe leaving the court with the impression that the members of the court did not really understand what was being said. The reports can be quite challenging to read for someone without a background in the field as there are many technical terms used. Some explain that they dumb down the language or use metaphors to try to make the content more accessible, while others are concerned that such simplification of the content may change the context and lead to a loss of important nuances.

The DFMs identified several challenges when personnel without sufficient training in working with digital evidence present digital evidence in court. One emphasized that the police hold enormous trust as witnesses in court but that this trust is something that quickly disappears if it is discovered that we do not know what we are talking about or have presented findings as evidence that later turns out not to stand up as evidence. This can have an impact on the reputation of both the police and the tools we use.

> *And then there is the fact that the police are very persuasive in court, we have a high level of trust, and we are believed. And if it should turn out it was wrong, we will lose the trust.*

DFM4

Trust emerged as a recurring theme in the interviews, particularly regarding the trust that expert witnesses in DF from the police receive when they testify in court. One interviewee notes that they are rarely met with critical questions and are often left with the impression that their testimony is accepted as the whole truth.

> *Trust in the police's practice of digital forensics as a subject that's something I feel is important; I think few understand how important it is beyond our ranks anyway. I don't believe the police system understands the consequence of losing it.*

DFM2

On the one hand, they are forced to outsource tasks to others in the DF process to accommodate the large volume of cases. On the other hand, they are aware of the risk associated with the choice made. Several describe trying to make themselves available to investigators and requesting to at least review reports before they are used in cases. However, this is up to each individual, and there are no guarantees that the correct reports are being examined.

> *Then, in theory, the police can write what they want and conclude what they want. And everyone agrees that this is the truth. And that is... then, there is a relatively large risk that a miscarriage of justice may be committed.*

DFM6

4.2.6 Summary

In this section, I will provide a concise summary of the significant findings within each theme. The aim is to present an overview of the key outcomes and insights derived from the interviews.

Summary of the theme roles and risks within the Digital Forensics Process

Here I will provide a brief summary of findings within each phase of the DF process.

Identification phase :

The identification phase involves first responders, investigators, and DF liaisons, with limited involvement from DF examiners. Risks include limited availability of DF units outside office hours and personnel with adequate training in identifying digital evidence. DFMs express a desire for early involvement in the identification phase, but routines need to be established to ensure this.

Collection phase:

During the Collection phase, DF Examiners are, in most police districts, the only ones involved in the acquisition of traditional sources like PCs, laptops, and hard drives; some police districts provide equipment for DF liaisons to acquire data from mobile devices. Risks include inadequate training, tools, time, and quality assurance. DFMs express concern over investigators lacking knowledge on tool usage and when to ask for help, as well as a limited understanding of where digital evidence may be located and DF unit capacity.

Examination phase:

The examination phase in DF is dominated by DF examiners. Three main risks stood out related to training, time, and examination of evidence acquired by others outside the DF unit. Investigators and DF liaisons are mainly trained to use a specific software suite for processing seized evidence and may not consider other tools that could be more suitable. There is little focus on training in the tools used to prepare data for analysis, and evidence is often processed through one of the tools at hand with little else done to make data stored on the evidence available for content analysis. DF examiners need training in the tools they use on a daily basis to ensure they are competent and skilled. Lack of funding and resources in DF units leads to a situation where staff cannot be provided with professional training courses in tools. They must rely on workshops, free classes, and webinars whenever they are available. One DFM expressed shame over what they described as an amateurish situation in relation to the lack of resources and training.

Analysis phase:

DF analysis is primarily conducted by investigators, with DF examiners only occasionally evaluating their findings. During the analysis process, there are several risks to consider, such as tools that fail to interpret the data, tools that misinterpret data, investigators who lack an understanding of digital evidence, and personnel who lack proficiency in using the tools. There are no formal requirements for investigators to meet before conducting an analysis of digital evidence. While DF units provide introductory training on the tools used, there is a lack of systematic training for both investigators and DF examiners. The DF examiners themselves are not always trained in the use of the tools.

Presentation phase:

DF investigations are predominantly conducted by investigators and DF liaisons, with DF examiners playing a less frequent role. This leads to a reduced number of reports produced by DF examiners and potential challenges in controlling the accuracy of reports. Lack of quality standards or quality assurance systems in DF can lead to claims that cannot be substantiated in court and potentially impact the outcome of a case. Additionally, there is a risk of investigators making unsubstantiated claims in their reports, which could further compromise the investigation's integrity. Limited time for comprehensive examination and analysis is another risk factor that can impact investigation quality.

Summary of the theme perception of risk

The definition of risk varies among participants, but all agree it involves the possibility of negative outcomes or errors. Thoroughness and precision can help mitigate perceived risks in DF. Quality assurance is crucial in DF to prevent potential errors that can compromise legal safeguards. DFMs feel a weight of responsibility when it comes to managing risks, but they feel that there is no safety net in place to mitigate risks and ensure quality in DF. Inadequate training in DF tools can affect legal safeguards and result in the risk of missing vital information or presenting false evidence. Content analysis presents a significant risk for errors, particularly when individuals lack a comprehensive understanding of the data. Making decisions based on incomplete or misinterpreted content analysis can potentially lead to miscarriages of justice. There is an ongoing risk throughout the DF process, highlighting the need for comprehensive measures to minimize these risks.

Summary of the theme administration of DF

Lack of resources and training for personnel in DF leads to outsourcing and compromised efficiency. Improved IT support is needed for the effective administration of DF. A standardized approach to documenting findings is necessary for consistency and accuracy. A clear role and training plan for DF liaisons is needed to ensure they can effectively carry out their duties. Understanding and sharing best practices among units is crucial to enhancing the effectiveness and quality of the work carried out. Institutional support and financial constraints hinder the development of DF, resulting in a mismatch between national focus and district investment priorities.

Summary of the theme attitudes toward Quality Control

Digital forensic managers face challenges with the volume of cases they handle, which can impact the quality of their work and cause backlogs. There are concerns regarding the quality and accessibility of reports describing digital forensic work, which can lead to misunderstandings in court and a loss of trust in the police and their tools. Trust is a recurring theme in DF, particularly regarding the trust that expert witnesses from the police receive when testifying in court. QC measures are seen as necessary but are also associated with uncertainty and concerns about implementation, including challenges related to time and resources. DFMs have identified errors made in the processes related to the treatment of digital evidence, which could have been avoided if adequate QC measures were in place. Implementing appropriate measures to avoid incorrect investigations and erroneous conclusions is important to prevent miscarriages of justice. Suitable mechanisms such as peer review and QC of reports should be employed to mitigate risks.

Summary of the theme perceived trust

Reports describing digital forensic work can be challenging to read for those without a background in the field, as they use technical terms that may be difficult to understand. DF examiners may need to dumb down language or use metaphors to make content more accessible, but this could result in a loss of important nuances. Personnel without sufficient training presenting digital evidence in court can lead to a loss of trust and reputation for both the police and the tools used. Trust emerged as a recurring theme in the interviews, particularly regarding the trust that expert witnesses in DF from the police receive when they testify in court. DFMs try to make themselves available to investigators and request to review reports before they are used in cases, but there are no guarantees that the correct reports are being examined.

Chapter 5

Discussion

In this discussion chapter, I will analyze the results of the empirical study conducted in this thesis. The discussion will be structured thematically, and the research questions will be answered within the themes that best address them. The first theme will explore the DF examiner role within the DF process. The second theme will explore the attitudes of DF managers and examiners towards QC and the extent to which it is currently implemented in practice. The third theme will focus on the perceived risks associated with DF investigations. Finally, the fourth theme will discuss the potential consequences of errors or oversights in the DF process. Throughout the discussion, I will relate the findings to relevant theoretical perspectives to shed light on the study's implications and identify areas for further research.

5.1 The Blurring Role Of Digital Forensic Examiners.

The role of the DF examiner has often been described with reference to the DF process. A frequently cited version was developed by Flaglien(2018), which illustrates the DF process as five stages mainly performed by the DF examiner, except for the identification phase, where Flaglien also describes the role of the first responder as significant. However, this study suggests that the role of the DF examiner deviates significantly from this perception and that it is becoming more blurred and limited. I will discuss each stage of the process to justify this point, starting with the identification phase. By examining the responsibilities of DF examiners at each stage, this section aims to provide a comprehensive understanding of the roles they play in the DF process and what other tasks have been assigned to the role. The discussion aims to answer the following research questions:

What is the digital forensic examiner's role within the DF process in the Norwegian police?

What is the extent of the digital forensic examiner's involvement and responsibilities within the DF process of the Norwegian police?

When investigating the extent of QC in the DF process, it is crucial to identify the practitioners within the DF process responsible for the work that could require control. There is only one role, in relation to DF, within the Norwegian Police that has explicitly described requiring competence in digital forensic investigation, namely the role of Digital Forensic Examiner (Politidirektoratet, 2019, p.22). However, the analysis of the data collected for the thesis indicates that the DF examiner may have a lesser role than expected throughout the DF process and that the decisions made by others within the process might have a greater impact on the results of digital investigations than those of the DF examiner.

Identification phase

First responders such as police patrols are the practitioners within the DF process that often first come in contact with potential digital evidence (Heitmann, 2019, p.98; Flaglien, 2018, p.19). This was also supported by interview data that suggested that police officers on patrol duty and investigators were the first to make decisions that affect the outcome of digital investigations by deciding which digital evidence to seize.

In their thesis, Andreassen and Andresen(2020, pp.86) found that the generalist of Norwegian police is trained to identify digital evidence, seize it, and transport it to the lab for further investigation. They also describe that tasks like live data forensics are performed by NPUC students since the police officers they were paired with did not feel competent to do so (Andreassen & Andresen, 2020, p.84).

When considering the combination of none of the DFMs having personnel available outside normal office hours to support decision-making in the early stages of an investigation. With the fact that the personnel with patrol as their main task often is exempt from the competency-building measures offered in the compulsory annual training for investigators (Heitmann, 2019, p.98), there is reason to question if the initial stages of digital investigations have had too little focus in Norwegian Police. Ideally, first responders would receive support from experienced professionals when dealing with digital crime scenes, but this is often not the case. Based on the interviews with DFMs, DF examiners only participate occasionally, usually in bigger or more complex cases, during the identification and seizure of digital evidence.

Collection phase

During the collection phase, when it comes to the acquisition of evidence, most DF managers reported that they also rely on other practitioners, such as investigators and DF liaisons, to acquire mobile devices and evidence sources from the internet due to workload and backlogs. However, DF examiners are still primarily responsible for traditional acquisitions from laptops and hard disk drives. In my experience, such acquisitions are, in some police districts, performed by investigators and DF liaisons as well.

Given that this phase might require access to various methods and tools in order to get a proper acquisition, it was expected that DF examiners would have a more prominent role (Horsman & Sunde, 2022, p.6). According to most of the DF managers interviewed, practitioners outside the DF units often lacked training and access to tools, potentially affecting the quality of acquisitions.

Examination phase

During the examination phase of the process, the DF examiner plays a significant role. Most of the DFMs interviewed emphasized that only their units are doing the parsing and pre-processing of data, preparing it for content analysis or technical analysis. However, this was an accurate description. During the RISK assessment in the interviews of the DF managers, it was revealed that DF liaisons and investigators who had received training in data acquisition from mobile devices also were involved in processing data for content analysis, using the automatic parsing available within tools such as for example Cellebrite UFED Physical Analyzer, and that the DF managers were concerned they had too little training within the field of DF and the tools to know how to prepare all the relevant data available in the acquisition. And as for the role of the DF examiner within this phase, one of the DF managers made a comparison to an assembly line and said that they only had enough time to properly assess the major cases or the ones that were considered technically challenging.

Analysis phase

The DFMs described in subsection 4.2.3, an increased workload that has led to backlogs of casework and outsourcing of tasks within the analysis phase that was previously done in the DF units. The analysis of evidence data to develop leads, find suspects and victims, and identify new evidence sources is considered an investigative activity and may not require extensive technical knowledge (Stoykova, 2021, p.11). While the primary objective of a digital investigation is to fulfill information needs and test hypotheses related to the crime, digital forensic science aims to ensure scientific validity regardless of jurisdiction (Stoykova, 2021, p.11). The importance of the analysis phase cannot be understated, as it involves evaluating the data from the evidence against the case hypotheses and assessing whether the findings hold up as evidence.

The interviews with the DFMs revealed that, in the analysis phase, investigators and DF liaisons in most districts conducted most of the content analysis of data prepared in the examination. This was due to an increased workload which had led to low capacity within the DF units. As a result, technical analysis or content analysis by DF examiners was mostly done in larger or more complex cases.

However, what also emerged from the interviews was that most of the analysis phase has been outsourced and reduced to mostly involve content analysis focusing on judicial judgments. This has been done without the support of a safety net in the form of a technical validation of the findings before presenting them as evidence. Therefore, it seems that the role of DF examiners in this phase has been significantly reduced.

Presentation phase

The diminished involvement of DF examiners in the analysis phase, as described by the DFMs during interviews, has led to a decrease in the number of reports documenting findings from content analysis. This is exacerbated by the fact that reports by investigators, which constitute the bulk of documentation for content analysis, as seen from the survey results, are typically not validated. Consequently, there is a reduction in the production of both technical and validation reports. These observations imply that the role of investigators and DF liaisons is significant in this phase, while the role of DF examiners has become less clear.

Balancing competing demands: The Roles of the DF examiner

During the interviews with DFMs, and especially in relation to management covered in subsection 4.2.3, it became evident that the increased workload and staffing shortages were recurring explanations for the reduced capacity of DF examiners. The workload was not just due to an increase in the number of investigative cases but also because DF examiners allocated time to training and competency development initiatives. Moreover, what is described as a lack of support from the PIT meant that DF examiners had to take on the additional role of system administrators responsible for maintaining and operating networks, servers, and computers that support data investigations. These operational tasks have become more complex in recent years with the introduction of systems such as VMWare Horizon, adding to the already heavy burden of maintaining their own competencies.

5.2 Ensuring Quality and Legal Security in Digital Forensic Investigations: A Look At Norwegian Police Practices

There are few empirical studies on QC within the DF process, and most of the studies focus on the work of the DF examiner. The results presented in this thesis suggest that a broader approach is necessary since it appears much of the DF work that would need to be controlled is performed elsewhere. Throughout this section, I will answer the following research questions and give insight into this claim:

To what extent is QC implemented and utilized within digital forensic investigations carried out by the Norwegian Police?

What are the perceptions of managers and employees in the Norwegian Police DF units regarding the value and feasibility of implementing systematic QC measures to improve the quality and reliability of digital forensic investigations and to safeguard the rule of law?

This will be done by drawing on survey and interview data and relating it to relevant earlier research. I will first discuss the current situation and follow up with a discussion on the DFMs attitudes towards QC.

An overview of current practices

The empirical knowledge about QC procedures in the Norwegian police before the current study was scarce. In the qualitative comparative study of DF and forensic science practitioners, Jahren(2020, p.43) found QC was only performed if the DF examiners themselves initiated it, and that it, in general, consisted of a peer review with a focus on a grammar and sense review. This description of the peer review that was initiated could fit into the hierarchy levels 1 and 3 as described by Sunde and Horsman(2021, p.22). Correspondingly, the survey conducted by Haraldseid(2021, pp.45, 61) showed that the result of a content analysis, which usually is performed by other investigators than DF examiners, would not routinely undergo peer review.

Quality Control within DF units

Based on the survey data, there is a lack of a standard structure for peer reviews and QC measures within the Norwegian Polices DF units. The data also suggest that individual examiners have discretion over what they focus on during peer reviews, potentially leading to inconsistent QC practices. Additionally, the lack of sufficient documentation to facilitate QC measures further highlights the need for improved consistency and comprehensiveness in QC measures.

The study by Stoykova et al.(2022, p.11) reinforces the findings from the survey data, where the results indicated that none of the cases included in their survey were sufficiently documented to allow for the assessment of the reliability of the digital evidence, which suggests that the reporting of work done by the practitioners in DF within the Norwegian Police is not consistent. The structure and what to report on in a digital forensic investigation should not be left to individual practitioners. The organization should have defined requirements for the content of reports based on established standards and experience while also meeting the organization's needs. This will enable QC of the work described in the reports (Horsman, 2021, pp.627-628).

To address these issues, the Norwegian Police need to establish standard guidelines and procedures for QC in DF investigations, including defined requirements for the content of reports based on established standards and experience. Adequate resources and training for personnel involved in DF investigations are also necessary to ensure the quality and reliability of evidence presented in court.

Overall, the data suggests that there are individual efforts to implement QC measures, but there are also challenges and limitations in their implementation.

Quality Control of DF in general

The quantitative data gathering in this study mainly focused on the work performed within the DF units. However, some questions were included to assess the QC of work done by other practitioners, such as investigators and DF liaisons. When these findings are considered in the context of the DF investigative process within the Norwegian Police, the answer to the research question would be that there is a low implementation and utilization of QC on work done within this process. According to the survey results, 79% of the respondents reported that investigators and DF liaisons carried out DF work in their police districts. Of these respondents, over 75% reported that they did not perform any QC on this work. An explanation for this could be that this QC was performed by someone else within the organization; in my experience, this would not be the case, but this cannot be ruled out without further research into the topic. QC measures, including peer-review processes, are considered vital in the field of DF. These mechanisms serve as an essential preventive measure, aiming to identify and mitigate potential errors and ensure the integrity of the work before it enters the legal system (Horsman & Sunde, 2020, p.9).

In his recent thesis Haraldseid(2021, pp.68-69) gives a description of the process of performing a content analysis in the Norwegian Police that is not supported by a common methodology. And that there is a need for the mandates used for such investigations to be more purposeful and specific in order to safeguard the legal rights of the accused effectively. There is also a described need for an increased understanding of electronic traces among investigators, prosecutors, and defense attorneys. This was also highlighted by DFMs during the interviews, where also the lack of common guidelines for reports and the understanding of DF as a subject amongst investigators, prosecution, defense attorneys, and the members of the court was defined as one of the risks in the analysis and presentation phases of the DF process.

Haraldseid(2021, pp.69-72) describes a need for a common methodology for how to conduct a content analysis of seizures and a guideline for how to document it in a report. To my knowledge, there has been introduced a national guideline for how to write a report after a content analysis. But there is no common method developed for how the content analysis should be conducted.

Quality Control, a desired measure of inconvenience

The results from both interviews and surveys suggest that there is a growing recognition of the importance of QC practices in digital forensic investigations. Survey data suggests that the employees and managers both agree QC should be integrated into the work process at their units and that DF reports should undergo QC before being used in a criminal investigation. Digital forensic managers interviewed in this study emphasized the need for adhering to recognized standards and best practices in DF, as well as the importance of adequate resources and training for personnel involved in these investigations.

In terms of the feasibility of implementing QC practices, digital forensic managers in this study were explicit in their positive reception and showed a strong desire to implement QC measures. They expressed a keen interest in improving the quality and security associated with the practice of DF. However, at the same time, they expressed concerns. Several saw this as another task that could be assigned to their unit, with an expectation that it should be solved without the provision of resources. And they pointed out that it could have negative consequences for case processing time and the general capacity to perform casework.

5.3 Trust, Reputation, And Risk: The Implications Of DF Management In Norway

The following section will discuss the empirical data collected in this study and analyze it in relation to relevant research to answer the research question:

What are the potential risks to the rule of law, reputation, and trust resulting from the management of DF within the Norwegian Police?

The section will begin with an overview of the DFMs perception of risk and then provide an overview of what was found to be the most significant risks associated with DF and their potential impact on the rule of law and the Norwegian police's reputation and trust.

The DFMs in this study provided valuable insight into their perception of risk in DF, emphasizing the potential negative outcomes and errors as central aspects of risk. They also highlighted the importance of understanding and managing risk, as it is inherent in DF and can be seen as a tradeoff between uncertainty and expected outcome. One DFM emphasized the importance of thoroughness and precision in mitigating perceived risk, as mistakes can compromise legal safeguards.

Table 4.4 describes the most significant risks identified during the different phases of the DF process during the risk assessment that was performed in the interviews. And if one combines these to identify some overarching risks, the following risks emerge:

- The risk that the practitioners involved in the process have insufficient DF understanding to make correct decisions.
- The risk that practitioners have insufficient training in the use of the tools used, which can result in incorrect usage or failure to detect errors.
- The risk of data being misinterpreted and incorrectly presented as evidence in cases.
- The police, and especially specialists, hold a lot of trust as witnesses in court.

All these risks have the possible outcome that if something goes wrong, they can affect legal safeguards and the police's trust and reputation.

The decision-making of practitioners in the DF process can have a significant impact on the overall outcome, as highlighted by Horsman and Sunde (2022, p.174). Their work also suggests that risks can be mitigated by implementing control strategies. However, the interview data presented in this thesis indicate that there are no effective measures in place to account for wrongful decision-making due to insufficient competence and understanding within the Norwegian Police's DF process. When these findings are considered in conjunction with those of Andreassen and Andresen (2020, pp.84-85), which describe a willingness to perform tasks without sufficient training or appropriate skills for several phases of the DF process, one might question whether the Norwegian Police operate with too high a risk when conducting DF work.

The phase where the risk for errors might be most significant is during the analysis phase when performing content analysis, as practitioners who lack an understanding of the data may be responsible for evaluating them in the context of criminal law, using tools they have been given little or no training in how to use. Such situations can lead to miscarriages of justice, highlighting the need for comprehensive measures to minimize risks throughout the DF process. The analysis of the evidence data for developing leads, finding suspects and victims, and identifying new evidence sources does not necessarily require deeper technical knowledge since this is regarded as investigative activities (Casey, 2016, p.A1). Personnel without post-graduate studies in digital investigations and forensics are more likely not to weigh the evidence in compliance with its technical quality and rather rely on judicial reasoning (Erlandsen, 2019, pp.71-72). By only analyzing the seizures with judicial reasoning as a focus, one cannot be certain that the results are valid as evidence since their validity was never tested. The evaluation of evidence found during investigative analysis requires specialized knowledge, formalized processes, testing, research, and quality oversight (Casey, 2016, p.A2).

In their study, Sunde and Dror(2021, p.9) found that DF examiners were prone to cognitive bias, which impacted their decision-making and analysis. To address this issue, they described an urgent need for quality assurance systems and control of DF work. Casey(2018, p.3) contends that in certain contexts, it is not uncommon for experts to exhibit an excessive level of confidence in their arguments and present digital evidence in a manner that benefits their clients. Such behavior can raise concerns about the integrity of their evaluation approach. The absence of training and guidelines for investigators and DF liaisons conducting a content analysis, coupled with the lack of QC and evaluation, raises concerns about the potential for unreliable and invalid digital evidence being presented in court.

The weight of responsibility that DFMs feel when it comes to managing risk is evident. DFMs recognize the need for adequate training to operate DF tools effectively and prevent the risk of missing vital information or presenting false evidence.

However, feedback from interviews reveals that tool courses are often expensive and not feasible within the economic constraints to offer to either DF examiners in their own unit or other practitioners performing tasks such as content analysis. The tools utilized during the analysis and presentation stages of DF are frequently commercially developed. However, recent research has highlighted substantial variations in the output produced by these tools across different versions (Jones & Vidalis, 2019, p.48). Horsman(Horsman, 2019, p.172) highlights the importance of distinguishing tool errors from user errors, which can be challenging since user errors are frequently misinterpreted as tool errors. It is the responsibility of the tool users to be capable of validating the appropriateness of the tool and the methodology they have chosen to employ in their task completion (Tully et al., 2020, p.10). Therefore, having knowledge of the proper use of tools is crucial to comprehend their functionality and identifying erroneous results produced by the tools.

5.4 Walking A Tightrope: Balancing Quality Control And Efficiency In Digital Forensics Investigations

In this section, we will discuss some of the potential consequences of the findings described while also addressing the following research question:

How does the management of DF in the Norwegian Police affect the quality of work within the DF process?

When discussing the management of DF as a field of subject, one has to differentiate between the management at the national and district levels, and therein one might find part of the problem. It is, to a large extent, up to every police district how they organize their effort within DF, and interview data suggests differences in organization and DF capacities between the different police districts. It is not within this thesis's scope to discuss the organization of DF units. It is important to note the differences in DF organization and capacities between the different police districts, as these factors could have an impact on the management of DF as a field of study and practice

The DF units within the Norwegian Police are not in a position to build the missing safety net on their own. During the interviews of the DFMs, it became clear that the strategic decision-makers in the different police districts did not necessarily understand what competence and tools a DF investigation entails. And this could halt the development of the DF units within the Norwegian Police since they depend on them to implement systems that facilitate quality assurance and QC. The consequences of not achieving this can mean that it poses a risk to the rule of law (Casey et al., 2019, p.136).

The results of this study suggest that the leadership in charge of the development of DF as a field of subject has failed to implement training in the tools that are used, adequate training for all personnel given tasks and responsibilities within the DF process and quality assurance systems that help mitigate risk to the rule of law. Additionally, the study found that the DF units are not adequately staffed with the necessary number of specialists to carry out their assigned tasks effectively. Failing to develop and adapt in line with society's technological development can lead to the Norwegian Police falling behind the curve. This can lead to relying on work methodologies not adapted to the actual need and failing to achieve effective work processes (Casey et al., 2019, p.128). Could this be the case for the management and development of units working with DF as a field within the Norwegian Police?

The "outsourcing" of DF tasks has been pointed out in earlier studies as a promising solution to meet the demands for employees with DF skills in combination with investigative skills. However, a prerequisite for success is understanding that such development must be supported systematically and needs anchoring at all levels of the organization. There must be common quality standards, quality assurance systems, common methodology, and training requirements. The involvement of practitioners within the DF process, like investigators and DFDF liaisons without adequate training and a common methodology to support their work, may pose a high risk of mistakes, loss of evidence, and leads due to their potential lack of awareness of the limitations in the tools and methods used (Casey, 2019, p.654). At the moment, none of this is in place, and there is no obvious "quick fix" for the problems that arise in their absence. These issues cannot be solved at a district level, and that could be an ineffective and costly approach. The development of tool courses and methods for securing access to information is not a one-off exercise; needs constantly change as new technology is introduced into society. This solution to the capacity issues within DF can be a risk for the rule of law, reputation, and trust.

Another issue related to management is that the DF units do not have operational support. Most of the DF units operate their own servers, machine parks, and tool portfolios. According to the interview data, this reduces their capacity and might introduce other risks to their operations in terms of loss of data, security, and such.

Chapter 6

Conclusions

This study aimed to investigate the extent of QC utilization in the DF process within the Norwegian Police and explore its potential impact on reputation, legal safeguards, and trust. To find answers to this question, I conducted a survey among all employees in the DF units of the Norwegian Police, as well as interviews with six DF unit leaders. To conclude, I will highlight three important findings:

First, the DF examiner's role is blurring and limited. While still essential in certain stages, the decision-making by other practitioners within the DF process appears to have a greater impact on investigation outcomes. Concerns arise regarding reduced examiner involvement, task outsourcing, and the lack of technical validation of content analysis. Furthermore, the findings indicate that DF examiners spend more time than expected on tasks beyond the scope of the DF process, such as fulfilling responsibilities as system administrators and participating in system development. These additional responsibilities, coupled with competing demands like educating others in the DF discipline and resource constraints due to understaffing, may contribute to their diminishing involvement. It is vital to clarify the role of DF examiners and maintain and strengthen their expertise to ensure the maintenance of quality and validity in digital investigations.

Secondly, it is evident that QC practices in the context of DF work in the Norwegian police lack a systematic approach. Building upon the research conducted by Jahren(2020), this study utilizes the PARS framework to delve into QC practices with greater depth and breadth. Previous research findings indicate that employees themselves primarily initiate QC. By providing empirical evidence on the actual implementation of QC, this study offers valuable insights into the true extent of QC in DF work within the Norwegian Police, emphasizing the need for a more structured and comprehensive approach.

The quantitative data collected during this study clearly demonstrate that, with a few exceptions, there is a notable absence of effective QC measures on the reports documenting DF work conducted within the Norwegian police. Findings show a lack of standardized QC practices within DF units, with individual examiners having discretion over whether and how to conduct peer reviews. The findings highlight the limited emphasis given to QC beyond grammar and sense review, revealing that limited QC extends beyond PARS level 3, which includes sense review.

Additionally, the study reveals the lack of proactive efforts in subjecting reports to comprehensive scrutiny. Another concerning finding was that DF examiners reported having insufficient time to dedicate to executing QC on their work. This time constraint further hinders the implementation of comprehensive QC measures and poses potential risks to the accuracy and reliability of the investigations.

Furthermore, the results indicate that content analysis in the context of DF work is primarily carried out by investigators rather than DF examiners. Additionally, the reports documenting content analysis undergo minimal or no QC measures, such as peer review or validation. This finding, coupled with the absence of standardized guidelines for conducting content analysis, limited training opportunities for the tools used, and investigators' limited training and competence in DF, highlights a significant risk in the Norwegian Police's DF process. This risk poses a threat to the rule of law and underscores the urgent need for improved practices.

To ensure the reliability and validity of content analysis in DF investigations, establishing standard guidelines and procedures for QC, including defined requirements for report content, as well as providing adequate resources and training for personnel, is crucial. This study shows that both managers and employees are positive toward QC. However, it is concerning to observe that they do not believe it is feasible due to understaffing and its potential impact on the increasing backlog of casework.

This study highlights the need for systematic QC measures to enhance the quality, reliability, and legal safeguards of DF investigations in the Norwegian Police.

And finally, how the field of DF in the Norwegian Police is managed poses significant risks, including insufficient understanding and training among practitioners, potential misinterpretation of data, and reliance on trust in court proceedings. These risks have the potential to compromise legal safeguards and the reputation of the Norwegian police. Effective measures, such as quality assurance systems and training, are needed to address these risks and ensure the reliability of digital evidence. Comprehensive measures throughout the DF process, along with adequate resources, are essential to mitigate risks and maintain trust in the justice system.

The interview data pointed towards a lack of sufficient understanding among leaders and strategic decision-makers in the different police districts. This lack of understanding pertains to the competence and tools necessary to practice the profession in a responsible manner. It could potentially result in different organizational structures and capacities across police districts, and it may lead to disparities in perceived legal protection and hinder the development of the DF profession. It is crucial to adapt to technological advancements and provide comprehensive support and alignment when outsourcing DF tasks. The findings of this survey indicate that the Norwegian Police has been outsourcing tasks within the DF process without any focus on training, quality, or the risks involved. This is further highlighted by the fact that several individuals have compared the task execution within certain parts of the DF process to assembly line production, and not in a positive sense.

The study suggests that immediate actions are required to improve training, implement robust quality assurance systems, and ensure sufficient resources for effective and high quality DF practice in the Norwegian Police. Failure to address these critical areas could have consequences for the legal protection of those involved and, in the worst case, lead to miscarriages of justice, jeopardizing the integrity of our legal system. This study's findings show that it is imperative that the Norwegian Police promptly prioritize these necessary improvements to safeguard the integrity of our justice system.

Chapter 7

Future Work

The main focus throughout this study was risks and QC. And future research should focus on evaluating the outcomes and effectiveness of implementing QC measures in digital forensics. Assessing the effects of QC implementation on the quality, efficiency, and reliability of digital forensic work is crucial. Comparative studies between units that have implemented robust QC practices and those that have not can provide valuable insights into the benefits and challenges associated with its adoption. By conducting such research, we can gain a better understanding of the impact of QC implementation and identify areas for improvement in digital forensic processes.

Another finding that would benefit from more research is the different roles within the digital forensics process. This research could focus on improving role definitions and boundaries within the digital forensics process. This includes differentiating training programs and establishing clear role descriptions for digital forensics examiners and other practitioners involved. Studying the impact of these improvements on the quality and efficiency of digital forensic work would be beneficial.

The study also highlights the impact of decisions made by practitioners outside the digital forensics unit, such as limited understanding and training, and challenges like understaffing and time constraints on the quality of digital forensics work. Further research into an AI-assisted framework for decision-making in digital forensics could address these issues and optimize resource allocation.

Researching the potential of an AI support system, trained on comprehensive knowledge of tool operations, can enhance the effectiveness and efficiency of digital forensics investigations. Developing and implementing an AI framework that provides support throughout the entire process, from data acquisition to analysis and reporting, is worth exploring.

Evaluation of the practical feasibility and effectiveness of the proposed AI-assisted framework is crucial. Collaborative experiments with digital forensics units can gather empirical data on the impact of the AI system on decision-making outcomes, resource utilization, and investigation quality.

Bibliography

Andreassen, L. E., & Andresen, G. (2020). *Live data forensics: A quantitative study of the norwegian police university college students ldf examinations during their year of practice* (Master's thesis). University College Dublin.

Årnes, A. (2017). Introduction. Chichester, UK: John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119262442.ch1

Aven, T., & Thekdi, S. (2022). *Risk science: An introduction*. Routledge, Taylor & Francis Group.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology [Publisher: Routledge]. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brinkmann, S., & Kvale, S. (2018). *Doing interviews*. SAGE Publications Ltd. https://doi.org/10.4135/9781529716665

Carrier, B., & Spafford, E. (2004). An event-based digital forensic investigation framework [Publisher: Elsevier]. *Digital Investigation*.

Casey, E. (2004). *Digital evidence and computer crime* (Vol. 2nd ed). Academic Press.

Casey, E. (2016). Differentiating the phases of digital investigations. *Digital investigation*, *19*, A1–A3.

Casey, E. (2018). Clearly conveying digital forensic results. *Digital Investigation*, *24*, 1–3. https://doi.org/10.1016/j.diin.2018.03.001

Casey, E. (2019). The chequered past and risky future of digital forensics [Publisher: Taylor & Francis]. *Australian Journal of Forensic Sciences*, *51*(6), 649–664. https://doi.org/10.1080/00450618.2018.1554090

Casey, E., Ribaux, O., & Roux, C. (2019). The kodak syndrome: Risks and opportunities created by decentralization of forensic capabilities. *Journal of Forensic Sciences*, *64*(1), 127–136. https://doi.org/10.1111/1556-4029.13849

Davidson, C. (2009). Transcription: Imperatives for qualitative research [ISBN: 1609-4069 Publisher: SAGE Publications Sage CA: Los Angeles, CA]. *International journal of qualitative methods*, *8*(2), 35–52.

Digital Forensics Research Workshop. (2001). *A road map for digital forensic research - DFRWS*. Retrieved May 14, 2023, from https://dfrws.org/presentation/a-road-map-for-digital-forensic-research/

Erlandsen, T. E. (2019). *Fallacies when evaluating digital evidence among prosecutors in the norwegian police service* (Thesis).

Etikan, I., & Babtope, O. (2019). A basic approach in sampling methodology and sample size calculation [Publisher: Name: Medtext Publications LLC]. *Med Life Clin*, *1*(2), 1006.

Flaglien, A. O. (2018). *Digital forensics: An academic introduction* (A. Årnes, Ed.). John Wiley & Sons Inc.

Halcomb, E. J., & Davidson, P. M. (2006). Is verbatim transcription of interview data always necessary? *Applied Nursing Research*, *19*(1), 38–42. https://doi.org/10.1016/j.apnr.2005.06.001

Haraldseid, S. (2021). *«kan du stikke opp og gå gjennom databeslaget?»: Fremgangsmåter for innholdsanalyse av databeslag og behovet for metodisk støtte* (Thesis). Politihøgskolen.

Harland, N., & Holey, E. (2011). Including open-ended questions in quantitative questionnaires—theory and practice. *International Journal of Therapy and Rehabilitation*, *18*(9), 482–486. https://doi.org/10.12968/ijtr.2011.18.9.482

Heitmann, O. (2019). *Digital investigation: The malnourished child in the norwegian police family?* (Thesis).

Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics. *Digital Investigation*, *28*, 163–175. https://doi.org/10.1016/j.diin.2019.01.009

Horsman, G. (2021). The different types of reports produced in digital forensic investigations. *Science & Justice*, *61*(5), 627–634. https://doi.org/10.1016/j.scijus.2021.06.009

Horsman, G., & Sunde, N. (2020). Part 1: The need for peer review in digital forensics. *Forensic Science International: Digital Investigation*, *35*, 301062.

Horsman, G., & Sunde, N. (2022). Unboxing the digital forensic investigation process. *Science & Justice*, *62*(2), 171–180. https://doi.org/10.1016/j.scijus.2022.01.002

ISO9000. (2015). *Ledelsessystemer for kvalitet : Grunntrekk og terminologi (ISO 9000:2015) = quality management systems : Fundamentals and vocabulary (ISO 9000:2015)* (Vol. NS-EN ISO 9000). Standard Norge.

Jahren, J. H. (2020). *Is the quality assurance in digital forensic work in the norwegian police adequate?* (Thesis).

Jones, A., & Vidalis, S. (2019). Rethinking digital forensics. *Annals of Emerging Technologies in Computing (AETiC), Print ISSN*, 2516–0281.

Kohn, M., Eloff, M., & Eloff, J. (2013). Integrated digital forensic process model. *Computers & Security*, *38*, 103–115. https://doi.org/10.1016/j.cose.2013.05.001

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design* (Eleventh edition, global edition). Pearson.

Lentz, L. W., & Sunde, N. (2021). The use of historical call data records as evidence in the criminal justice system: Lessons learned from the danish telecom scandal. https://hdl.handle.net/11250/2719778

McKemmish, R. (2008). When is digital evidence forensically sound? In I. Ray & S. Shenoi (Eds.), *Advances in digital forensics IV* (pp. 3–15). Springer US.

Nytt kvalitetsrundskriv – riksadvokaten. (n.d.). Retrieved April 25, 2023, from https://www.riksadvokaten.no/document/nytt-kvalitetsrundskriv/

Peltier, T. R. (2005). *Information security risk analysis* (2nd ed.). Auerbach.

Politidirektoratet. (2019, January 10). Nasjonale rolledefinisjoner med kompetansekrav v1.0.

Riksrevisjonen. (2021, February 2). Undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT [https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-politiets-innsats-mot-kriminalitet-ved-bruk-av-ikt/[Accessed: 2023-03-24]].

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, *42*, 105575. https://doi.org/10.1016/j.clsr.2021.105575

Stoykova, R., Andersen, S., Franke, K., & Axelsson, S. (2022). Reliability assessment of digital forensic investigations in the norwegian police. *Forensic Science International: Digital Investigation*, *40*, 301351.

Sunde, N. (2017). *Non-technical sources of errors when handling digital evidence within a criminal investigation* (Master thesis) [Accepted: 2017-06-15T08:56:24Z Publication Title: 111 + vedlegg]. Politihøgskolen, NTNU, Faculty of Technology, Electrical Engineering, Department of Information Security and Communication Technology.

Sunde, N., & Bergum, U. (2019, May 24). Npl - dataetterforskning – en ungdom med voksesmerter [https://www.parat.com/npl/dataetterforskning-en-ungdom-med-voksesmerter-5410-406272[Accessed: 2023-03-26]].

Sunde, N., & Dror, I. E. (2021). A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making. *Forensic Science International: Digital Investigation*, *37*, 301175. https://doi.org/10.1016/j.fsidi.2021.301175

Sunde, N., & Horsman, G. (2021). Part 2: The phase-oriented advice and review structure (pars) for digital forensic investigations. *Forensic Science International: Digital Investigation*, *36*, 301074.

Tully, G., Cohen, N., Compton, D., Davies, G., Isbell, R., & Watson, T. (2020). Quality standards for digital forensics: Learning from experience in england & wales. *Forensic Science International: Digital Investigation*, *32*, 200905. https://doi.org/10.1016/j.fsidi.2020.200905

Valjarevic, A., & Venter, H. S. (2015). A comprehensive and harmonized digital forensic investigation process model [Place: HOBOKEN Publisher: HOBOKEN: Blackwell Publishing Ltd]. *J Forensic Sci*, *60*(6), 1467–1483. https://doi.org/10.1111/1556-4029.12823

Appendix A

Appendix - Sikt Approvals For Survey And Interview Conduct

A.1 Sikt Approval For Survey

Sikt

Meldeskjema / Kvalitetskontroll innen digitalt politiarbeid / Eksport

Meldeskjema

Referansenummer
389721

Hvilke personopplysninger skal du behandle?

- Adresse eller telefonnummer
- E-postadresse, IP-adresse eller annen nettidentifikator

Prosjektinformasjon

Prosjekttittel

Kvalitetskontroll innen digitalt politiarbeid

Prosjektbeskrivelse

Prosjektet har som formål å kartlegge på hvilket nivå det blir utført kvalitetsikring av rapporter som dokumenterer arbeid innen fagfeltet digital kriminalteknikk (digital forensics).

Begrunn hvorfor det er nødvendig å behandle personopplysningene

Vil benytte telefonnummer og/eller epost adresse i forbindelse med distribusjon av spørreundersøkelse hvor svarene vil være anonyme.

Ekstern finansiering
Ikke utfyllt
Type prosjekt
Studentprosjekt, masterstudium

Kontaktinformasjon, student
Rune Kenneth Bauge, runekba@stud.ntnu.no, tlf: [redacted]

Behandlingsansvar

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)
Lasse Øverlier, lasse.overlier@ntnu.no, tlf: [redacted]

Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?
Nei

Utvalg 1

Beskriv utvalget

Ansatte ved enheter i Politiet som jobber innenfor fagområdet Digitalt politiarbeid

Beskriv hvordan rekruttering eller trekking av utvalget skjer

Rekrutterer ved at ledere med personalansvar for ansatte ved Digitalt politiarbeid i Politiets distrikter og særorgan blir kontaktet og forespurt kontaktinformasjon på de ansatte ved enhetene. Deretter blir hver av de ansatte kontaktet direkte med en forespørsel om deltakelse i en anonym spørreundersøkelse.

Alder
20 - 70

Personopplysninger for utvalg 1

- Adresse eller telefonnummer
- E-postadresse, IP-adresse eller annen nettidentifikator

Hvordan samler du inn data fra utvalg 1?

Elektronisk spørreskjema

Vedlegg

spørreskjema_dpa_v1.docx

Grunnlag for å behandle alminnelige kategorier av personopplysninger
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Informasjon for utvalg 1

Informerer du utvalget om behandlingen av personopplysningene?
Ja

Hvordan?
Skriftlig informasjon (papir eller elektronisk)

Informasjonsskriv

informasjonsskriv_spørreundersøkelse_master.doc

Tredjepersoner

Skal du behandle personopplysninger om tredjepersoner?
Nei

Dokumentasjon

Hvordan dokumenteres samtykkene?

- Manuelt (papir)
- Elektronisk (e-post, e-skjema, digital signatur)

Hvordan kan samtykket trekkes tilbake?

Ved direkte kontakt kan samtykke trekkes, kontakten kan være elektronisk (e-post/sms) eller muntlig.

Hvordan kan de registrerte få innsyn, rettet eller slettet personopplysninger om seg selv?

Innsyn er tenkt håndtert ved at en tar kontakt per e-post for å be om innsyn, slik at en får dokumentert at en har krevd innsyn og når dette ble gitt.

Totalt antall registrerte i prosjektet
100-999

Tillatelser

Skal du innhente følgende godkjenninger eller tillatelser for prosjektet?
Ikke utfyllt

Behandling

Hvor behandles personopplysningene?

- Ekstern tjeneste eller nettverk (databehandler)

Hvem behandler/har tilgang til personopplysningene?

- Prosjektansvarlig
- Student (studentprosjekt)
- Databehandler

Hvilken databehandler har tilgang til personopplysningene?

nettskjema.no

Tilgjengeliggjøres personopplysningene utenfor EU/EØS til en tredjestat eller internasjonal organisasjon?
Nei

Sikkerhet

Oppbevares personopplysningene atskilt fra øvrige data (koblingsnøkkel)?
Ja

Hvilke tekniske og fysiske tiltak sikrer personopplysningene?

- Personopplysningene anonymiseres fortløpende

Varighet

Prosjektperiode
01.09.2022 - 01.06.2023

Hva skjer med dataene ved prosjektslutt?
Data anonymiseres (sletter/omskriver personopplysningene)

Hvilke anonymiseringstiltak vil bli foretatt?

- Personidentifiserbare opplysninger fjernes, omskrives eller grovkategoriseres
- Koblingsnøkkelen slettes

Vil de registrerte kunne identifiseres (direkte eller indirekte) i oppgave/avhandling/øvrige publikasjoner fra prosjektet?
Nei

Tilleggsopplysninger

Sikt

Meldeskjema / Kvalitetskontroll innen digitalt politiarbeid / Vurdering

Vurdering av behandling av personopplysninger

Referansenummer	Vurderingstype	Dato
389721	Standard	26.09.2022

Prosjekttittel
Kvalitetskontroll innen digitalt politiarbeid

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig
Lasse Øverlier

Student
Rune Kenneth Bauge

Prosjektperiode
01.09.2022 - 01.06.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 01.06.2023.

Meldeskjema

Kommentar
OM VURDERINGEN
Personverntjenester har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket.

Personverntjenester har nå vurdert den planlagte behandlingen av personopplysninger. Vår vurdering er at behandlingen er lovlig, hvis den gjennomføres slik den er beskrevet i meldeskjemaet med dialog og vedlegg.

VIKTIG INFORMASJON TIL DEG
Du må lagre, sende og sikre dataene i tråd med retningslinjene til din institusjon. Dette betyr at du må bruke leverandører for spørreskjema, skylagring, videosamtale o.l. som institusjonen din har avtale med. Vi gir generelle råd rundt dette, men det er institusjonens egne retningslinjer for informasjonssikkerhet som gjelder.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til den datoen som er oppgitt i meldeskjemaet.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake.

Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
Personverntjenester vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:
- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen

-formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål

-dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet

-lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER

Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), og dataportabilitet (art. 20).

Personverntjenester vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER

Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Ved bruk av databehandler (spørreskjemaleverandør, skylagring eller videosamtale) må behandlingen oppfylle kravene til bruk av databehandler, jf. art 28 og 29. Bruk leverandører som din institusjon har avtale med.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

MELD VESENTLIGE ENDRINGER

Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-i-meldeskjema

Du må vente på svar fra oss før endringen gjennomføres.

OPPFØLGING AV PROSJEKTET

Personverntjenester vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

A.2 Sikt Approval For Interviews

Meldeskjema / Kvalitetskontroll innen digitalt politiarbeid / Eksport

Meldeskjema

Referansenummer
918965

Hvilke personopplysninger skal du behandle?

- Navn (også ved signatur/samtykke)
- Adresse eller telefonnummer
- E-postadresse, IP-adresse eller annen nettidentifikator

Prosjektinformasjon

Prosjekttittel

Kvalitetskontroll innen digitalt politiarbeid

Prosjektbeskrivelse

Prosjektet har som formål å kartlegge på hvilket nivå det blir utført kvalitetsikring av rapporter som dokumenterer arbeid innen fagfeltet digital kriminalteknikk (digital forensics).

Begrunn hvorfor det er nødvendig å behandle personopplysningene

Personopplysninger skal benyttes i forbindelse med invitasjon til deltakelse.

Ekstern finansiering
Ikke utfyllt
Type prosjekt
Studentprosjekt, masterstudium

Kontaktinformasjon, student
Rune Kenneth Bauge, runekba@stud.ntnu.no, tlf: [redacted]

Behandlingsansvar

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)
Lasse Øverlier, lasse.overlier@ntnu.no, tlf: [redacted]

Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?
Nei

Utvalg 1

Beskriv utvalget

Leder ved avsnitt eller seksjoner for digitalt politiarbeid i norsk politi.

Beskriv hvordan rekruttering eller trekking av utvalget skjer

Jeg jobber i Vest Politidistrikt og vil kontakte ledere i politiet som har et lederansvar innenfor fagområdet digitalt politiarbeid.

Alder

20 - 70

Personopplysninger for utvalg 1

- Navn (også ved signatur/samtykke)
- Adresse eller telefonnummer
- E-postadresse, IP-adresse eller annen nettidentifikator

Hvordan samler du inn data fra utvalg 1?

Personlig intervju

Vedlegg

intervju.pdf

Grunnlag for å behandle alminnelige kategorier av personopplysninger
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Informasjon for utvalg 1

Informerer du utvalget om behandlingen av personopplysningene?
Ja

Hvordan?
Skriftlig informasjon (papir eller elektronisk)

Informasjonsskriv

samtykkeskjema_intervju.doc

Tredjepersoner

Skal du behandle personopplysninger om tredjepersoner?
Nei

Dokumentasjon

Hvordan dokumenteres samtykkene?

- Elektronisk (e-post, e-skjema, digital signatur)

Hvordan kan samtykket trekkes tilbake?

Samtykke kan trekkes tilbake ved å sende e-post eller SMS til prosjektansvarlig.

Hvordan kan de registrerte få innsyn, rettet eller slettet personopplysninger om seg selv?

Innsyn, retting og sletting kan kreves ved å kontakte prosjektansvarlig via e-post eller SMS.

Totalt antall registrerte i prosjektet
100-999

Tillatelser

Skal du innhente følgende godkjenninger eller tillatelser for prosjektet?

- Annen godkjenning

Annen godkjenning

Trenger godkjenning fra politidistriktet intervjuobjektet er ansatt i.

Behandling

Hvor behandles personopplysningene?

- Maskinvare tilhørende behandlingsansvarlig institusjon

Hvem behandler/har tilgang til personopplysningene?

- Prosjektansvarlig
- Student (studentprosjekt)

Tilgjengeliggjøres personopplysningene utenfor EU/EØS til en tredjestat eller internasjonal organisasjon?

Nei

Sikkerhet

Oppbevares personopplysningene atskilt fra øvrige data (koblingsnøkkel)?

Ja

Hvilke tekniske og fysiske tiltak sikrer personopplysningene?

- Opplysningene krypteres under lagring

Varighet

Prosjektperiode

01.09.2022 - 01.09.2023

Hva skjer med dataene ved prosjektslutt?

Data anonymiseres (sletter/omskriver personopplysningene)

Hvilke anonymiseringstiltak vil bli foretatt?

- Personidentifiserbare opplysninger fjernes, omskrives eller grovkategoriseres
- Koblingsnøkkelen slettes
- Lyd- eller bildeopptak slettes

Vil de registrerte kunne identifiseres (direkte eller indirekte) i oppgave/avhandling/øvrige publikasjoner fra prosjektet?

Nei

Tilleggsopplysninger

Sikt

Meldeskjema / Kvalitetskontroll innen digitalt politiarbeid / Vurdering

Vurdering av behandling av personopplysninger

Referansenummer	Vurderingstype	Dato
918965	Standard	26.05.2023

Prosjekttittel
Kvalitetskontroll innen digitalt politiarbeid

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig
Lasse Øverlier

Student
Rune Kenneth Bauge

Prosjektperiode
01.09.2022 - 01.09.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 01.09.2023.

Meldeskjema

Kommentar
Personverntjenester har vurdert endringene registrert i meldeskjemaet.

Vedlegget for Intervjuguide er oppdatert.

Vår opprinnelige vurdering av hvordan personopplysninger behandles i prosjektet blir ikke endret av dette, og prosjektet kan bare fortsette som planlagt.

OPPFØLGING AV PROSJEKTET
Vi vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet/pågår i tråd med det du har oppgitt i meldeskjema.

Lykke til videre med prosjektet!

Appendix B

Appendix: Consent Forms For Interviews And Surveys

B.1 Participant Consent Form For Survey

Vil du delta i forskningsprosjektet

Kvalitetskontroll ved digitalt politiarbeid

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å kartlegge i hvilken grad en gjennomfører kvalitetskontroll i forbindelse med digitalt politiarbeid. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Spørreundersøkelsen er del av en masterstudie hvor formålet er å undersøke i hvilken grad en gjennomfører kvalitetskontroll på arbeid som blir utført innen digital kriminalteknikk (digital forensics). Det er i hovedsak satt søkelys på arbeids om blir utført i enhetene som i politiets distrikter blir omtalt som seksjoner eller avsnitt for digitalt politiarbeid.

Hvem er ansvarlig for forskningsprosjektet?
Norges teknisk-naturvitenskapelige universitet (NTNU) er ansvarlig for prosjektet.

Prosjektet blir gjennomført av:
Rune Kenneth Bauge,
NTNU i Gjøvik, Teknologivegen 22, 2815 Gjøvik
E-post: runekba@stud.ntnu.no, mobil: [redacted]

Veiledere
Lasse Øverlier (NTNU, stedfortreder inntil veileder er avklart)
Nina Sunde (Politihøgskolen)

Hvorfor får du spørsmål om å delta?
Spørreundersøkelsen retter seg mot dataetterforskere, ledere og andre ansatte i politietatens distrikter og særorganer som har arbeidsoppgaver relatert til digital kriminalteknikk. Dette er bakgrunnen for at du er forespurt om å delta i spørreundersøkelsen.

Hva innebærer det for deg å delta?

Din deltakelse vil bestå i å svare ut et spørreskjema som det tar ca. 5-10 minutter å svare ut.
Det vil ikke bli stilt spørsmål som vil kunne identifisere deg som person, den inneholder heller ikke spørsmål om opplysninger som er taushetsbelagt. Hoved tema i spørsmålene er relater til kvalitetskontroll av rapporter som er utarbeidet på ditt arbeidssted. Det vil også være spørsmål om arbeidserfaring, utdanning og lignende. Dine svar blir registrert automatisk og det vil ikke være mulig for å koble dine svar mot din kontaktinformasjon.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Rapporter og svar i

spørreskjema vil bli lagret på en kryptert og passordbeskyttet harddisk, denne er det kun prosjektansvarlig og veiledere som har tilgang til. Opplysninger som fremkommer i publikasjoner, skal ikke kunne tilbakeføres til enkeltpersoner.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Prosjektet vil etter planen avsluttes 01.06.2023. Etter prosjektslutt vil datamaterialet med dine personopplysninger anonymiseres.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra *NTNU Gjøvik* har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- *NTNU Gjøvik* ved Lasse Øverlier eller Politihøgskolen ved Nina Sunde
- Vårt personvernombud: *Thomas Helgesen, mob.*[redacted] *e-post: thomas.helgesen@ntnu.no*

Hvis du har spørsmål knyttet til Personverntjenester sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata ASpå epost (personverntjenester@sikt.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

Prosjektansvarlig/Veileder *Master student*
Nina Sunde Rune Kenneth Bauge

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *[sett inn tittel]*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

□ å delta i *spørreundersøkelse*

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

----

(Signert av prosjektdeltaker, dato)

B.2 Participant Consent Form For Interviews

Vil du delta i forskningsprosjektet

Kvalitetskontroll ved digitalt politiarbeid

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å kartlegge i hvilken grad en gjennomfører kvalitetskontroll i forbindelse med digitalt politiarbeid. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Interjuvet er del av en masterstudie hvor formålet er å undersøke i hvilken grad en gjennomfører kvalitetskontroll på arbeid som blir utført innen digital kriminalteknikk (digital forensics). Det er i hovedsak satt søkelys på arbeids om blir utført i enhetene som i politiets distrikter blir omtalt som seksjoner eller avsnitt for digitalt politiarbeid.

Hvem er ansvarlig for forskningsprosjektet?
Norges teknisk-naturvitenskapelige universitet (NTNU) er ansvarlig for prosjektet.

Prosjektet blir gjennomført av:
Rune Kenneth Bauge,
NTNU i Gjøvik, Teknologivegen 22, 2815 Gjøvik
E-post: runekba@stud.ntnu.no, mobil: [redacted]

Veiledere
Lasse Øverlier (NTNU)
Nina Sunde (Politihøgskolen)

Hvorfor får du spørsmål om å delta?
Interjuvene retter seg mot ledere i politietatens distrikter og særorganer som har arbeidsoppgaver relatert til digital kriminalteknikk. Dette er bakgrunnen for at du er forespurt om å delta i et personlig intervju om tema.

Hva innebærer det for deg å delta?

Din deltakelse vil bestå i å delta i et personlig intervju som vil ha en antatt varighet på 1 time.
Det vil ikke bli stilt spørsmål som vil kunne identifisere deg som person, en vil heller ikke stille spørsmål om opplysninger som er taushetsbelagt. Hoved tema i spørsmålene er relater til kvalitetskontroll og risiko knyttet til digitalt politiarbeid. Intervjuet vil bli tatt opp på lyd. Interjuvet og opplysningene om deg som deltaker vil bli anonymisert.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Rapporter og opptak fra intervjuet vil bli lagret på en kryptert og passordbeskyttet harddisk, denne er det kun prosjektansvarlig

og veiledere som har tilgang til. Opplysninger som fremkommer i publikasjoner, skal ikke kunne tilbakeføres til enkeltpersoner.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Prosjektet vil etter planen avsluttes 01.09.2023. Etter prosjektslutt vil datamaterialet med dine personopplysninger anonymiseres.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra *NTNU Gjøvik* har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- *NTNU Gjøvik* ved Lasse Øverlier eller Politihøgskolen ved Nina Sunde
- Vårt personvernombud: *Thomas Helgesen, mob. 93079038, e-post: thomas.helgesen@ntnu.no*

Hvis du har spørsmål knyttet til Personverntjenester sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@sikt.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

Prosjektansvarlig/Veileder	*Master student*
Lasse Øverlier / Nina Sunde	Rune Kenneth Bauge

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet Kvalitetskontroll ved digitalt politiarbeid og har fått anledning til å stille spørsmål. Jeg samtykker til:

å delta i *personlig intervju*

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

----

(Signert av prosjektdeltaker, dato)

Appendix C

Appendix: Research Instruments: Interview Guide And Survey

C.1 Survey - Norwegian

Kvalitetskontroll ved digitalt politiarbeid

Bakgrunnsspørsmål

1. Hvor i politiorganisasjonen arbeider du?

I et politidistrikt

I et særorgan

2. Hvilken rolle har du?

leder

ansatt

3. Hvilken bakgrunn har du?

Med bakgrunn mener vi i dette tilfellet utdanning og stillingstype.

Sivil

Politi

Politi med sivil tilleggsutdanning

Sivil med bachelor fra Politihøgskolen

4. Hva er din høyest oppnådde akademiske grad?

Dette elementet vises kun dersom alternativet «Sivil med bachelor fra Politihøgskolen» eller «Sivil» er valgt i spørsmålet «3. Hvilken bakgrunn har du?»

Ingen grad

Bachelorgrad (BSc)

Mastergrad (MSc)

Doktorgrad (PhD)

5 .Hvor mange års erfaring har du innen fagområdet digitalt politiarbeid?

Med erafring innen fagområdet mener vi antall år hvor arbeid innen digitalt politiarbeid har vært en av primæroppgavene dine.

0 - 2
3 - 5
6 - 8
9 +

6. Har du gjennomført noen videreutdanning innen etterforskning for sivile?

Dette elementet vises kun dersom alternativet «Sivil med bachelor fra Politihøgskolen» eller «Sivil» er valgt i spørsmålet «3. Hvilken bakgrunn har du?»

Du må velge minst ett svaralternativ.

Generell innføring i etterforskning – strategier og prinsipper (7,5 stp)

Generell innføring i etterforskningsmetodikk (7,5stp)

Videreutdanning i etterforskning (VEF)(15 stp)

Nei

7. På hvilket nivå har du gjennomført Politihøgskolen sitt utdanningsprogram NCFI?

Politihøgskolen sitt utdanningsprogram, Nordic Computer Forensic Investigators, tilbyr en rekke studier innen fagområdet digitalt politiarbeid. Her er det ønskelig at du svarer med å velge det høyeste nivået hvor du har fullført en videreutdanning innen dette programmet.

NCFI modul 1 (core concepts in digital investigation and forensics)

NCFI modul 2 (en eller flere moduler)

NCFI modul 3 (en eller flere moduler)

Master i samarbeid med NTNU

Ingen av disse

Spørsmål om kvalitetskontroll ved ditt arbeidssted.

8. På mitt arbeidssted finnes det tilstrekkelig dokumentasjon i form av prosedyrer, rutiner, maler eller lignende som beskriver og legger til rette for kvalitetskontroll av arbeidet som blir gjort ved DPA.

Helt enig

Delvis enig

Nøytral

Delvis uenig

Helt uenig

Her kan du kommentere/utdype svaret ditt. (FRITEKST FELT)

9.På mitt arbeidssted gjennomføres systematisk kvalitetskontroll av rapportene som skrives. Dette spørsmålet omhandler rapporter som omfatter undersøkelse/analyse av databeslaget, teknisk analyse og/eller innholdsanalyse og som er skrevet av DPA ansatt

Helt enig

Delvis enig

Nøytral

Delvis uenig

Helt uenig

Her kan du kommentere/utdype svaret ditt. (FRITEKST FELT)

10. I vårt distrikt gjennomfører vi systematisk kvalitetskontroll av etterforskere sine «gjennomgangsrapporter».

Helt enig

Delvis enig

Nøytral

Delvis uenig

Helt uenig

Her kan du kommentere/utdype svaret ditt. (FRITEKST FELT)

11. Ved min enhet har vi tilstrekkelig tid til å gjennomføre kvalitetskontroll av arbeidet som blir gjennomført.

Helt enig

Delvis enig

Nøytral

Delvis uenig

Helt uenig

Her kan du kommentere/utdype svaret ditt. (FRITEKST FELT)

12. Kvalitetskontroll bør være integrert i arbeidsprosessene ved Digitalt politiarbeid.

Helt enig

Delvis enig

Nøytral

Delvis uenig

Helt uenig

Her kan du kommentere/utdype svaret ditt. (FRITEKST FELT)

13. Kvalitetskontroll av resultater før de blir brukt som bevis i straffesak burde være en naturlig del av arbeidsflyten i distriktet.

Helt enig

Delvis enig

Nøytral

Delvis uenig

Helt uenig

Her kan du kommentere/utdype svaret ditt. (FRITEKST FELT)

14. Hvilken rolle har de som har gjennomfører kvalitetskontroll av rapporter ved deres enhet?

Dette elementet vises kun dersom alternativet «leder» er valgt i spørsmålet «2. Hvilken rolle har du?»

Her kan du kommentere/utdype svaret ditt. (FRITEKST FELT)

Leder innen fagfeltet

DPA ansatt

Påtale

Andre

15. I løpet av det siste 12 månedene har jeg tatt initiativ til at det blir utført kvalitetskontroll på egne rapporter.

Ja

Nei

16. I løpet av de siste 12 månedene har jeg selv utført kvalitetskontroll på rapporter på et eller flere nivåer i kvalitetskontroll hierarkiet?

Dette elementet vises kun dersom alternativet «leder» er valgt i spørsmålet «2. Hvilken rolle har du?»

Ja

Nei

17. I vårt distrikt utføres det arbeid innenfor fagområdet digitalt politiarbeid av fagkontakter eller tilsvarende.

Dette elementet vises kun dersom alternativet «I et politidistrikt» er valgt i spørsmålet «1. Hvor i politiorganisasjonen arbeider du?»

Vi tenker da ikke på arbeid hvor en får bistand fra særorgan eller «rapporter om gjennomgang» utarbeidet av etterforsker.

Ja

Nei

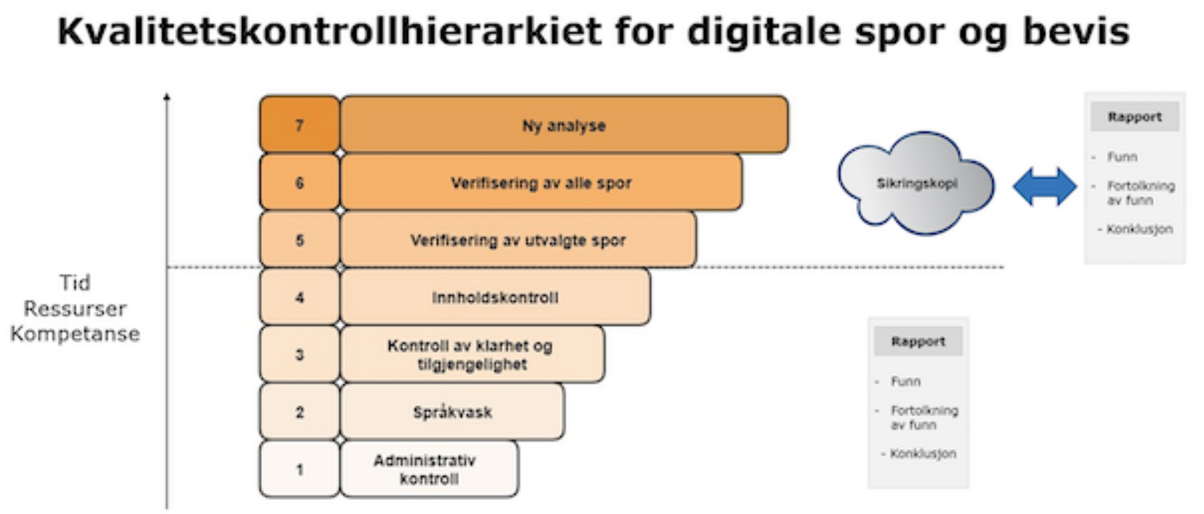
18. I vårt distrikt gjennomfører vi kvalitetskontroll av arbeid som utføres av fagkontakter og tilsvarende.

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «17. I vårt distrikt utføres det arbeid innenfor fagområdet digitalt politiarbeid av fagkontakter eller tilsvarende.»

Med andre mener vi i dette spørsmålet ansatte ved andre enheter enn den en selv er ansatt ved. Dette kan for eksempel være en fagkontakt eller en etterforsker som har utført arbeid utover det en kan forvente av en "gjennomgang".

Ja

Nei


Kvalitetskontrollhierarkiet for digitale spor og bevis

Spørsmålene under viser til nivåene i Kvalitetkontrollhierarkiet (The peer-reveiw hierarchy for DF) som er beskrevet av Nina Sunde og Graeme Horsman i 2021.

19. Ved vår enhet utføres det kvalitetskontroll på nivå 1, administrativ kontroll.

Dette elementet vises kun dersom alternativet «leder» er valgt i spørsmålet «2. Hvilken rolle har du?»

En administrativ kontroll omfatter hvorvidt etterforskningen er gjennomført i tråd med formelle krav og i henhold til oppdraget, altså at avtalte undersøkelser er gjennomført på de beslaglagte enhetene.

Alle

de fleste

noen få

Ingen

20. Ved vår enhet utføres det kvalitetskontroll på nivå 2, språkvask

Dette elementet vises kun dersom alternativet «leder» er valgt i spørsmålet «2. Hvilken rolle har du?»

Språkvask omfatter en vurdering av om rapporten inneholder stave- og grammatiske feil som bør rettes opp

Alle

de fleste

noen få

Ingen

21. Ved vår enhet utføres det kvalitetskontroll på nivå 3, kontroll av klarhet og tilgjengelighet.

Dette elementet vises kun dersom alternativet «leder» er valgt i spørsmålet «2. Hvilken rolle har du?»

Kontroll av klarhet og tilgjengelighet innebærer å vurdere om rapportskriver evner å framstille resultatet av undersøkelsen på en tydelig, forståelig og ryddig måte for en leser uten særskilt teknisk kompetanse.

Alle

de fleste

noen få

Ingen

22. Ved vår enhet utføres det kvalitetskontroll på nivå 4, innholdskontroll.

Dette elementet vises kun dersom alternativet «leder» er valgt i spørsmålet «2. Hvilken rolle har du?»

Innholdskontroll omfatter en grundig kontroll av rapportens innhold som beskriver resultatet av etterforskningen, men avgrenses mot en verifisering av funn/resultater. Hovedfokus rettes mot den vitenskapelige og logiske fundamentet i rapporten. Vurdering av sammenhengen mellom bevisene som presenteres og konklusjonen er spesielt viktig.

Alle

de fleste

noen få

Ingen

23. Ved vår enhet utføres det kvalitetskontroll på nivå 5, verifisering av utvalgte spor.

Dette elementet vises kun dersom alternativet «leder» er valgt i spørsmålet «2. Hvilken rolle har du?»

Ved verifisering av utvalgte spor tar en et utvalg av funnene som er beskrevet i en rapport og verfiserer ved bruk av et annet verktøy eller annen metodikk. En verifiserer ikke alle funn, men et utvalg av de viktigste funnene.

Alle

de fleste

noen få

ingen

24. Ved vår enhet utføres det kvalitetskontroll på nivå 6, verifisering av alle spor.

Dette elementet vises kun dersom alternativet «leder» er valgt i spørsmålet «2. Hvilken rolle har du?»

I forbindelse med en verifisering av av alle funn beskrevet i en rapport så gjøres det en fullstendig verifisering av alle funn ved bruk av annet verktøy eller metodikk.

Alle

de fleste

noen få

ingen

25. Ved vår enhet utføres det kvalitetskontroll på nivå 7, ny analyse.

Dette elementet vises kun dersom alternativet «leder» er valgt i spørsmålet «2. Hvilken rolle har du?»

Ny analyse innebærer at hele undersøkelsen blir gjort på nytt av personell som ikke har tidligere kjennskap til den aktuelle saken.

Alle

de fleste

noen få

ingen

I påfølgende spørsmål bes du oppgi antall ganger du har utført ulike typer kvalitetskontroll.

26. I hvilket omfang har du de siste 12 månedene utført kvalitetskontroll på nivå 1, administrativ kontroll?

Dette elementet vises kun dersom alternativet «ansatt» er valgt i spørsmålet «2. Hvilken rolle har du?»

En administrativ kontroll omfatter hvorvidt etterforskningen er gjennomført i tråd med formelle krav og i henhold til oppdraget, altså at avtalte undersøkelser er gjennomført på de beslaglagte enhetene.

0

1 - 5

6 - 9

10 +

27. I hvilket omfang har du de siste 12 månedene utført kvalitetskontroll på nivå 2, språkvask?

Dette elementet vises kun dersom alternativet «ansatt» er valgt i spørsmålet «2. Hvilken rolle har du?»

Språkvask omfatter en vurdering av om rapporten inneholder stave- og grammatiske feil som bør rettes opp

0

1 - 5

6 - 9

10 +

28. I hvilket omfang har du de siste 12 månedene utført kvalitetskontroll på nivå 3, kontroll av klarhet og tilgjengelighet?

Dette elementet vises kun dersom alternativet «ansatt» er valgt i spørsmålet «2. Hvilken rolle har du?»

Kontroll av klarhet og tilgjengelighet innebærer å vurdere om rapportskriver evner å framstille resultatet av undersøkelsen på en tydelig, forståelig og ryddig måte for en leser uten særskilt teknisk kompetanse.

0

1 - 5

6 - 9

10 +

29. I hvilket omfang har du de siste 12 månedene utført kvalitetskontroll på nivå 4, innholdskontroll?

Dette elementet vises kun dersom alternativet «ansatt» er valgt i spørsmålet «2. Hvilken rolle har du?»

Innholdskontroll omfatter en grundig kontroll av rapportens innhold som beskriver resultatet av etterforskningen, men avgrenses mot en verifisering av funn/resultater. Hovedfokus rettes mot den vitenskapelige og logiske fundamentet i rapporten. Vurdering av sammenhengen mellom bevisene som presenteres og konklusjonen er spesielt viktig.

0

1 - 5

6 - 9

10 +

30. I hvilket omfang har du de siste 12 månedene utført kvalitetskontroll på nivå 5, verifisering av utvalgte spor?

Dette elementet vises kun dersom alternativet «ansatt» er valgt i spørsmålet «2. Hvilken rolle har du?»

Ved verifisering av utvalgte spor tar en et utvalg av funnene som er beskrevet i en rapport og verfiserer ved bruk av et annet verktøy eller annen metodikk. En verifiserer ikke alle funn, men et utvalg av de viktigste funnene.

0

1 - 5

6 - 9

10 +

31. I hvilket omfang har du de siste 12 månedene utført kvalitetskontroll på nivå 6, verifisering av alle spor?

Dette elementet vises kun dersom alternativet «ansatt» er valgt i spørsmålet «2. Hvilken rolle har du?»

I forbindelse med en verifisering av av alle funn beskrevet i en rapport så gjøres det en fullstendig verifisering av alle funn ved bruk av annet verktøy eller metodikk.

0

1 - 5

6 - 9

10 +

32. I hvilket omfang har du de siste 12 månedene utført kvalitetskontroll på nivå 7, ny analyse?

Dette elementet vises kun dersom alternativet «ansatt» er valgt i spørsmålet «2. Hvilken rolle har du?»

Ny analyse innebærer at hele undersøkelsen blir gjort på nytt av personell som ikke har tidligere kjennskap til den aktuelle saken.

0

1 - 5

6 - 9

10 +

C.2 Survey - English

This is the questionnaire translated into English by Nina Sunde.

Quality control in digital forensics

Background

1. Where in the police organisation are you situated?

A police district/local unit

A national unit

2. What is your role?

Manager

Employee

3. What is your professional background?

With 'professional background' we mean education and type of position.

Civil

Police

Police with additional civil education

Civil with bachelor's degree from the Police University College

4. What is your highest academic degree?

This is shown if the respondent ticks off any of the «Civil» or "Civil with bachelor's degree from the Police University College" alternatives in Q3.

No degree

Bachelor's degree (BSc)

Master's degree (MSc)

Doctoral degree (PhD)

5 .How many years of experience do you have within the digital forensics discipline?

With ‘experience’ we mean the number of years where digital forensics has been one of your primary tasks.

0 - 2
3 - 5
6 - 8
9 +

6. Have you completed any continuing professional development courses for civil personnel?

This is shown if the respondent ticks off any of the «Civil» or “Civil with bachelor’s degree from the Police University College” alternatives in Q3.

Du må velge minst ett svaralternativ.

General introduction to criminal investigation – strategies and principles (7,5 ECTS)

General introduction to investigative methodologies (7,5ECTS)

Continuing professional development in criminal investigation (15 ECTS)

Nei

7. On which level have you completed the Norwegian Police University College’s education within the NCFI portofolio?

The Norwegian Police University College course portofolio NCFI (Nordic Computer Forensic Investigators) offers a number of courses within digital forensics. Please reply by choosing the highest course-level you have completed within this educational program.

NCFI module 1 (core concepts in digital investigation and forensics)

NCFI module 2 (one or more modules)

NCFI module 3 (one or more modules)

Master’s programme – offered by The Norwegian Police University College and NTNU (MISEB)

None of these

Questions about quality control conducted at your unit.

8. In my unit, there is sufficient documentation available such as procedures, routines, templates describing and facilitating quality control of digital forensic work performed at the unit.

Completely agree

Partly agree

Neutral

Partly disagree

Completely disagree

Here you may comment/elaborate your response. (Open field for comments)

9. In my unit, the reports undergo systematic quality control. This question concerns reports resulting from examination/analysis of the evidence file, which involves technical analysis and/or content analysis performed by an employee at a digital forensics unit.

Completely agree

Partly agree

Neutral

Partly disagree

Completely disagree

Here you may comment/elaborate your response. (Open field for comments)

10. In our police district we perform systematic quality control of the criminal detective's reports resulting from investigative review of the evidence file.

Completely agree

Partly agree

Neutral

Partly diagree

Completely disagree

Here you may comment/elaborate your response. (Open field for comments)

11. At my unit, we have enough time to perform quality control of the casework.

Completely agree

Partly agree

Neutral

Partly disagree

Completely disagree

Here you may comment/elaborate your response. (Open field for comments)

12. Quality control should be integrated into the work processes at digital forensics units.

Completely agree

Partly agree

Neutral

Partly disagree

Completely disagree

Here you may comment/elaborate your response. (Open field for comments)

13. Quality control of results prior to being used in a criminal investigation should be a natural part of the work flow in the police district.

Completely agree

Partly agree

Neutral

Partly disagree

Completely disagree

Here you may comment/elaborate your response. (Open field for comments)

14. What is the role of those performing quality control at your unit?

This element is shown if the alternative «manager» is ticked off in Q2.

Here you may comment/elaborate your response. (Open field for comments)

Manager at a digital forensics unit

Employee at digital forensics unit

Prosecution

Other

15. During the last 12 months, have you initiated quality control of own reports?

Yes

No

16. During the last 12 months, have you perfomed quality control according to the scope of one or more of the Peer Review Hierarchy for Digital Forensics levels?

This element is shown if the alternative «manager» is ticked off in Q2.

Yes

No

17. In our police district, digital forensic work is performed by digital forensic liaisons (Norwegian: «fagkontakter») or similar positions. This does not include assistance from national units or investigative review of the evidence file performed by criminal detectives.

('fagkontakt' is a police officer with more formal education/experience in digital forensic than the typical police officer – and acts as a liaison between the experts and patrol officers/criminal detectives).

This element is shown if the alternative «in a police district/local unit» is ticked off in Q1.

Yes

No

18. In our district, the work performed by digital forensic liaisons or similar positions is subject to quality control. By 'or similar' we mean employees from other units than the one you are situated at. They may for example have performed work beyond what may be expected from a typical investigative review of the evidence file.

This element is shown if the alternative «Yes» is ticked off in Q17.

Yes

No

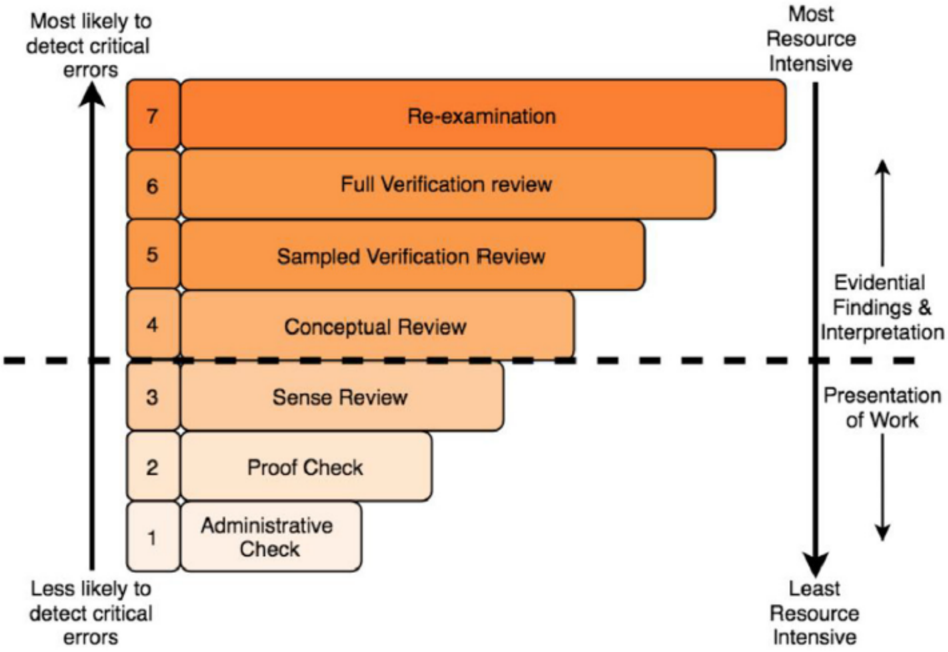


Fig. 3. The 'peer review hierarchy' for DF (Horsman and Sunde, 2020).

The following questions refer to the 'The peer reveiw hierarchy for Digital Forensics' described by Nina Sunde og Graeme Horsman in 2021.

19. At our unit, quality control of reports is performed at level 1, Administrative Check.

An Administrative Check entails to control whether the investigation is performed in compliance with formal requirements and according to the agreed assignment – meaning, the agreed tasks have been performed on the seized devices.

This element is shown if the alternative «manager» is chosen for Q2.

All

Most

A few

None

20. At our unit, quality control of reports is performed at level 2, Proof Check. A Proof Check involves assessing whether the report contains spelling or grammatical errors that should be corrected.

This element is shown if the alternative «manager» is ticked off in Q2.

All

Most

A few

None

21. At our unit, quality control of reports is performed at level 3, Sense Review. A Sense Review involves assessing whether the report author presents the result in a clear, understandable, and coherent manner for a reader without particular technical expertise.

This element is shown if the alternative «manager» is ticked off in Q2.

All

Most

A few

None

22. At our unit, quality control of reports is performed at level 4, Conceptual Review. A Conceptual Review is a thorough control of the report content describing the result of the investigation but does not include verification of findings/results. The focus is directed towards the scientific and logic foundation of the report. Assessing the relationship between the evidence and the conclusion is of key importance.

This element is shown if the alternative «manager» is ticked off in Q2.

All

Most

A few

None

23. At our unit, quality control is performed at level 5, Sampled Verification Review. A Sampled Verification Review verifies selected findings from the report by using a different tool/method than used in the original examination.

This element is shown if the alternative «manager» is ticked off in Q2.

All

Most

A few

None

24. At our unit, quality control is performed at level 6, Full Verification Review. A Full Verification Review involves verification of all reported results by using a different tool/method than used in the original examination.

This element is shown if the alternative «manager» is ticked off in Q2.

All

Most

A few

None

25. At our unit, quality control is performed at level 7, Re-examination. A Re-examination means that the full examination is done a second time by personnel with no former knowledge of or involvement in the case.

This element is shown if the alternative «manager» is ticked off in Q2

All

Most

A few

None

In the following questions you will be asked to state how many times you have performed quality control at the respective levels.

26. To what extent have you performed quality control at level 1 Administrative Check during the last 12 months?

An Administrative Check entails to control whether the investigation is performed in compliance with formal requirements and according to the agreed assignment – that is, that the agreed tasks have been performed on the seized devices.

This element is shown if the alternative «employee» is ticked off in Q2.

0

1 - 5

6 - 9

10 +

27. To what extent have you performed quality control at level 2 Proof Check during the last 12 months?

A Proof Check involves assessing whether the report contains spelling or grammatical errors that should be corrected.

This element is shown if the alternative «employee» is ticked off in Q2

0

1 - 5

6 - 9

10 +

28. To what extent have you performed quality control at level 3 Sense Review during the last 12 months?

A Sense Review involves assessing whether the report author is able to present the result in a clear, understandable, and coherent manner for a reader without particular technical expertise.

This element is shown if the alternative «employee» is ticked off in Q2

0

1 - 5

6 - 9

10 +

29. To what extent have you performed quality control at level 4 Conceptual Review during the last 12 months?

A Conceptual Review is a thorough control of the report content describing the result of the investigation but does not include verification of findings/results. The focus is directed towards the scientific and logic foundation of the report. Assessing the relationship between the evidence and the conclusion is of key importance.

This element is shown if the alternative «employee» is ticked off in Q2

0

1 - 5

6 - 9

10 +

30. To what extent have you performed quality control at level 5 Sampled Verification Review during the last 12 months?

A sampled verification review verifies selected findings from the report by using a different tool/method than used in the original examination.

This element is shown if the alternative «employee» is ticked off in Q2

0

1 - 5

6 - 9

10 +

31. To what extent have you performed quality control at level 6 Full Verification Review during the last 12 months?

A full verification review involves verification of all reported results by using a different tool/method than used in the original examination.

This element is shown if the alternative «employee» is ticked off in Q2

0

1 - 5

6 - 9

10 +

32. To what extent have you performed quality control at level 7 Re-examination during the last 12 months?

A Re-examination involves that the full examination is done a second time by personnel with no former knowledge of or involvement in the case.

This element is shown if the alternative «employee» is ticked off in Q2

0

1 - 5

6 - 9

10 +

C.3 Interview Guide

Innledning

Takk for at du har sagt deg villig til å delta i dette intervjuet om som er del av datainnsamlingen til masteroppgaven min. Oppgaven handler om kvalitetskontroll ved digitalt politiarbeid og jeg ønsker å kartlegge «nå situasjonen» samt undersøke om det er mulig å innføre en eller annen form for kvalitetskontroll ved DPA enhetene. I den sammenhengen er det også av interesse å få vite litt mer om DPA ledere sitt forhold til risiko opp mot Digital Forensics (DF) prosessen som beskriver fasene innen digital kriminalteknikk. Dette intervjuet skal ikke berøre taushetsbelagt informasjon og vil derfor be om at en er klar over taushetsplikten når en svarer på spørsmålene i intervjuet.

For å sette en ramme rundt intervjuet ønsker jeg at du først deltar på en liten risikovurdering knyttet opp mot forvaltningen av fagområdet digital kriminalteknikk.

Risikovurdering

Spørsmål 1:

Før vi går i gang med selve risikovurderingen så tenkte jeg du kanskje kunne fortelle litt om hva du legger i begrepet risiko?

Spørsmål 2:

Er risiko noe du har reflektert over opp mot utøvelse av digital kriminalteknikk som fag?

Presentasjon av verdier

En risikovurdering forutsetter at en har et forhold til hvilke verdier en risikovurderer.
I vårt tilfelle ønsker jeg at vi skal ha søkelys på faget digital kriminalteknikk. For at interjuvene skal ha samme utgangspunkt har jeg identifisert følgende verdier knyttet opp mot digital kriminalteknikk som fag.

1. rettsikkerheten til de involverte (skyld/uskyld like viktig)
2. tillit til politiets utøvelse av digital kriminalteknikk som fag (omdømme)
3. tillit til bruk av kommersielle verktøy og tolkningen av det som blir presentert av

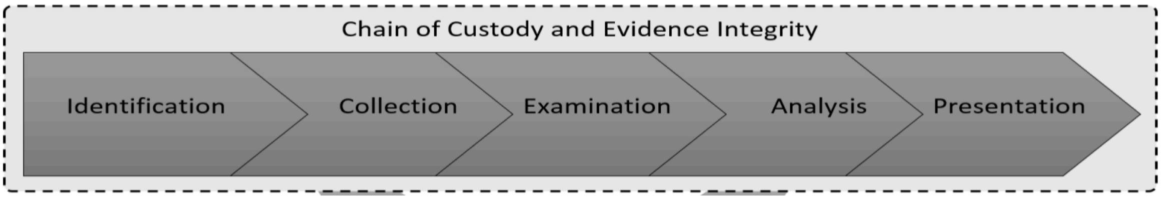
   disse.

Spørsmål 3:

Hva tenker du om disse verdiene? Noe du vil tilføye/trekke fra?

Informasjon om DF prosessen

Risikovurderingen vil ta utgangspunkt i de forskjellige fasene i DF prosessen beskrevet av Anders o. Flaglien.



Flaglien (2018)

Spørsmål 4:

Hvordan praktiseres DF prosessen i ditt distrikt og hvem er involvert i de forskjellige fasene?

Introduksjon til risikovurdering og hvordan den gjennomføres

			usannsynlig (1)	**mulig (2)**	**sannsynlig(3)**
	Rettsikkerhet	**Omdømme / Tillit til verktøy**	Jeghar ikke hørt om eller opplevd en slik hendelse tidligere	Trolig, men forutsetter flere samtidige feil.	Det er lett å se for seg et slikt scenario.
Svært stor utstrekning (3)	Uskyldig blir dømt	Tilliten til etatens utøvelse av fag er svekket. / Tillit til aktuelt verktøy er svekket.	3	6	9
Middels utstrekning (2)	En får ikke belyst saken riktig	Tilliten til distriktets utøvelse av faget blir svekket. / Tillit til distriktets bruk av verktøyet blir svekket.	2	4	6
Ubetydelig utstrekning (1)	Påvirker ikke bevisvurderingen	Tillit til individs utøvelse av faget blir svekket. /Tillit til individs bruk av verktøy blir svekket.	1	2	3

Extremely Low	Low	Moderate	High	Critical

Risikovurderingen gjennomføres ved at en vurderer risiko opp mot de gitte verdiene i hver av fasene i DF prosessen.

Hver risiko i fasene vurderes da med en verdi fra 1 til 3 i forhold til konsekvens og sannsynlighet. Produktet av disse verdiene gir risikoen.

1. Identifisering (Identification):

Denne fasen beskriver identifiseringen av digitale sporsteder. Dette kan være både fysiske databærerer og data lagret på internett (sky-tjenester, SOME osv.)

Risk ID	Identifiserte risikoer	Risikoeffekter	Eksisterende tiltak	Konsekvens	Sannsynlighet	Risiko
1						
2						
3						
4						

2. Innsamling (Collection):

Sikringsfasen handler om å skaffe seg kontroll over data lagret på sporstedene funnet i identifiseringsfasen.

Risk ID	Identifiserte risikoer	Risikoeffekter	Eksisterende tiltak	Konsekvens	Sannsynlighet	Risiko
5						
6						
7						
8						

3. Klargjøringsfasen (Examination):

I denne fasen gjøres data tilgjengelig for innholdsanalyse.

Risk ID	Identifiserte risikoer	Risikoeffekter	Eksisterende tiltak	Konsekvens	Sannsynlighet	Risiko
9						
10						
11						
12						

4. Analysefasen (Analysis):

Data som er blitt gjort tilgjengelig blir vurdert opp mot sakens informasjonsbehov for å vurdere om de kan benyttes som bevis.

Risk ID	Identifiserte risikoer	Risikoeffekter	Eksisterende tiltak	Konsekvens	Sannsynlighet	Risiko
13						
14						
15						
16						

5. Presentasjonsfasen (Presentation):

Denne fasen omhandler dokumentasjon av funn som er gjort i hele prosessen.

Risk ID	Identifiserte risikoer	Risikoeffekter	Eksisterende tiltak	Konsekvens	Sannsynlighet	Risiko
17						
18						
19						
20						

Spørsmål 5:

Har du selv opplevd eller kjenner til situasjoner hvor noen av risikoene vi når har snakket om har forekommet?

Spørsmål 6:

Basert på risikoanalysen så kom risk ID (sett inn nr) ut med høy risikoverdi. Hvilken betydning vil det ha for faget at en slik hendelse inntreffer? Hvilke tiltak tenker du må på plass for å motvirke denne risikoen?

Spørsmål 8:

Hva ser du på som den største utfordringen ved å innføre en systematisk kvalitetskontroll av arbeid som utføres innen digital kriminalteknikk? Hvorfor? Hva betyr dette?

Spørsmål 9:

Hvis en skulle innført systematisk kvalitetskontroll ved alle DPA-enheter, tenker du dere har tilstrekkelig kompetanse lokalt til å håndtere dette?

Spørsmål 10:

Hvis en skulle innført systematisk kvalitetskontroll ved alle DPA-enheter, tenker du dere har tilstrekkelig kapasitet lokalt til å håndtere dette?

Spørsmål 11:

Jeg ønsker at du reflekterer litt over følgende scenario. Du får beskjed fra ledelsen om at det skal innføres systematisk kvaliteskontroll av rapporter som beskriver funn hvor digitale bevis er avgjørende i straffesakene. Din enhet får ansvar for implementasjon og gjennomføring.

Spørsmål 12:

Hva tenker du er den største utfordringen digital kriminalteknikk står ovenfor som fagmiljø i norsk politi?

NTNU

Norwegian University of
Science and Technology