

Jørn Helge Jahren

# Is the quality assurance in Digital Forensic work in the Norwegian police adequate?

Master's thesis in IMT4905 Experience-based Master's Thesis

Supervisor: Politioverbetjent Nina Sunde, Politihøgskolen

July 2020



Jørn Helge Jahren

# **Is the quality assurance in Digital Forensic work in the Norwegian police adequate?**

Master's thesis in IMT4905 Experience-based Master's Thesis  
Supervisor: Politioverbetjent Nina Sunde, Politihøgskolen  
July 2020

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



Norwegian University of  
Science and Technology



## ABSTRACT

This master's thesis is a qualitative study based on semi-structured interviews with *Digital Forensic Examiners (DFE)* and *Forensic Technicians (FT)* from various police districts in Norway. All the interviewees were experienced in their disciplines and thus had knowledge of the conditions before and after the *Nærpolitireformen* (1). The study has a hermeneutical phenomenological approach, and the problem description is:

*Is the quality assurance in Digital Forensics in the Norwegian police adequate?*

The study revealed that there was little involvement or quality management from the leaders in the field of *Digital Forensics (DF)* in the participating districts, which might be due to a lack of digital expertise. Any quality assurance measures in the work had to be implemented by the individual DFE.

A part of the study has been to compare quality assurance in the fields of *Forensic Science (FS)* and Digital Forensics.

In contrast to the field of Digital Forensics, the field of Forensic Science has a national quality standard that guides the units and management in how the forensic work is to be carried out and managed with quality; in addition, Forensic Technicians essentially work in pairs in dual-investigator teams.

The results of the data analysis showed that the focus on quality in the two disciplines was no stronger after the reform. The majority of participants in the study felt, rather, that they had lost resources and gained an increased workload, and that the areas of Forensic Science and Digital Forensics had not been prioritized in the reform on a par with those of operational disciplines and investigation. Some were concerned about the extent to which this might affect the rule of law of those involved in an investigation.

### Keywords:

Digital Forensics, Digital Policing, Quality Management, Quality Assurance, Quality Control, Forensic Science, Digital Forensic Process, criminal investigation, forensic investigation, digital evidence, digital competence, errors in investigation

## SAMMENDRAG

Denne masteroppgaven er en kvalitativ studie som baserer seg på semi-strukturerte intervjuer med dataetterforskere og kriminalteknikere fra forskjellige politidistrikter i politiet i Norge. Alle de intervjuede var erfarne i sine disipliner, og hadde således kunnskap om forholdene før og etter «Nærpolitireformen» (1).

Studien har en hermeneutisk fenomenologisk tilnærming og problemstillingen som belyses er:

*Er kvalitetssikringstiltakene i fagområdet dataetterforskning tilfredsstillende?*

Studien viste at det var lite involvering og kvalitetsstyring fra ledelsen i fagområdet dataetterforskning i de deltagende distrikter, og at dette kan skyldes manglende digital kompetanse. Eventuelle kvalitetssikringstiltak i arbeidet måtte iverksettes av den enkelte dataetterforsker.

En del av studien har vært å sammenligne kvalitetssikring i fagområdet kriminalteknikk med fagområdet dataetterforskning.

I motsetning til fagområdet dataetterforskning, har fagområdet kriminalteknikk en nasjonal kvalitetsstandard som veileder mannskap og ledelse i hvordan det kriminaltekniske arbeidet skal gjennomføres og styres med kvalitet, i tillegg til at kriminalteknikere i hovedsak jobber i parvise etterforskningsteam.

Resultatene fra dataanalysen viste at fokuset på kvalitet i de to fagområdene ikke var økt etter reformen. Flertallet av deltakerne i studien mente snarere at de hadde mistet ressurser og fått økt arbeidsmengde, og at områdene kriminalteknikk og dataetterforskning ikke hadde blitt prioritert i reformen på nivå med operative fagdisipliner og etterforskning. Noen var engstelige for i hvilken grad dette kunne påvirke rettsikkerheten til de involverte i en etterforskning.

### **Nøkkelord:**

Digital etterforskning, Dataetterforskning, Digitalt politiarbeid, Dataetterforskningsprosessen, kvalitetsstyring, kvalitetssikring, kvalitetskontroll, kriminalteknikk, digitale bevis, feil i etterforskningen, digital forståelse, digital kompetanse

## **ACKNOWLEDGMENTS**

I would like to thank the Norwegian University of Science and Technology and the Norwegian Police University College for the interesting and challenging years.

I could not have done this without the professional guidance of my supervisors, Nina Sunde and Katrin Franke.

I am very grateful for the support from my employer, NC3 at NCIS, Kripos, for their goodwill during the last year, especially colleagues at SIO, Police Inspector Andreas Berge and my manager, Assistant Chief of Police, Lise Matheson.

A special thanks to the participants from the three police districts who shared their experiences so openly, and the other contributors, Ulf Bergum, Kjell Harald Andersen, Morten Olsen Sandnes, Trond Austad and Andreas Røed who has so kindly responded to my inquiries, for proof reading and valuable inputs.

Thanks to my family for putting up with me in this run. Love you!

# CONTENT

<b>ABSTRACT</b> .....	<b>2</b>
<b>SAMMENDRAG</b> .....	<b>3</b>
<b>ACKNOWLEDGMENTS</b> .....	<b>4</b>
<b>1 INTRODUCTION AND PROBLEM DESCRIPTION</b> .....	<b>7</b>
1.1 Delimitations and list of abbreviations .....	8
1.2 Research problem .....	11
1.3 Research method .....	11
1.4 Problem description - why compare DF to FS .....	11
1.5 What is Digital Forensics? .....	11
1.6 What is Forensic Science (Kriminalteknikk)? .....	12
1.7 What is quality in investigations? .....	12
1.8 What is Forensic Investigation? .....	12
1.9 Structure of the thesis .....	13
<b>2 STATE OF THE ART</b> .....	<b>14</b>
2.1 Introduction .....	14
2.2 Background and theory – Digital Forensics .....	14
2.3 The reform – brief history and purpose .....	21
2.4 The reform – enhancing quality in investigations .....	21
2.5 The new organization – new DF and FS units .....	22
2.6 Competence and quality standards in DF – status .....	23
2.7 Competence and quality standards in FS – status .....	25
<b>3 METHODOLOGY</b> .....	<b>27</b>
3.1 Introduction .....	27
3.2 Research method .....	27
3.3 Phenomenological perspective .....	27
3.4 Gathering information - research interviews .....	28
3.5 Data collection and ethical considerations .....	29
3.6 Transcription of data .....	30
3.7 Data analysis .....	31
3.8 Quality assurance .....	32
<b>4 RESULTS</b> .....	<b>33</b>
4.1 Introduction .....	33
4.2 Focus on quality after the reform of the police .....	34
4.3 Focus on quality after the investigation reform .....	36
4.4 Competence plans or planning .....	37
4.5 Accreditations, certifications and standardizations .....	40



4.6 Quality management – instructions/standards .....	41
4.7 Quality assurance – what is done – is it adequate? .....	42
4.8 Perceptions on the term quality.....	45
4.9 Summary .....	46
<b>5 DISCUSSION .....</b>	<b>47</b>
5.1 Introduction .....	47
5.2 Has the reform contributed to an enhanced focus on quality in DF and FS? .....	47
5.3 Quality assurance in DF in the Norwegian police, is it adequate? .....	50
<b>6 SUMMARY AND FUTURE WORK.....</b>	<b>59</b>
6.1 Summary .....	59
6.2 Future work .....	59
<b>7 BIBLIOGRAPHY .....</b>	<b>61</b>
<b>8 APPENDIXES .....</b>	<b>67</b>
8.1 Appendix 1 .....	67
8.2 Appendix 2.....	72
8.3 Appendix 3.....	73
8.4 Appendix 4.....	77
8.5 Appendix 5.....	80

# 1 INTRODUCTION AND PROBLEM DESCRIPTION

The digital age and our way of “digital living” has added many new challenges for the police to handle but has also revealed a major asset of valuable information in every investigation today.

Digital Forensics (DF) is a new branch of Forensic Science (FS) and may be the fastest growing discipline in terms of complexity and extent. There is an increased focus on DF and *Digital Evidence* in criminal investigations today, since there is a digital component in many of the ways people live, interact and communicate. These activities leave a large number of traces that may be obtained and can support or refute hypotheses in criminal investigations.

While the demand for digital evidence is growing, it is worrying that there are still no adequate competence requirements or standards in methods or tools, or instructions regarding quality assurance and *quality management* (QM) in DF in the Norwegian police.

In June 2019, errors in the *Call Data Records* that Danish police collected from phone service providers were unveiled. The failure related to errors in the police handling of the retrieved raw data, resulting in a stop on using such data in investigations in Denmark, later in the autumn of 2019, for a period of two months. The failure led to a scrutiny of over 10,000 criminal cases from 2012-2019 and over 40,000 requisitions of Call Data Records, which has imposed a tremendous burden on the Danish justice system and on the involved parties in the cases. Quality assurance measures might have prevented such errors (2).

In this thesis, have focused on the quality assurance in DF in the Norwegian police, to examine whether the theory would reveal an updated picture, since my own experience has been that quality control was left up to the judge when I presented digital evidence in court.

The analysis of the qualitative data in the study has given insight into how quality assurance is being practised in the participating districts. I have compared the findings in DF with the analysis of the qualitative data gathered from the FS field, in addition to reading relevant literature and previous research.

## 1.1 Delimitations and list of abbreviations

I will only focus on Digital Forensics and Forensic Science in the police organization and not in the private sector and will concentrate on the roles of the Digital Forensics Examiner (DFE) and the Forensic Technician (FT) and no other roles.

When I discuss DF in this thesis, it will be in relation to the DF conducted within the police. Due to the increased complexity of digital evidence, DF is divided into several sub-disciplines, such as mobile forensics, computer forensics, network and cloud forensics. I will not separate DF in these sub-disciplines in this thesis; DF will be the term I use for all disciplines. There are some abbreviations in this thesis, and in some strategic places, I have repeated the full descriptions to make it easier for the reader.

Translation from Norwegian is not always easy, especially in citations. Most translations have been done by me. There are although terms, publications, organizations or names that have not been possible to translate to English, so these are displayed in Norwegian.

### List of abbreviations:

#### COC – Chain of Custody

- *The process to preserve evidence in its original form and to document all actions done to the evidence in order to prove its authenticity and integrity (4, p.6)*

#### DE – Digital Evidence

- *"Digital Evidence is defined as any digital data that contains reliable information that can support or refute a hypothesis of an incident or crime" (4, p.7)*

#### DF - Digital Forensics (*Digitalt politiarbeid*)

- *"Digital Forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation 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" (4, p.6)*

#### DFaaS – Digital Forensic as a Service

- *a service-based approach for processing and investigating high volumes of seized digital material (16)*

DFE - Digital Forensic Examiner (*Dataetterforsker eller spesialetterforsker*)

- *A police or civilian with relevant competence who preserves, collects, validate, identifies, analyzes, interprets and presents digital evidence acquired from digital sources*

DFL – Digital Forensic Liaison (*Fagkontakt digitalt politiarbeid*)

- *A police or civilian with basic competence, primarily to conduct examinations on material acquired and prepared by DFEs – a support and "middleman/woman" for DFEs and investigators*

FS – Forensic Science (*Kriminalteknikk*)

- *"Examination, preserving and documenting crime scenes, persons and traces, with the purpose of discovering the events of a criminal act, fire or accident, clarifying the cause and identifying implicated persons" (5, p.5).*

FT - Forensic Technician (*Kriminaltekniker*)

- *An employee who is specially trained to identify, document and to preserve forensic evidence and who has forensic investigation as primary function", (5, p.5).*

FTC – Forensic Technician Coordinator (*Kriminalteknisk koordinator*)

- *Role with responsibility to coordinate the FS work and serve as a liaison between FS and the chief of investigations (34)*

ICT-Crime

- *Crime against computer systems and / or data networks, such as data breaches and service denial attacks (36, p.7)*
- *Crime where key elements of the course of action are committed using computer equipment and / or computer networks. This will in many cases be traditional crime, but it changes character, scope and effect due to new technology, such as threats, fraud and the spread of abuse images (36, p.8)*

NCFI – Nordic Computer Forensic Investigator

- *A description for a set of studies offered by the Norwegian Police University College in Digital Forensics (34)*

NCIS – National Criminal Investigation Service (*Kripas*)

- *National Unit for Combating Organized and Other Serious Crimes.*
  - o *national competence center for Norwegian police*
  - o *national contact point for international police cooperation*
  - o *responsible for processing central registers in the police*
  - o *national forensic laboratory*
  - o *an actor for prevention and social security (40)*

NC3 – National Cyber Crime Center (*Nasjonalt Cyber Crime Center*)

NDPP - Norwegian Director of Public Prosecutions (*Riksadvokaten*)

NPD – National Police Directorate (*Politidirektoratet*)

NPUC – Norwegian Police University College (*Politihøgskolen*)

QM – Quality Management (*Kvalitetsstyring*)

- *"Quality management is the activities to direct and control an organization with regard to quality" (7, e23)*

SDP – Section for Digital Policing (*Seksjon for digitalt politiarbeid - DPA*)

SFS – Section for Forensic Science (*Seksjon for Kriminalteknikk - KTEK*)

## 1.2 Research problem

The research problem of this thesis is:

*"Is the quality assurance in Digital Forensic work in the Norwegian police adequate?"*

The research problem is broken down to the following research questions:

- *Can Digital Forensics learn something from Forensic Science in terms of quality assurance of their work?*
- *Has the reform contributed to an enhanced focus on quality in Digital Forensics and Forensic Science?*

## 1.3 Research method

Since I want to investigate how quality assurance is conducted in DF and FS, I have chosen a qualitative approach in this study and have interviewed three DFEs and three FTs. The outcome of the interviews has been transcribed and analysed, in addition to reading relevant literature/theory mainly related to the fields of DF and FS in the subject of quality.

## 1.4 Problem description - why compare DF to FS

The thesis is a continuation of my project report, *Quality assurance in Digital Forensics in the Norwegian Police, is it good enough?* in which I carried out an initial study of the quality assurance in the fields of DF and FS in Norway. In this report, I got an impression of how FS had a more formalized framework of QM and more established practices to assure quality (3).

In the current study, my aim was to gain a more extensive knowledge about practice related to quality assurance in both the DF and FS fields.

## 1.5 What is Digital Forensics?

A definition from the introduction of A. Årnes's (2018) book, *Digital Forensics*, follows:

*Digital Forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation 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 (4, p. 4).*

## 1.6 What is Forensic Science (Kriminalteknikk)?

Below, I present the definition of *Kriminalteknikk* from the quality standard in the Norwegian police, *Kvalitetsstandard for kriminalteknisk etterforskning*, published by the *Norwegian Police Directorate (NPD)* in 2012 (5).

*"Examination, preserving and documenting crime scenes, persons and traces, with the purpose of discovering the events of a criminal act, fire or accident, clarifying the cause and identifying implicated persons"* (5, p.5).

## 1.7 What is quality in investigations?

This study will describe many different aspects of quality, and it is therefore important to explain the different concepts and what they mean.

In relation to quality in criminal investigations, in the *Kvalitetsrundskrivet*, the *Norwegian Director of Public Prosecutions (NDPP), Riksadvokaten*, referred to the term 'quality' as follows: *"Quality is often used to specify that the investigation and the prosecution have to satisfy certain demands or given standards"* (6, p.5).

The NDPP describes how quality should be understood and assessed in criminal investigations; states that an objective and transparent investigation process is necessary to be perceived as trustworthy to the society; and emphasizes the requirement to be objective in all parts of the criminal justice chain, to avoid errors of justice and to secure the rule of law (3, 6). The NDPP's explanations on quality in investigations will be further introduced in Chapter 2.4.

Quality management (QM) (*Kvalitetsstyring*), quality assurance and quality measures and controls are terms often referred to in this study. *"Quality management is the activities to direct and control an organization with regard to quality"*. *"Quality assurance (Kvalitetssikring), a part of QM, is focused on providing confidence that quality requirements will be fulfilled"*. *"Quality control (Kvalitetskontroll), a part of QM, focused on fulfilling quality requirements"*.

Explanations of the terms are gathered from Watson and Jones' (2013) book, *Digital Forensics Processing and Procedures - Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements* (7, e23).

## 1.8 What is Forensic Investigation?

Since DF is a branch of FS, the definition of Forensic Investigation, also taken from the Norwegian quality standard in FS, includes both fields:

*"Forensic investigation includes all elements of search, preserving and handling of technical and digital evidence. It also includes following up work done by external laboratories and experts"* (5, p.5).

Although the DFE and FT handle different types of evidence (digital vs physical traces), their general workflow processes are quite similar. They both preserve, identify, collect, validate, analyse, interpret and present their findings. There are some major differences in the workflows regarding the focus on quality assurance. This will be presented and discussed in Chapter 5.3 (3, 4).

French scientist, *Edmond Locard*, introduced a principle known as *Locard's exchange principle* in forensics, which states, "*When a person or object comes in contact with another person or object, a cross transfer of materials occurs*" (4, p. 3). The principle may not be directly transferable to DF, because the traces and leads are not in physical forms, but, when one visits a website, traces are stored on web servers, and cached content and logs are stored on the local device used for the activity. The crime scenes are not as defined as in FS, but traces and digital evidence material are created and present.

### **Definition and objectives in an investigation**

"*An investigation can be defined as a systematic examination, typically with the purpose of identifying or verifying facts*" (4, p.3). "*A key objective during an investigation is to identify key facts related to a crime or incident, and a common methodology is referred to as the **5WH**, defining the objectives of an investigation as **what, where, who, when, why and how***" (8, p.1).

A common strategy in investigations is to try to find answers to the 5WH questions, also referred to as the *Investigative star*, briefly explained as:

*What* happened, *Where* did it take place, *Who* is involved, *When* did it take place, *Why* did it happen and *How* did it happen? (9, p.26).

## **1.9 Structure of the thesis**

The thesis has five main chapters, beginning with an introduction in Chapter 1, in which I present my motivation, along with background information, for choosing the research topic.

In Chapter 2, *State of the Art*, I discuss relevant literature, theory and official publications regarding quality. The recent police reform's impact and influence on the DF and FS fields will also be discussed.

In Chapter 3, I present and explain the research methodology for the thesis. The results of the collected and analysed data are described in Chapter 4, which is followed by a discussion of the results in relation to the theory, in Chapter 5.

To conclude, a summary is presented, and future work related to the research is debated in Chapter 6.



## 2 STATE OF THE ART

### 2.1 Introduction

In my preliminary report (3), the reform introduced in 2016, with reorganization of the Norwegian police was described, with plans and measures, especially for raising the level of competence and quality related to criminal investigations. These changes have affected not only DF and FS but everyone working in the police. I will give an updated description, based on the preliminary report, with some new considerations and add-ons.

The results from the interviews in the current study have added a new dimension to the research, and some relevant new angles will be presented, in addition to a literature review.

It is important, however, to look at what is done internationally in terms of quality assurance. In the next chapter, relevant theory about the subject will be presented, with a focus on DF. The importance of focusing on DF is due to the fact that it is a new field in forensics and the Norwegian police are presumably influenced by international methods, tools and guidelines, because, as will be presented later, there are few guidelines/instructions in DF in Norway, compared to FS.

It is also important to investigate what other researchers have done in relation to my research problem, and to document some of the history of DF.

### 2.2 Background and theory – Digital Forensics

When I told a distinguished colleague, with 20 years' experience in DF, about my research problem, he commented: "*Well, I think the quality assurance in our field takes place in the preparation*". This statement fits very well with the situation today: A wide variety of courses on DF are offered to prepare the DFEs for their work. However, the question is whether knowledge is an adequate measure to mitigate errors.

#### Brief history of DF

Politt describes the history of DF as short but complex and in epochs in decades from before 1985, which he names "pre-history". At the beginning of the 1980s, individual hobbyists, interested in computers, within law enforcement and government agencies, started sharing what information could be extracted from the new personal computers. At the start, and for many years, the DF field was called *Computer Forensics*. The discipline did not start in a lab environment but in offices and basements, with examinations being conducted at desks and wherever there was space. There are several steps that could be described to highlight the rise and evolution of the DF discipline, but these will not be described in detail in this thesis. Gradually, the discipline evolved, due to the rapid technological development, with the Internet, data carriers, and many other factors.

This led to a new organized discipline in governmental institutions, agencies and private companies, called Digital Forensics (10).

## **Relevant theory and previous research - related to quality in DF**

In the UK, a government-funded institution was established in 2007 within the legal system, called the *Forensic Science Regulator*. The institution has the function of: “*The Forensic Science Regulator ensures that the provision of forensic science services across the criminal justice system is subject to an appropriate regime of scientific quality standards*” (11). DF is also undergoing scrutiny for the implementation of suitable quality assurance measures, and DF units in the UK can get accreditation of their labs and methods according to the *Codes of Practice and Conduct* (12).

In the Netherlands, *The Netherlands Register of Court Experts*, is a measure established to assure high quality standards, as demanded by their *Experts in Criminal Cases Act*. They have created a detailed *Code of Conduct* for the registered court experts. The website, where you can find the list of registered experts, has the illustrative headline: *The Netherlands Register of Court Experts connects law and science*. There are registered experts in many different fields of science, including DF, and one can look up the registered experts on the website and find the subjects in which they have expertise. To become a registered court expert, one must submit a detailed application with documentation within the field of expertise. There are defined areas in FS, and several under DF, like Network Forensics, Computer Forensics, Device Forensics, etc. If one is accepted as a court expert, the period of acceptance is five years before one must re-apply/re-register (13).

Not all DF experts are convinced that accreditation is the right solution for DF. In his article, *Accrediting digital forensics: what are the choices?*, Peter Sommer, a professor at Birmingham City University, discusses quality assurance measures like the accreditation of labs and procedures, individual experts and court procedures in the DF, and points out that the complexity and change rate in digital evidence can make it difficult to create standards that fit the DF; he suggests advisory good practice guides instead (14).

The same issues have been debated at the advanced DF lab at NC3, NCIS, in Norway, where the choice has been made not to seek to accredit the labs or methods. According to head engineer, *Kjell Harald Andersen*, contacted on June 5, 2020, who is responsible at the advanced national DF lab at NC3 at NCIS, their reason for not undergoing accreditation is the rapid shifts in the methods they have to develop and use to acquire and analyse data, and therefore it is not appropriate to accredit the methods. Secondly, Andersen said it would be extremely resource-intensive to maintain an accreditation system on this, demanding full-time positions, and these kinds of resources are currently not available. Andersen said they have similar quality systems established at the lab:

*That said, we have created a kind of quality system based on some common principles for such systems. That is, we have defined workflows, checklists, documentation requirements and nonconformity systems, but we are not subject to any external audit of this, and it is not approved by any external party.*

*It all boils down to individual employees' personal integrity, open and serious discussion, and tolerance for admitting mistakes without unreasonable consequences. This has to do with culture and is completely independent of certification and accreditation.*

## **Previous research**

Several studies have been conducted in Norway in relation to quality assurance in DF in recent years. In his study, *The Paradox of Automation in Digital Forensics* (15), Borhaug examined *Digital Forensics as a Service, (DFaaS)*, and the considerations when automating the DF process, also as regards quality. Digital Forensics as a Service is a service-based approach for processing and investigating high volumes of seized digital material (16). Borhaug explains that *"The paradox of automation is when the work processes are increasingly automated which means less human intervention, but the human control is also increasingly important"* (15, p.79). What a data system produces, or processes must be verified; this is important in using any tool and method in DF, and this must be carried out by a human resource. A judge in court should not accept a report that says that an automated data system found the evidence, without quality control, verification and consideration by a human. According to Borhaug, in a DFaaS system *"Humans are less involved, but their involvement becomes more critical"* (15, p.79).

In his (2019) research, *Digital investigation: The malnourished child in the Norwegian police family?* (17), Heitmann investigated the digital competence Norwegian police officers possess. The results from the research indicated a lack of competence when the police faced DE, especially in the early stages of an investigation involving DF. He also pointed to the fact that there were inadequate systems for the verification of digital evidence before it was presented in court. Another finding in the study was that there were no competence requirements for investigators working with digital investigations, and that the training in digital investigation in the districts seemed to be insufficient. Of particular value to this study was the finding that 56% of the respondents in the research had not had a review or control of the material by others, before presenting it in court (17 p.70).

*Erlandsen*, in his research, *Fallacies when Evaluating Digital Evidence among Prosecutors in the Norwegian Police Service* (18), carried out a case study in which he had police prosecutors weighing digital evidence in fictive criminal cases. The study indicated that prosecutors with postgraduate studies in DF weighed the digital evidence more correctly and reasonably than the prosecutors without any postgraduate studies in DF, who only weighed the judicial aspects of the case. This could lead to wrong conclusions which could, in the worst case, end with miscarriages of justice or wrongful acquittals. As measures to avoid fallacies in criminal cases, Erlandsen recommends studies/courses in DF for prosecutors;

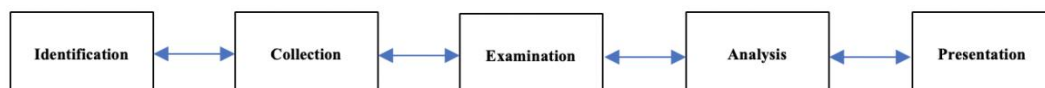
obligatory quality peer reviews for DFEs and others that analyse digital evidence; "increased use of visualization of the digital evidence when presented to the prosecutor"; and mandatory walk-throughs of the digital evidence with prosecutors before trials in courts" (18, p. 77).

In 2017, Sunde carried out a qualitative study, *Non-technical Sources of Error when Handling Digital Evidence within a Criminal Investigation* (19), which focused on the possible human-related error-factors in handling digital evidence, posing a risk for quality and the rule of law. The results from the study suggest that cooperation between DFEs and tactical investigators was considered successful when DFEs were involved at the early stages of investigations containing DE. Other findings related to good cooperation in DF investigations were "clear leadership and adequate resources" (19, p.4). In the study, Sunde identified sources of errors when investigating digital evidence during the DF process, such as insufficient investigative competence, the right competence not being present at the right time, cognitive bias and organizational challenges. "Errors may cause poor quality and efficiency of the investigation, which again may lead to insufficient protection of the rule of law in the form of inadequate penalties, wrongful convictions or acquittals", Sunde concludes (19, p.4).

## The Digital Forensic process

The digital forensic process exists in many versions. INTERPOL uses the steps in the process to initially explain what DF is: "Digital Forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing and reporting on data stored on a computer, digital devices or other digital storage media" (20, p.12). The process aims at preserving evidence integrity and the Chain of Custody (COC).

Figure 2.1 The Digital Forensic Process (modified by me)



A brief explanation of the phases in the process follows:

Figure 2.1 shows the Digital Forensic process gathered from my preliminary report (3). The process uses the same phases as in Flaglien's book, *Digital Forensics* (21, p.16). Flaglien describes the process as iterative. I have modified Fig. 2.1 with the arrows pointing both ways in all phases to demonstrate that it can be iterative in the whole process.

*Identification* is of possible digital evidence, *collection* is copying data, *examination* is processing and structuring the collected data, *analysis* is to seek and find possible evidence in the data, while *presentation* of the findings takes place in reports or in courts or in other interests.

The iterative process can be explained as the necessity to go back and forth in the phases to test the hypotheses, validate findings, and identify and collect

subsequent new evidence discovered in the examination and analysis phases (3, 4).

The process enhances quality control, by ensuring evidence integrity and the chain of custody, by documenting all the steps – but the control is allegedly conducted by the DFE him/herself (3).

## **Quality assurance in DF – recommended measures**

Measures in quality assurance can be divided into two categories, *preventive* and *control* measures.

Preventive measures can be explained as concerning the environment the digital evidence is handled and processed in, like laboratories, where methods and tools have been tested and approved due to a certain standard, and where the personnel who handle the evidence are required to have a certain competence and follow rules/guidelines to conduct the work processes (22).

This is also referred to as *Digital Forensic Readiness*, to be forensically ready, to be prepared to efficiently conduct digital investigations and present the evidence in a court of law or before others (22, p.117).

Control measures are those related to control activities undertaken during the handling of the digital evidence and the assessment of the results.

## **Preventive measures**

*Standardization* and *accreditation* refer to ISO-standards and are described by the ISO organization as a formula that describes the best way of doing something. Laboratories and methods can be accredited at ISO-standard levels, which means that, if certain procedures are followed and technical requirements are met, accreditation can be achieved. This is considered a recognition of quality (54). The national FS unit at NCIS has an accredited laboratory, in accordance with ISO 17025, and accredited methods within e.g. ballistics, fingerprint analysis, and chemical analysis (23).

As already referred to, *Chain of custody (COC)* and *evidence integrity* are important terms in DF. They are the basis for all digital forensic work to handle digital evidence in a *forensically sound* manner (4, p.6). Evidence integrity means maintaining the evidence in the original form and not changing it in any way throughout the whole DF process. COC is the process of documenting every step of the handling of the seized evidence, physical or digital, in a case, to assure transparency (3, 4 p.6,).

*Competence* is a critical part of DF. People investigating digital evidence need to have competence and training in investigation techniques, the DF process, methods and tools, procedures, guidelines, current rules and laws, as well as skills in communication. Different roles can be defined for some of the knowledge needs mentioned, but a DFE in the police in the districts probably needs them all (22).

Templates and checklists are mechanisms that can underpin standardization and may facilitate presentation in a balanced and transparent manner, in terms of both procedures and results.

## **Control measures**

Dual-tool verification is a quality control measure conducted on digital evidence in the DF process. The measure is aimed at checking whether two different tools interpret the meaning of the data similarly. For example, when exploring the metadata of a file, the measure could be used to check whether the different tools interpret and display the same timestamps, based on the same metadata (4, p.32).

However, dual-tool verification has several limitations. A similar result obtained from two different tools is not a guarantee for validity, since two tools may produce the same – but incorrect – conclusion. In addition, the result does not indicate anything about the probative value of the evidence in an investigation. Hence, dual-tool verification alone is not an adequate quality control measure.

Page et al. (24) compared the quality procedures in the examination of digital evidence, body fluids and DNA evidence in the UK, and concluded that there was a lack of comparable quality control measures in DF compared to the other disciplines. The situation in the UK seems to be somewhat similar to that in Norway, at least regarding quality control measures. Examples of QM and quality assurance in FS disciplines, like fingerprint examinations and DNA analysis, are demonstrated, and the authors recommend similar measures for the DF field. The authors suggest quality control conducted by other qualified experts in five levels of peer review for DF. *Peer review is the procedure by which a professional of equal standing conducts a quality review of work, often in scientific environments* (3, 24).

Sunde refers to the peer review model suggested by Page et al. in Årnes's book, *Cyber Investigation*, in the chapter, *Cyber investigation Process* (25, p.23-24), where she recommends the five levels and proposes how they can be implemented as control measures for quality assurance in cyber investigations.

Page et al. also recommend the dual-investigator/examiner principle for quality assurance, where two DFEs work together during the whole process. This approach can prevent errors in investigations: *"Dual-examining does not double the workload like a re-examination, but adds the benefit of multiple practitioners being able to collaborate during an investigation, exposing findings to twice the scrutiny and twice the discipline specific experience and investigatory knowledge"* (24, p.8).

These recommendations will be discussed in Chapter 5.

## **Principals and guidelines in DF – examples**

Multiple guidelines for DF have been published. The purpose is to guide DFEs in good practice in handling digital evidence and conducting digital investigations.

A widespread and frequently referenced guide for good practice in DF is the *Association of Chief Police Officers' Good Practice Guides for Digital Evidence* (26), with four principles for handling DE.

The guide was first published in 1998, with the last version coming out in 2012 (27). The principles are followed by a detailed explanation on how to handle variants of digital evidence in the UK, with appendixes. The ACPO were replaced in 2015 by the *National Police Chiefs' Council* and the ongoing programme, *Transforming forensics* (28), but the principles are still referred to by reputable organizations, for example INTERPOL (27).

DF is one of the major areas listed as needing transformation in the police in the UK. Another major area listed is ISO accreditation, and it is stated that "*All elements of forensics will be required to undergo ISO accreditation to ensure quality standards are upheld*" (28). Until new principles are eventually presented, the Good Practice Guides for Digital Evidence still guides DFEs in how to handle digital evidence. The four principles are (26):

**Principle 1:** "No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court."

**Principle 2:** "In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions."

**Principle 3:** "An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result."

**Principle 4:** "The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to."

In the recent article, *ACPO principles for digital evidence: Time for an update?* Horsman suggests a revision of the principles he sees are outdated and suggests "*Eight revised principles as a means of acknowledging the current challenges faced by practitioners in this field*" (27, p.1).

It is not in the scope of this thesis to go through all eight suggested principles, but, in short, they are broken up and derived from the current principles and are more detailed in how one should handle digital evidence and – especially relevant for this study – "*All extracted and interpreted data deemed to be 'digital evidence' must have undergone robust testing and validation using accepted testing methods and peer review in order to verify accuracy.*" (27, p.4, Principle 7).

INTERPOL has a newly published guideline, the *Global guidelines for digital forensics laboratories* (20). The guide refers to the ACPO and is very detailed in describing everything from setting up a DF laboratory to handling all kinds of DE, competence qualification requirements, standardizations, reporting, accreditation and quality assurance.

The quality assurance recommendations in the guide involve professionalism when it comes to laboratories, equipment, staff training, validation and verification of methods, and there is a specific chapter on quality assurance. It recommends a technical and administrative review of the forensic results, which probably means a quality control measure like peer review, conducted by others (20, p.56).

## **2.3 The reform – brief history and purpose**

Since one of the main goals of the reform was to raise the quality of policing in general, it is natural in this study to describe some of the main measures introduced and conducted (1). It is not easy to be brief in describing the reform, but the broad lines of the history, with the major events, prior to and during the reform, will be presented.

After the terrorist attacks in Oslo and on the island of Utøya in July 2011, a government-initiated commission evaluated the police effort, and a report was delivered to the authorities in August 2012, *Rapport fra 22. juli kommisjonen* (29). Several challenges were uncovered in leadership, cooperation, how the police were organized and their emergency readiness.

In November 2012, a new commission was appointed with a mandate to investigate the police and to uncover possible areas of improvement. In the summer of 2013, the commission delivered its report, *Politianalysen*, which resulted in several recommendations for how the police could be better organized in the future to handle their societal function (30).

This led to a proposition to reform the police, in the spring of 2015, *Nærpolitireformen*, which was approved by the Parliament in June 2015 (1).

The reorganization started in January 2016, and one of the main goals of the reform was to create more robust districts with units/sections that were better organized and rigged for handling large-scale crises and investigations. Another was to make the police better at coordinating and organizing themselves digitally, to meet future challenges.

## **2.4 The reform – enhancing quality in investigations**

The reform is also called *the quality reform*, and a major part of it was to raise the competence and quality in investigations and the overall work with criminal cases in Norway (1). In the spring of 2016, the NPD released a strategic plan to raise the competence in investigations, *Handlingsplan for løft av etterforskningsfeltet, (Etterforskningsløftet)*, (31). The plan was a result of cooperation between the NDPP and the NPD.



The NDPP had, for a long time, called for a general increase in competence in the field of investigation.

The NDPP listed a set of markers of quality in the plan, related to the whole *criminal justice chain*, which represented his office and the NPD's improved concept related to quality in investigations. One of these markers refers to the fact that the quality concept in investigations should focus not only on results but also on the important side of dedication to and execution of the task. This is an important concept because there has been a dominating focus on results, such as time spent per investigation, in the police in Norway. This is important, for both the public and the police but must not affect the quality of the investigative work (3, 31).

For most of the investigators, chief investigators and police attorneys, the investigation reform introduced yearly training in investigation-related subjects, to raise their level of competence. This was initiated in 2018, with a combination of virtual, self-study and physical meetings in different subjects. As a part of the plan, the districts created new positions responsible for the subjects of investigation and law. These coordinators were given special tasks to take care of and to follow up competence enhancement in the districts, as well as regarding the yearly training.

## **2.5 The new organization – new DF and FS units**

The police districts were reduced from 27 to 12, and several of the old districts were merged into larger districts, in terms of both the number of people to serve and the increased geographical area of responsibility (1).

DFEs were gathered in sections or units called *Seksjon/Avsnitt for Digitalt Politiarbeid (DPA) (Section for Digital Policing (SDP))*. There were new role descriptions in the guidelines, with detailed descriptions of areas of responsibility for the DFEs, for *Fagkontakt DPA, (Digital Forensic Liaisons (DFL))*, for of SDP leaders and so on (32).

The same was done in FS with the FTs. They were organized in larger sections or units, *Seksjon for Kriminalteknikk (KTEK) (Section for Forensic Science (SFS))*, and the guidelines provided detailed descriptions of the roles of the FTs, role descriptions for SFS leaders, and so on (32).

In early 2019, the NPD published new competence requirements for many of the defined roles within the police (33). For a DFE, a police education or other relevant bachelor is required, in addition to three years of experience in DF. As base knowledge in DF, *Nordic Computer Forensic Investigator (NCFI) Core Concepts (15 ECTS)*, the introductory course of study at *Norwegian Police University College (NPUC) (Politihøgskolen)*, is required (20). Civilians are also required to undertake study in investigation and a 15-ECTS study in criminal investigations (34). This will be further discussed in Chapter 5.

For an FT, a police education or other relevant bachelor is required, in addition to three years of experience in FS. As base knowledge in FS, *module 1A*, the course of study at NPUC, is required (34). There is also a role description for the *Forensic*

*Technician Coordinator (FTC)*, which is a newly established role, with the responsibility for coordinating the FS work and serving as a liaison between FS and the chief of investigations. The role requires extensive competence and experience. Due to the scope of this thesis, I will not compare this function to that of the DFE in detail, but it will be described to some extent, because some of the interviewees explain the value of the role in terms of quality assurance.

## **2.6 Competence and quality standards in DF – status**

### **Competence**

The first DF study was introduced by NPUC as a 30-ECTS part-time course in 2004. Since then, NPUC has developed a broad range of various educational courses in DF. The courses currently have three levels, the third level of which is part of the master programme, in cooperation with the *Norwegian University of Science and Technology*: an experience-based master programme (3, 34, 35).

The entry level 1 study for all the DF studies is the NCFI Core Concepts. After completing level 1, students can choose to follow and specialize in three paths: *Advanced Computer Forensics, Online Investigation and Network Forensics & Cybercrime*.

At level 3, there are currently a variety of advanced studies in Windows, Linux, and Macintosh computer forensics and also modules in memory forensics, forensic tool development and a new module in report generation visualization (34).

The information on the different courses in the learning outcome sections states that NPUC aims for high-level skills and quality in forensic investigations (34). Over the past 10-15 years, NPUC has established relationships and cooperation with police academies in other countries in Europe.

According to Police Superintendent and Head of the DF education at NPUC, *Ulf Bergum*, contacted on May 6<sup>th</sup>, 2020, all the Nordic countries and Poland and Germany are currently participating and contributing at NPUC's NCFI studies, and DFEs and investigators in the police in these countries attend the various study courses in the NCFI portfolio.

Given the broad spectrum of offered studies in DF, if DFEs in Norway are motivated and allowed to attend, this should give them a solid base for conducting data-technical examinations and delivering high-quality digital forensic work. All the interviewed DFEs had completed one or more NCFI courses of study.

### **Quality standards**

The NPD's report from 2012, *Politiet I det digitale samfunn* (36), describes the situation prior to the reform and concludes that standards are needed in methods, tools and competence, to meet the challenges in the DF field and handle digital evidence in investigations with good quality (3, 36).

The only official document that some interviewees referred to as an instruction in DF was circular 2010/007, rev. 2017 from the NPD *Behandling av beslag I straffesaker* (37).

There are explanations on what digital evidence is or could be, how and what data/information can be seized and, most importantly, that digital evidence can only be seized by qualified personnel with special and adequate training, equipment and software (3, 37):

*Acquiring digital evidence requires special competence and must not be conducted by personnel without adequate training, equipment and software. A seizure report should be prepared, in addition to a report which provides an overall description of the procedures used in the acquisition process* (37, section 3.3).

This is, currently, the only official instruction/standard in respect of how digital evidence should be handled in Norway.

One measure in the investigation reform process was to establish a professional and academic development apparatus to systemize the development in several professions related to the field of investigation.

By order of the NPD, in association with the NDPP in 2018, national groups were created within disciplines in the investigation field; this apparatus is called *Fagforvaltningsapparatet*. These groups were tasked with developing and identifying the need to enhance the quality in their respective disciplines. This measure was an important part of the reform, and the DF and FS fields were two of the professional disciplines, both groups led by NCIS, with competent participants from the districts. The groups have the responsibility for creating and further developing methods, standards, and procedures for national use (3, 38). The national groups began their work in January 2019. The status of their work is not available because it is exempted from public scrutiny.

*The Department of Justice* published a strategy document in 2015, "*Justis -og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*", in which they agreed on establishing a set of measures to combat Cybercrime (3, 39).

One of the measures in this document was to create a *National Cybercrime Centre (NC3)*. It was established in January 2019 and is under construction. The centre is a part of NCIS, and it is planned to increase the number of employees. NC3 aims at preventing, averting and combating technologic criminality, especially cybercrime and Internet-related crimes against children. NC3 has a national digital forensics laboratory and assists the districts and special branches in the police with its expert scientists (39).

NC3 develops methods and tools in advanced data-technical examinations and data-technical investigation and acquires possible digital evidence from digital devices, data systems, Internet, service providers and manufacturers. The centre also offers training, guidance, "HOWTOS" and instructions on how to acquire and process investigative information from international service providers, especially from Internet-related sources. The centre also develops and conducts tactical and technical prevention solutions on the Internet, both hidden and open (3, 39, 40).

All units in NCIS assist the districts in severe crimes cases, including specifically challenging tasks which require expertise. It is the national unit for combating organized and severe criminality and is also the national point of contact for international cooperation with the police in other countries. Together with the NPD, NCIS has also developed a national digital wiki for subjects and methods related to police work (40).

## **2.7 Competence and quality standards in FS – status**

### **Competence**

There are several specialized education courses for FS, and four levels of education. As in the DF field, there is a basic entry-level study, module 1A, with a focus on the crime scene. Other modules in level 1 are photography and documentation. At levels 2 and 3, one can specialize in different subjects like fire-related crime scenes, violence and death, severe accidents, blood traces and explosions.

The newest, and highest level four course, released in 2018, is education for the Forensic Technician Coordinator, FTC, which, as referred to in Chapter 2.5, focuses on cooperation between the FTs and the chief investigators in criminal investigations. According to the education programme, the course aims to ensure that forensic science work is being done with the highest quality (3, 34).

In areas like fingerprint identification and DNA analysis, districts send samples collected in their daily service for registration and the possible identification of suspects in criminal cases. The quality control of these collected samples is performed at the forensic laboratories at NCIS or their cooperatives, such as the *Oslo University Hospital*, which performs DNA and toxicologic analyses for the police.

FS at NCIS is associated with several laboratory functions, like laboratories for the ballistic research of firearms, chemical laboratories for different analyses like the identification and registration of quantities of drugs, handwriting examinations, fingerprints, fire-related examinations, etc.

NCIS has a national responsibility for most of these laboratory functions. The districts send material, like drug samples, for laboratory examination and registration at NCIS, and in return they receive reports with the results, when the examination/analysis has been conducted (3, 40).

### **Quality standards**

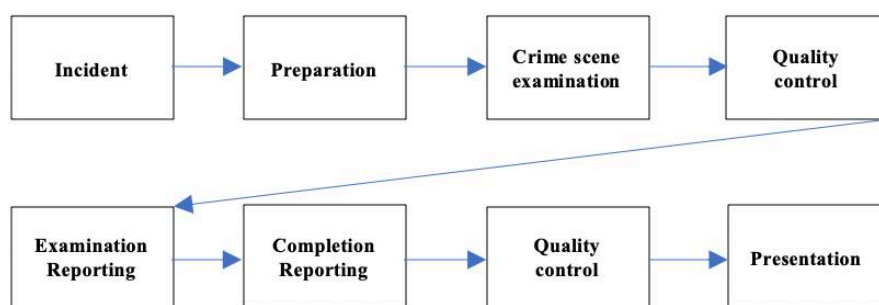
NCIS has national responsibility for the development and implementation of new technology and methods in the FS field in Norway. This is specifically emphasized in the quality standard document from the NPD (5). Although Digital Forensics is included as a discipline under the umbrella term 'Forensic Science', it is stated explicitly that Digital Forensics is excluded from the requirements of the document (3, 5).

Some important excerpts from the quality standard, which describes FS education and how FS should be organized and managed with quality assurance measures implemented in the Norwegian police, follow (3, 5):

- The document defines a standard for all work in the FS field with areas of responsibilities set for the local districts, the NPUC, the NCIS and the NPD, in order to assure that the guidelines within are followed and maintained.
- Quality management is defined as a responsibility for the leaders in the districts, to further create routines that assure quality in every part of the forensic work, so that processes are documented and can be verified. The responsibility also includes having a system for following up faults/mistakes and for identifying, documenting, analysing and reporting them with the measures that have been taken.
- Review of all reports and verification of the documentation in the examinations should be conducted by at least one qualified person.

There is also a flowchart, illustrating the forensic science workflow in the document, with steps of quality control. Figure 2.2 is a recreated illustration of the flowchart translated in English by me, adapted from my preliminary report (3, 5).

Fig. 2.2 Forensic Science Workflow Process



There are two quality controls in the process. The first is typically after collecting or seizing and preserving possible evidence at a crime scene. The second control occurs when examination and reporting is completed, before an eventual presentation in court. The process will be compared with the DF process in Chapter 5.

## **3 METHODOLOGY**

### **3.1 Introduction**

Choosing the right research method is an important part of a thesis. There seemed to be moderate knowledge on how quality is handled in DF, and it was an opportunity for me to investigate this theme more closely in this thesis.

To obtain a descriptive picture and to seek knowledge of how the two professions handled quality assurance and management, a qualitative approach was chosen. Qualitative research involves forms of in-depth interviews which give researchers insight into how people perceive the world and what matters to them.

The study could have been even more informative if I had used other approaches, in addition to the interviews, like questionnaires or observations, a *triangulation method*, but that is outside the scope of this thesis.

### **3.2 Research method**

I have conducted qualitative individual interviews of informants who have self-experienced knowledge about the subjects in my research, from both the DF and the FS milieus. The theme and subject of this research has been the prime guide for the choice of research method. The purpose of a qualitative research method is not to measure or test theories but, rather, to explore, in order to gain a better understanding of a situation or situations.

Qualitative research is characterized by describing reality with texts and not with numbers, figures, tables and statistics. It is important that the researcher is aware of his/her own perception, experiences and standing regarding the issues in the research. Although it cannot be assumed that the researcher will not be influenced by his/her theoretical background, experience and self-lived events, it is important for the researcher to set these aside as much as possible.

My background could be a disadvantage for me in my research, since I have over 30 years' experience of the Norwegian police, but, by emphasizing and highlighting this, I hope to reduce the risk of wrongful influence of the outcome/result of the research.

On the other hand, my experience might also be an advantage. My prior knowledge allows me to focus more directly on areas that I know are relevant. My knowledge could also increase my ability to challenge the interviewees with more specific questions about what they say during the interviews.

### **3.3 Phenomenological perspective**

A study with a phenomenological perspective focuses on a phenomenon that will be explored, often with the starting point of an individual's experience of the situation and how he/she describes it (41). The study often involves a group of individuals who have experienced the phenomenon. The group varies in size from

3-4 to 10-15. Data collection in the form of interviews of the individuals is the most common procedure, followed by data analysis of the transcribed content of the interview material (42).

One type of phenomenological approach is a *hermeneutical phenomenological perspective*, which is described as combined research of self-lived events/experiences and analysis of texts (42). This research leans towards this type of phenomenological perspective, since I focus on the interviewees' experiences and perspectives and aim at a rich and detailed information basis for how quality assurance is carried out in DF and FS.

### **3.4 Gathering information - research interviews**

In the process of gathering relevant information for the research, I first decided to interview DFEs and FTs working in police districts in the Norwegian police. To capture differences in the way the two professions work to assure and manage quality, I chose to conduct in-dept research interviews with informants from a small, a medium-sized and a large police district, summing up to three DFEs and three FTs. As described in Chapter 2, the Norwegian police has just gone through the largest re-organization in history and has been reduced from 27 to 12 districts. Smaller units have been merged into bigger departments/sections, to become more robust and effective.

My motivation for choosing informants from small, medium and large districts was to capture essential differences in how they worked with quality assurance/management in those three dimensions. Oslo police district was not chosen because it differs in organization and size from the other districts in the Norwegian police.

Another important factor I considered when choosing informants was their experience within the fields, since I ask about the quality focus prior to and after the reform. I therefore chose informants with six or more years' experience in the DF and FS disciplines. A qualitative research interview is a "longer run", with planning, execution, and the analysis process thereafter. Choosing the right form to obtain the most accurate answers to the research questions can be a challenge.

I chose to conduct semi-structured face-to-face interviews in which all the informants were asked the same questions but where I could follow up with questions, depending on their answers. In this kind of interview, the follow-up questions will differ, allowing the interviewees to bring up relevant topics and issues that were not covered in my plan.

This is a looser form of interview, more like a conversation, and probably the best suited for my project, to be able to collect and gather relevant information associated with the informant's own experiences and meanings related to quality assurance and management in their work (41, 43).

Kvale and Brinkman describe this as the world-life interview, "Where *the purpose is to capture descriptions from the informant's world of life, to be able to interpret the importance and meaning*" (41, p.22).

There are downsides to being an "inside-researcher" and conducting this type of research interviews. The interviewees know who I am, and I know them, and this could have created barriers, preventing me from asking critical questions. Another matter to consider is the "*Hawthorne effect*", where people participating in a study can change their behaviour because they know they are being observed in a piece of research (43, p.104).

It is important to be aware of possible biases related to this; for example, some interviewees can describe a situation in a more positive way than it really is or act differently to be helpful/kind to the researcher.

### **3.5 Data collection and ethical considerations**

The informants were recruited by my calling them personally. The appointments for the interviews were set, and, before each interview, I informed them that I would record the interviews and preserve the recordings in a safe environment/place with encryption. The interviews lasted from 20 to 40 minutes. Participants were also told not to reveal confidential information, since I had not applied for exemption for this in my preliminary application to the NPD. I received the consent from the NPD to conduct interviews in November 2019.

The fact that I did not apply to get exemption from the duty of confidentiality might have had an impact on the informants: they might have constrained themselves in the way they answered the questions in the interviews. I discussed this with my supervisor, and we agreed that this probably not would result in significant biases, since my research would not query criminal cases and other confidential data. When my application to the NPD was processed, they agreed on the fact that my research would not be dealing with confidential issues or data.

I also applied to the *Norsk Senter for Forskningsdata* to conduct the interviews and received consent/confirmation in November 2019. As an important part of its work, this institution manages and considers all research that involves the processing of personal data in Norway, to assure that the data is treated carefully and securely with minimum possibility of misuse (44). The recorded interviews were stored on an encrypted drive, which could only be accessed by me, and the transcriptions from the interviews were anonymized and stored on the same encrypted drive.

The interviews were conducted in February 2020, all on Skype. In advance, I had made an interview guide, in which I had constructed questions which I hoped would provide the most honest answers to the project. I hoped that the themes would encourage discussions during the interviews.

I also sent an information circular to the informants, in which I told them about my project and how I wanted to gather information from relevant participants. In this circular, I also informed them that participants could withdraw from the project at any given time.



## **Motivation for and explanation of the questions in the questionnaire**

The interview guide with the questions asked is attached in Appendix 4.

The first questions I asked the interviewees were about the management's focus on quality prior to and after the reform, and whether any forms or systems of quality assurance and QM were established. The aim of these questions was to measure essential differences in quality assurance related to the implementation of the quality reform.

The second part of the interview guide concerned competence, essential competence plans and whether any form of standards had been established for methods and tools. My motivation for this was to investigate whether any such measures had been introduced in the participating districts, because there could be variable constellations, since there are so few national guidelines, especially in DF, in the Norwegian police. The third part was about which type of quality controls were conducted, how, and by whom, to gain insight into how the DFEs and FTs assured quality in their daily work.

The last questions were about perception of the term 'quality' and whether the participants felt the quality measures in their units were adequate. People may have different perceptions of the term 'quality'. I also wanted to capture the participants' views as regards whether the quality measures were satisfactory, and if they had suggestions for measures to improve quality in their work.

## **Additional information sources in this study**

During the work on this research, it became crucial to contact a number of resource persons in the police, to clarify some issues that arose along the way. Used citations from the conversations were sent to the contributors for approval, to check that the citations were correct translated. The contributors had no objections.

## **3.6 Transcription of data**

Transforming a video-recorded interview to text was a new experience for me. It can be time-consuming, especially if you have not done it before. I initially considered using a transcription tool, and tried to use *Google Speech-to-Text* but it did not give a satisfactory result.

Kvale and Brinkmann describe this structural process of transcribing from oral to text as being easier and more suitable for analysis. "*The structuring gives a better overview of the material and is in itself a start on the analysis*" (41, p.206).

I transcribed the interviews probably a month after they were conducted. This was because I had an extensive workload period in my daily work. I do not know whether this had a negative effect on the transcription process. When I performed the transcriptions, I remember that I thought the opposite: that it was

good to have a distance in time because I had had time to reflect on the aspects and circumstances of each interview. Each interview had its own “soul” or place in my memory. I learned a lot from transcribing the interviews, especially regarding my own behaviour in the conversations, and I presume I got better as a researching interviewer by the end.

Kvale and Brinkmann warn not to see the interviews as transcriptions but as what they are, living conversations (41, p.218):

*Too much focus on the transcription can lead to a fragmented analysis, and the text is reduced to a collection of words or individual opinions perceived as verbal data. The alternative to the focus on transcriptions is to ask: How do I analyze what the informants told me in a way that enriches and elaborates the meaning of what they said.*

### **3.7 Data analysis**

Creswell describes the characteristics of five different approaches in qualitative research. For phenomenological research’s data-analysis procedure, the author highlights analysis strategies as “*significant statements, meaning units, textual and structural description and description of the essence*” (42, p.105).

I used Malterud’s *Systematic Text Condensation* as the method for analysing the data (45). This approach is a method of thematic cross-sectional analysis of qualitative data and is developed to give beginners an easy approach to how the analysis process can be conducted in a systematic and manageable way (45, p.97).

The analysis process is performed in the following four steps (45):

1. *Getting an overall impression*
2. *Identifying meaning units*
3. *Condensing the substance of the meaning units*
4. *Summarizing the essence in the material – recontextualizing*

The first transcriptions I did were more like summaries, so it was difficult to structure the text into descriptions of essential value, statements and meanings, but I gained an impression of possible themes to start with. I did the transcript process in a more thorough and detailed way the second time and used a data program to structure and code the text into meaning units. There were a lot of citations that illustrated meanings in the text, that I also coded. This process is iterative, and I had to go back and forth to get to know the material well, and to extract the essential descriptive codes.

In step 3, I extracted the elements in the text that I had coded as meaningful and sorted them by codes and also sub-codes.

In the last step, I created categories, which I thought summarized the meanings from the extracted code groups, compared to the raw material.

According to Johannessen et al., this is an important step, to check whether the impression from the analysed material coincides with the impression from the un-coded material (46, p.176).

The categories were:

- Focus on quality after reform of the police
- Focus on quality after investigation reform
- Competence plans or planning
- Accreditations, certifications or standardizations
- Quality management – instructions/standards
- Quality assurance – what is done – is it adequate?
- Perceptions of the term 'quality'

### **3.8 Quality assurance**

The role of the researcher as a person – his integrity – is crucial for the quality of the scientific knowledge and for the ethical decisions taken in qualitative research. It is important that the results are controlled and validated as far as possible before they are published, and a striving for transparency is essential, to explain how the processes led to the results and conclusions (41, p.108).

Validity in qualitative research should be addressed at the start of the study, actually at the planning stage, to avoid conducting a study that has little worth and credibility, in terms of either minimizing alternative explanations for the obtained results or being generalizable to the real world (43, p.106).

Researchers do not necessarily use 'validity' as a term descriptive of their research but, instead, use terms like 'quality', 'credibility', 'trustworthiness', 'confirmability' and more (42, 43, citing Lincoln & Guba (1985), O' Cathain (2010)).

Creswell presents eight possible strategies to increase validity and suggests using a minimum of two of these strategies in research (42).

#### **Internal validity**

First, I have tried to clarify possible biases for me as a researcher. This is a strategy Creswell names *clarifying researcher bias* (42).

I have described my background, current employment, that I know who most of the participants are, and that they know who I am. I have openly made it clear that this may influence the results. This will give the reader an opportunity to consider the validity of the research; hopefully, this reflexivity can increase credibility and give the reader a better understanding of the work.

The second strategy has been to give a *rich thick description* of the situation regarding quality assurance in the DF and FS fields in the Norwegian police. This description is provided in Chapter 4 Results and is deliberately separated from the discussion, to distinguish the informants' voices from mine and to enable discussion of the findings in Chapter 5 – Discussion.

This detailed description can contribute to the readers being able to draw their own conclusions, based on the presented data (42, 43, p.106).

## **External validity**

To check whether the results and conclusions of a qualitative study can be generalized to other contexts, three common strategies are often used.

The first is to see whether the study was conducted in a "*real-life setting*". Researchers often perform studies in laboratory environments, to have more control over the variables. However, this can be an artificial setting and may not be transferable to the real world.

The second is to check whether a representative sample is used; the third considers replication: whether the results and conclusions of the study can be replicated in a different context by another researcher (43, p.105).

This thesis is based on data collected from the "real world". The recruited informants were typical experienced DFEs and FTs from districts in different geographical regions of Norway. The sample may not be representative, and another researcher may come to different results. The conclusion of the thesis, however, can provide valuable findings, which can be further investigated in the future.

## **Reliability**

I think every piece of research will have factors, areas or dimensions that will not be adequately covered. In other terms, there will be weaknesses in all research. The main thing is to be aware of this and to try to address it as well as possible. Reliability is often related to the question of whether results can be replicated at a different/later time by other researchers. "*Will the interviewees respond differently to another researcher?*". "*Is it possible to get the exact same answers in two separate studies, with different settings?*" (41, p.276).

In a qualitative study, reliability is important, in both the interview and the transcription process. In the interviews, I have tried not to ask questions in a leading way but, instead, to focus on letting the interviewees answer the questions and tell their stories as they please, without interrupting or diverting them. I recorded the interviews to transcribe them in the best possible way, to be able to extract the essence for the coding and analysis process. To strengthen the quality, I sent the citations I have used to the informants for a validity check, to make sure that that I had not misunderstood anything in the translations.

# **4 RESULTS**

## **4.1 Introduction**

In this chapter, I will present the data gathered from the interviews in a categoric/theme-based way. I have found it relevant to present the findings from

DF and FS fields together under each theme, to more easily reveal possible differences and similarities. I will present possible differences and similarities in a subchapter at the end and will also point out potential differences regarding findings in small, medium or large police districts. The participants will be referred to as DFE, FT, interviewee or participant, to ensure anonymity.

In Chapter 6.7, I conclude on these main categories, based on the analysis of the texts:

- *Focus on quality after reform of the police*
- *Focus on quality after investigation reform*
- *Competence plans or planning*
- *Accreditations, certifications or standardizations*
- *Quality management – instructions/standards*
- *Quality assurance – what is done – is it adequate?*
- *Perceptions of the term 'quality'*
- *Summary of findings*

With this presentation of the categories/themes, I have tried to give an insight into how the situation is in three districts in the DF and FS fields, in relation to quality assurance and management, and how this is managed in the DFEs' and FTs' daily work. I have used a lot of citations from interviewees from the analysis, because I think it is important to emphasize their experiences and views as they expressed them.

I start each category with findings from the DF field; the citation blobs are coloured yellow when citing a DFE and green for a FT. The findings from the interviews are summarized in the last section, 4.9.

## **4.2 Focus on quality after the reform of the police**

As mentioned, the reform is also called a quality reform, and the new organization structure with the new districts was completed during 2018. Smaller units were basically merged into larger sections, intended to be more robust.

The new sections should have been operational for about two years, and it was important to get a picture of the current situation, compared to the situation prior to the reform: especially whether there was more focus on quality.

The majority of the participants explained that they had experienced standstill or fewer resources, in terms of people, after the reform, and that this could have an impact on quality.

## DF

Not all districts were merged with other districts in the reform, but the new structure, with new units and sections, was created. One of the participating districts was not merged with others.

*"I can't really blame the reform, because we have not been merged with any districts, but the management's decisions have resulted in reduced positions in our section."*

Another DFE working in a merged new district described their situation:

*"The reform has affected us in the way that we have got a lot more work, because of the new bigger district, but we have not got more resources in terms of people, DFEs."*

## FS

The situation seems to be much the same in the FS field, in terms of fewer people. An FT stated that they do the best they can in terms of assuring quality in the cases they handle, but they are not involved as much as before the reform because of the lack of resources.

*"The FS field has not really been prioritized in the reform. We were six FTs before, and now we are four. It is difficult to say something about quality without mentioning that we are fewer people now, because it does something to the quality, after all."*

Another FT commented that some things may have been a little better, that one should have more people, but the problem was the economic situation that led to the need to have open vacancies. A consequence of merging districts was that it also entailed merging different “working cultures”, which was a challenge as regards quality.

*“Working hours in cars related to driving to and from assignments steals about 1-2 positions in the new larger district. When you merge districts, several cultures must also merge into one, and that is also a challenge regarding quality.”*

### **4.3 Focus on quality after the investigation reform**

As described in Chapter 2.4, the strategic plan to raise competence in the field of investigation was introduced in 2016 (31). For most investigators, this resulted in having yearly training/education, for 20-25 hours, in different subjects related to investigations.

The DF and FS fields are special areas of investigations, and the aim of this study was to find out whether the focus on quality had increased, in their opinion, with this new measure. Most participants said that the yearly training was a good initiative, but the themes were best suited to the general investigator and not special investigators like DFEs and FTs.

#### **DF**

One DFE said that the training was very positive because it had set a focus on the rule of law, in terms of documenting sources and verification.

*“If you think about the yearly education, this has set a focus on the rule of law, and this has inspired me. We have followed the chief investigator training, and it has conveyed a lot of knowledge, and has been challenging on technical issues regarding sources and verification.”*

Another DFE stated that it was too focused on themes intended for the general investigator:

*"It is focused on increasing investigators' competence in general, but not focused on increasing the competence of a DFE. The training involves more on analysing interrogations and so on, and some of this can be useful in cases where we have done work, but much of the content does not 'meet' us, and we could be better off using this time on internal 'knowledge sharing'."*

## **FS**

All the FTs had news regarding their yearly training, as they will be getting a customized arrangement this year. The new special yearly training is a cooperation between NCIS and NPUC and involves 22-25 hours with subjects in FS.

*"The yearly training in the FS field is evolving, because the one we follow now does not suit us; we feel it is something the district has to check, to ensure that we are making certain progress – and it is never a waste of time to cooperate with others – but now we will get our own yearly education within FS this spring."*

None of the DFEs mentioned or seemed to have knowledge about an upcoming similar alternative yearly training for the DF field.

## **4.4 Competence plans or planning**

In general, updating one's competence is a necessity. The rapid development of technology, methodology and variety of particularly challenging tasks in both DF and FS, do need plans for enhancing competence. I asked the participants about their knowledge regarding established competence plans in their districts.

All participants agreed that it is important to have plans for enhancing competence, and that these plans involved a commitment to implement and conduct training and studies at evenly intervals.

## **DF**

A DFE had heard about competence plans in the district, but not been involved in planning or otherwise informed.



*"No, there is a lot spoken about competence plans, but I have not seen them, and not lived by them, but when we announce for new DFEs we demand that they have a minimum education of NCFI Core Concepts."*

They have not had any training courses in the computer forensics tools they use.

*"It is challenging that we do not have training in the tools we use, I have called for it for 9 years now, but it costs a lot and they have not prioritized to spend money on this".*

Another DFE helped the management creating a competence plan for DF but was afraid that this only was to have a paper on the subject, and not to follow and conduct the plan.

*"My superior had to create competence plans, and I contributed creating this one year ago. I have not heard anything since. It has probably been put in a drawer because there has not been any follow-up on this. They probably needed a paper on that this was done. We are also so pressed/pushed and run from side to side, it is hard to maintain our competence, so it is a struggle".*

Several DFEs complained on the lack of competence of the management and about the perceptions some leaders have on the need for education, competence and training in DF.

*"There is an understanding that the tools we have are so easy to use, everyone can use them, and the most frightening thing about it is that some of the contributors to this perception is some people in NPD, and NCIS. Unfortunately, we see, that managers who say things about the DF field, have no competence, and to say it bit silly, some of our managers have an opinion that if you can handle Microsoft Word, you are good in data handling and can help the Section for Digital Policing (SDP)".*

In another district the DFEs can set themselves up on "wish lists" for training courses, but few can attend because there has been a lack of funding for many years.

*"There has not been enough funding to take certifications and training courses in the last years. It is bit of a shame really because it affects the rule of law, related to that we not are trained in using the tools we have. It seems like it is a thing or understanding that we can learn to use the tools by our own, and to get the best out of it. I often think of comparing us DFEs with the operatives who are obligated to attend yearly training and approve tests in shooting, pepper spray handling, emergency response driving, but a DFE can get a toolbox of computer programs, and can have to stand in court and either acquit or convict in a case.*

*I feel that we should, the police should have stronger requirements to a DFE, to strengthen the rule of law".*

## **FS**

The situation in FS is a bit different in this area. They have a quality standard (5) that if followed, should cover their need for competence updates. The FT's said they could attend the courses and studies they needed to enhance their competence, and 2 of the 3 participants had competence or education plans.

*"We do not have a competence plan, but we do have an education plan. There are different directions to choose in studies, and I have been contributing to developing the studies at NPUC. We have a plan for separating a specialist from an FT, and, for example, you should not interpret blood-trails if you have not done studies in this or else are competent in doing so."*

#### **4.5 Accreditations, certifications and standardizations**

I wanted to find out whether requirements had been created/formed when it comes to standards in tools, mandatory certifications, accredited methods or laboratories in DF and FS.

In FS, as mentioned, NCIS has national responsibility for fingerprint analysis, ballistics etc., and has accredited methods and laboratories for this.

I wanted to investigate what was done locally about this.

#### **DF**

One DFE's response sums up most of the answers from all the DFEs:

*"There is no ISO-standard level here, but we use standard methods for acquiring data. When it comes to COC, we partly follow the trail, but, in cases where the material is seized by others, we cannot have control over what is done with it. We believe they do not tamper with it and handle it properly. We then follow the COC and document what we do."*

#### **FS**

All the FTs explained that there is work going on to accredit/standardize crime scene work, and, currently, that it is only the national FS unit at NCIS that has accredited laboratories and methods in Norway; the quality standard (5) from 2012 is still the leading guideline for the FS field.

## 4.6 Quality management – instructions/standards

Quality management (QM) is a responsibility the management should have. In this position, the leader is responsible for establishing quality assurance measures that ensure that solid and reliable work is delivered.

The participants were asked about the status of QM in their fields and the management's focus and involvement in this, and if there were established instructions or measures regarding quality assurance.

### DF

One of the DFEs especially had a lot to say about the current situation in the district, about the absence of management, and the lack of attention from the leaders.

*"The management should have responsibility to assure quality in this work. I have never experienced a field in the police which gets so little attention. There are not set requirements or any questions asked, and there are no follow-ups. I believe it is because the leaders have not attended this school. They have attended the analogue school and are familiar with investigations but do not know anything about this and dare not touch this field. Our district has also had revisions by NPD, but they never touch us, our way of storing/handling evidence, or routines."*

And, further, about the management's involvement:

*"The management never ask me anything. I ask about directions and visions, if we should be measured or guided in some ways. There is no response and they are totally absent. I am talking about the section leaders and above. My section leader has been in my office three times, and only in connection with problems with a personal mobile phone, or one time regarding a personal document that would not open. Beyond that, totally absent."*

The other DFEs had similar descriptions about the situation in their districts, with lack of leadership, support, involvement and focus on DF from the management.

## FS

As mentioned, the FS field has its national quality standard (5), and, if it is followed, there is an implicit responsibility for the top-level management in each police district to have local quality assurance instructions.

The FTs said the quality standard was followed. One district had also created local instructions with measures assuring quality, in addition to following the quality standard as much as possible.

*"Yes, we have local instructions with quality assurance measures, but they are a bit outdated in relation to the reform. We are currently waiting for a new forthcoming update on the national standard. We follow the current national standard as much as possible in the new organization. Our former leader took some decisions and did not see a need for updating the local instructions, and that is the main reason that the instructions have not been updated."*

### 4.7 Quality assurance – what is done – is it adequate?

Some of the quality assurance measures have already been discussed in the above themes, especially regarding who should be responsible for managing quality assurance, but, in this subchapter, the focus is on what measures/controls, if there are any, are carried out, and whether the participants believe they are adequate.

One DFE told about the lack of quality controls and that they had to take the initiative themselves to carry out controls.

*"No, there is no control of the work being done. It is really up to the person who conducts the data-technical work, whether some control of the examination process is done. We fellow DFEs have discussed whether there could be a possibility to use some of the yearly investigator training hours to look at each other's cases and reports, to get inputs, learn from each other and guide each other."*

It is, as revealed earlier, hard to carry out quality assurance without support, resources and understanding from the management.

*"The management has no understanding of how demanding this is, in terms of the necessary competence, and no understanding of how much work and how many resources one needs."*

Because of the lack of quality assurance measures, this DFE had, on his own initiative, started an evaluation project in their SDP section, where they evaluate their work and reports in selected cases – the whole DF process, all the way to the court proceedings.

*"We have started a piece of work, a regime, an evaluation document, where we evaluate data-technical reports before they are submitted. The whole case process is another evaluation, but this is specifically on the reports, and the DFEs get feedback on given parameters. The parameters are wide in range, to apply to all types of criminal cases. We evaluate the whole process, which ends with me following the case in court, to watch whether the court understands what is presented, and I also read the judgement papers afterwards."*

## **FS**

Dual-investigator is a quality control measure, because there are more eyes on the work, and they can control each other, but, as previously mentioned, there is a lack of people in SFS sections since the reform.

*"We read each other's reports and try to work in pairs on the serious cases, but often we have to split up, and then we have to ensure the quality ourselves. The control on reports is mostly done on definitions used and orthography, and we do not in general both sign the reports if the case is not a severe offence."*

The FT stated that they had proper control measures in FS in their district.

*"I do not know, but I feel we have good control over what we are doing here, and we use external specialists if needed, experts, relatively often. We are very certain of this, that there are many things we do not have knowledge about, and then we can call on others for advice."*

The other participants from FS said they had control measures in accordance with the forensic science process described in the quality standard (5), which means quality control of the seized objects and the samples from the crime scenes and control of the reports before they are submitted. The new position has also been established, as described in Chapters 2.5 and 2.7, the FTC, assuring quality of the FS work in investigations.

*"In severe crime cases, we use the Forensic Technician Coordinator (FTC), and, in those cases, both the FT and the FTC sign the reports before they are submitted. We have not such good routines in less severe cases. I believe that we do have the potential to do this in these cases too."*

The FTs in this district also try to work in pairs in all cases and follow the quality standard, having the reports controlled by a third party.

*"We have tried to work in pairs on all cases and have had a section leader who has conducted the quality control of the reports. This has not always been feasible, but the report has always been controlled by a third party. I think our control measures are good enough today, but it presupposes that everyone follows the quality standard. To formalize even more, we could adopt the model on NCIS, where the person who conducts the control also signs the report."*

## 4.8 Perceptions on the term quality

'Quality' is a term that can have different meanings for different people.

The final question to all the participants was what quality meant to them, in relation to their work. Some DFEs know about their colleagues in FS, who often work in pairs, and have experienced this themselves with a positive outcome, in some cases.

*"I wish we could work in pairs in the cases, so we could spar with each other all the way, and I would also like to have training courses in the tools we use, so we do not only do the same in every case and just push buttons and do not really know what we are doing. I would also like to have the possibility to dig deeper in the examinations, without having to prioritize a new case that comes tumbling in. It is a question of resources really, having the fundamental competence and more people."*

Another DFE said this about quality related to work:

*"Quality is when you have conducted a thorough examination in the case and have illustrated it in the right way. When you have performed a good piece of work."*

### FS

An FT mentioned the importance of getting assistance from other experts in their field, like experts in NCIS, in areas they do not have expertise in locally.

*"That the examination/work is thorough, that one is as certain as possible not to have missed anything, at the same time having documented the same in reports and illustrations, and in large cases have included drawings and maps. To be certain that you have delivered work, good enough, together with others, like NCIS, and to "call a friend" if we are unsure on something."*



Some thought it was difficult to translate the term 'quality' into Norwegian.

*"Difficult word, and not so easy to "Norsify", but, when we deliver something with good quality, it should be done in a proper and understandable way, and the methods and systems used should be anchored and approved."*

## 4.9 Summary

There are significant differences in how the FS field has established routines for quality controls, not only on paper but conducted in real life, compared to DF, where there seems to be an obvious lack of QM, and few or no quality controls are conducted.

The FTs do not work in pairs all the time, and they have challenges with the lack of resources in terms of people, especially since the reform. The work-pairs read each other's reports and follow the national quality standard as far as possible. Some have local instructions in accordance with the quality standard.

The DFEs must control their own work, in terms of dual-tool verification of findings, and, if possible, get a colleague to read their reports, but not systematically.

They lack resources, a demand for competence, and understanding from the management; they are also worried about the effect the lack of quality assurance measures can have on the rule of law.

The reform seems to have had a negative impact on both fields, regarding resources. Nearly all the interviewees said there are fewer DFEs and FTs in the sections since the reform, mostly because of the poor economy in the new districts.

As regards whether there were differences between the small, medium and large districts, I found that there were some, even though the participants described situations with many similarities. For merged districts – here, the small and the large – there are new challenges related to merging cultures and travelling distances at work.

There are also differences in how they are organized. In the small-sized district, the DFEs and FTs are placed together in a section for specialists, and they do not have a leader with background knowledge in FS or DF. All these factors can influence the quality of the work and will be discussed in the next chapter.

## 5 DISCUSSION

### 5.1 Introduction

In this chapter, I will discuss the findings related to the theory and try to answer the research problem and the research questions. I will discuss findings from the analysis in relation to the theoretical perspectives. My research problem is:

*Quality assurance in Digital Forensics in the Norwegian police, is it adequate?*

And the sub-questions are:

- *Can Digital Forensics learn something from Forensic Science in terms of quality assurance of their work?*
- *Has the reform contributed to an enhanced focus on quality in Digital Forensics and Forensic Science?*

The discussion starts with the last sub-question: whether the focus on quality has improved since the reform.

### 5.2 Has the reform contributed to an enhanced focus on quality in DF and FS?

One of the main goals of the reform was to strengthen the professional milieu, by merging the smaller groups and units from the old districts into larger sections (1).

*Glomseth* has recently published a research report in which he interviewed top-level managers about different aspects of leadership in the Norwegian police. In the report, the leaders said the reform had led to an extensive professionalism in the police and pointed especially to a generally increased competence in the organization as a reason for this. The managers also said the quality of the police work had increased remarkably in important disciplines (47).

The response of the participants from DF and FS to the question about increased focus on quality after the reform (1) (Chapter 4.2) was that they had experienced a standstill or loss of resources, a worsening economic situation, with larger areas of responsibility, and the same or heavier workload. All these factors could have an impact on the quality.

The reform has devoted significant attention to increasing the quality in investigations, through the project *Etterforskningsløftet* (31). The interviewees connected this project mostly to the new yearly training, with themes in the area of investigation. However, most of the participants felt that the subjects were too general and not suited to their need as specialists, although some stated that it was useful to be updated on new subjects and themes, especially themes about quality and strengthening of the rule of law. For the FS, plans have been introduced this year for new training, adapted to their specialized subjects. This research has not revealed plans for a similar specialized training in DF.

The reform has been evaluated every year since the start of the implementation, by the *Direktoratet for forvaltning og økonomistyring (DFØ)*, and the last report was published this spring, evaluating last year: *Følgerevaluering av nærpolitireformen – statusrapport for 2019*. They had several critical comments regarding the implementation of the reform (48).

The first comment in the report was one from the report for 2018, where the main message was that, *"Too many things were initiated at once, and ambitions should be considered in the light of available resources, tasks and requirements of the police"* (48, p.1).

Another comment was to prioritize and increase the resources to combat digitally based criminality, and also that the Norwegian police is the least digitalized of the governmental services. *"The police face tremendous challenges, both in competence and technologically. Digital crimes occur in all types of cases"* (48, p.60). The DFØ concludes that the competence and required resources in this area must be more prioritized in future discussions.

The results in this study revealed similar experiences to those drawn in the report from the DFØ and the negative impact this had on the quality of the forensic work and the concern for the effect this could have on the rule of law (Chapter 4.2).

Management and leadership were recurring themes, especially with the interviewees from DF, and it became important to focus on this in this study. They experienced a lack of involvement from the management. The leaders seemed to have insufficient digital competence and knowledge about the challenges in the discipline. Sunde pointed to possible sources of errors in investigations, such as organizational challenges and insufficient competence (19). Competence in DF/digital evidence should not be mandatory *only* for those working within the discipline but also for the management and the whole justice chain, to prevent errors in investigations. Erlandsen also found possible sources of error in his thesis, where police lawyers without training/education in DE could weigh the value of digital evidence insufficiently or wrongly (18).

The participant FTs experienced more involvement and understanding from the management, and there are some possible explanations for this. FS is a much older discipline and has grown and developed in the police, establishing sufficient education, routines and workflows over time. FS has been a mandatory subject at the basic police education at NPUC for decades. DF has been a subject in the basic education for less than a decade. This means that police officers, and also leaders, are educated in FS, but only the newly examined officers have basic education and knowledge in DF. These factors indicate that most police managers have more knowledge in FS.

The NPD should have been aware of the need for digital competence in the police, since this had already been stated in 2011 in the report from the working group initiated by the NPD itself (36). One of the conclusions in the report about this was *"Expertise on how digital evidence can be investigated, what goes on in ICT-crime and what opportunities the police have on the Internet are important in all aspects of the police"* (36, p.27).

And, especially referring to the leaders, "*Leaders who take decisions on priorities, staffing and organization will have good use for this knowledge*" (36, p 27). Erlandsen has also commented on this in his study, as well as the lack of implementation of measures to enhance competence in digital evidence for the police in general (18).

As referred to in Chapter 2.6, circular 2010/007 from the NPD, on how to handle seized material in the police (37), is the only document that describes how DE should be handled, and by whom, with abstract terms like "special competence" and "adequate training", and it is not specified further in the document or elsewhere.

In 2019, the NPD published updated role descriptions, with specific competency requirements (33, Chapter 2.5). For a DFE, the NCFI Core Concepts at NPUC is required. An interviewee stated this was too basic for a DFE and more suited to an investigator intended to examine DE, but not to validate possible DE, like a DFE does. The study was developed as a basic study intended for the Digital Forensic Liaisons (DFL), the liaisons between DFEs and tactical investigators, so it is understandable that the DFE indicated that it is insufficient as a basis for their profession.

Based on my personal expertise and experience, I think the entry level qualifications for a DFE should be at least at NCFI level 2 or similar, which is also the opinion of the staff providing DF education at NPUC (33, 49). The reform focused on education, and, if sufficient requirements had been set for the special disciplines, this would probably have raised the quality.

Low, insufficient requirements in competence could be a pretext for a management ignorant of digital challenges and could lead to a decrease in quality, instead of improvement.

One of the DFEs compared the lack of requirements and training in DF with the operatives in the Norwegian police, who have obligatory tests in shooting and one week of practical exercises on different relevant scenarios every year. The absence of requirements and tests in DF could have a negative impact on the quality and the rule of law.

This shows that distinct and clear requirements for competence and testing are functioning for the operatives, and the management would surely pay attention to the consequences of failure to pass shooting tests or emergency driving tests.

As regards DF in Norway, control measures to assure quality are not particularly debated or mentioned in the reform or in publications prior to the reform (1, 36, 39). The prime focus for raising the level of quality seems to be on preventive measures, like competence, methods and equipment. In their studies, Erlandsen, Borhaug, Heitmann and Sunde have all referred to the importance of control measures like peer reviews to mitigate errors in investigations, in addition to preventive measures (15,17, 18, 19).

To summarize, within the police management, there seems to be a strong and one-sided focus on competence and in favour of paying attention to other quality measures.

This may be explained, first by an overestimation of knowledge as a safeguard for high quality and, second, by a lack of knowledge about possible errors that may occur in police work and how to effectively mitigate them.

In the next section, the main research question will be discussed, together with the background of the theory, in light of the results from Chapter 4.

### **5.3 Quality assurance in DF in the Norwegian police, is it adequate?**

To discuss the findings from the interviews in relation to the theory in an orderly way, I have separated them under the headlines, Preventive measures and Control measures. The results from DF and FS are compared and debated.

#### **Preventive measures**

In Chapter 2.2, there is mention of numerous preventive measures that could be implemented to prevent investigative errors in DF. Some of these measures were competence, accredited laboratories and methods, standards in tools, templates and guidelines.

The DFEs in the study had all attended the NCFI levels 1 and 2 at the NPUC. These courses were based on open source tools and not on the main tools in their daily work. It is important to also learn to use open source tools, especially to understand the bits-and-bytes raw basics without a graphical “push-button” interface. On the other hand, in a modern investigation, processing large volumes of data, the open source tools often lack capability and also the ability to present data in such a way that the investigators can easily investigate the content. It is important to understand the separate workflows that the DFEs and the tactical investigators have in investigations in the Norwegian police. This is the procedure in the vast majority of types of ICT-related crime cases, but not all.

The DFEs have responsibility for the technical side of the investigation, where they acquire and process/examine and present the data for the investigators, who analyse the data, bookmarking possible digital evidence for their cases. The investigators write reports on their content-analysis of the data, and the reports are meant to be examined by DFEs before they are submitted. The DFEs write technical reports based on the content analysis, documenting the technical aspects of the possible digital evidence, bookmarked by the investigators. A DFE in this study had experienced investigative errors in the district related to investigators who had conducted content analysis, written reports without control and validation from a DFE, and reached the wrong conclusions. The DFE had averted these investigative errors before they led to further proceedings.

This shows that DFEs need training in the tools they use daily, but it is also of the *utmost importance* that the investigators who investigate the data content are skilled in using the same tools. The investigators often get practice in using these tools together with the DFEs, but they also need training. More and more of the tools used in DF have *investigator modules* for tactical investigators.

The cooperation between the DFEs and the investigators is crucial, to achieve the best results. It is the tactical case responsible investigators who have the depth of knowledge about what possible evidence is important in their investigations, and, in cooperation with the DFEs, they will be able to take advantage of the full potential of digital evidence. In the results in her thesis, Sunde has revealed the importance of the cooperation between the DFE and the investigators, in addition to clear leadership and adequate resources (19).

In the Section for Digital Policing (SDP) in Oslo police district, they have developed a work method in cases involving Child Sexual Abuse Material, in which it is incorporated that DFEs are directly taking part in the investigations, together with the case management, police lawyers and tactical investigators. Communication lines are direct, with no delaying intermediaries, solving possible problems and misunderstandings, saving time and assuring efficiency. DFEs and tactical investigators validate digital evidence findings together, which the authors of a case study on this new working method explain as valuable for conducting the digital investigation in an effective and more forensically sound way (50).

Oslo police district has the largest SDP in the Norwegian police and has established and organized Digital Forensic Liaisons (DFL) in specialized groups in every police station, ensuring that there is competence in DF spread out over the whole district. The management in Oslo seems to have understood the importance of digital evidence and DF in criminal investigations and has invested a lot of resources in the discipline in recent years.

In 2018, Oslo police district delivered a report, which was a pilot project, measure no. 8, given by the Justice Department as a part of their strategy to fight ICT-crime (39). In this report, the Oslo police recommend "how the police can develop their tasks in a wide range when it comes to investigating and preventing ICT-crime that does not fall under a national cybercrime center"; one of the recommendations was to establish a net of DFLs in the districts, as they have done (51). In Oslo, this has been a success, and they have educated the DFLs internally with resources from the SDP.

*Trond Austad*, Assistant Chief of Police and Head of the SDP in Oslo police district and leader of the pilot project, contacted on July 2nd, delivered the report to the NPD in 2018. The NPD implemented the project in the reform. Austad explained:

*The only measure that has not been followed up in any form is the unified organization of the unit that has the SDP's functional responsibilities in the districts, and there is an inequality in how the districts organize investigations and data crime prevention.*

The organizational differences of the SDPs, as Austad refers to, have been described by the participants in this study. Only one of the participant districts was organized in a unit that solely has responsibility for DF and investigating ICT-crime cases. The other districts are organized together with FS or other special disciplines. This can be unfortunate, especially in relation to leaders of the units, who seldom have prime knowledge in two or more subjects, which again affects the specialists who rely on the managements knowledge and understanding in their disciplines.

The interviewees from DF in this study did not have the same experience with the implementation of DFLs as in Oslo. The participating districts have appointed DFLs, but they have received limited training and guidance. Some of them have attended the NCFI Core Concepts study but have had little practice. According to the role descriptions referred to in Chapter 5.2, there are no qualification requirements for DFLs; in fact, the role is not mentioned in the updated role description-publication from the NPD (33). The DF staff at NPUC found it odd that a role that was defined in the reform documents and implemented in practice in the districts was not described at all in the new role-description publication (1, 32, 33, 49).

Challenges related to the geographical aspects that the districts in this study face probably make it more difficult to maintain communication and cooperation between DFEs and DFLs, compared to Oslo, where the police stations are situated in the city. As referred to earlier in this chapter, it is very important that DFLs' work is guided and also controlled by DFEs.

The DFEs in this study experienced that funding was too limited to attend training in the tools, and they mostly did "learning by doing" and had concerns for the impact this could have on the rule of law. The forensic tools used in DF are often comprehensive, to cover the complexity and various parts of modern digital evidence. Cloud, mobile extractions, network and Internet, files systems in different operating systems – these are often all covered by the same tools. This requires base knowledge, as described, in open source tools, but also training in using the commercial tools.

Other preventive measures, such as COC, require full control over the digital evidence from when it is seized to when it is presented in court. There seemed to be awareness of the principle by the participating DFEs, but the study shows that evidence is not always handled in compliance with it. The DFEs followed the principle in their handling of the digital evidence, but, when others seized it and handed it to the DFEs, they could not document the handling prior to the handover.

None of the participants from DF included in this study had accredited laboratories or methods in their districts in accordance with ISO standards. As referred to in Chapter 2.2, Sommer asked the question whether it would be better to create and implement good practice guides instead, because DF does not fit into today's standards (14). In the advanced DF laboratory at NC3, they share Sommer's opinions on this matter and have instead created a system of documentation with checklists and fault registrations. A possible alternative solution could involve seeking accreditation for the workflow process, including checklists, documentation and nonconformity systems, as senior engineer, Kjell Harald Andersen, explained as they worked at the advanced DF laboratory at NC3.

Related to digital evidence in the cloud, many DFEs experience a struggle related to acquiring data from *Internet Service Providers* and personal cloud accounts. These types of data, and how and where they are stored, protected and available, change on a daily basis.

To accredit methods for the acquisition of these data would be almost impossible because of the constant shift in procedures one has to endure to obtain the data.

The participants from FS in this study are guided by the document, *Kvalitetsstandard for kriminalteknisk etterforskning* (5), when it comes to assuring quality and also in relation to preventive measures. It sets out requirements for the districts to have established measures, such as competence-plans, specially customized localities and methodology in the local FS sections. In this study, not all participant districts from FS had created competence plans, even though their experience was that they were permitted to attend the studies and courses they wanted, approved by the management. The FTs had attended studies at levels 1, 2, 3 and 4. Methodology in FS in the districts incorporates a lot of collaboration with the national FS section at NCIS, and they send seized material for analysis at their accredited national laboratories. They also send material for examination to external experts in DNA analysis, electricity, etc.

Compared to FTs in this study, DFEs seem to have fewer opportunities to achieve the required competence in their discipline. It is assumed that DF demands for competence differ from those of FS in this regard because digital evidence is fast shifting compared to physical evidence. This is a constant challenge for DF professionals. The DFEs' explanations about their situations in the study seem to expose an absent leadership, abandoning the individuals themselves to assure quality, without guidance or influence on important issues like training, education and workflow.

## **Control measures**

Control measures, as explained in Chapter 2.2, are those related to control activities undertaken during the handling of the digital evidence and the assessment of the results. The measures listed were dual-tool verification, peer review and the dual-investigator work form. The main purpose of these controls is to have someone *other than the examining FT or DFE* performing quality controls during and after the examination processes, to prevent investigative errors. The DFEs in this study explained that they had to initiate quality controls themselves, and they occasionally conducted dual-tool verification and peer reviews, such as reading each other's reports. They all stated that this was insufficient. Reading each other's reports is often no more than a grammar check or a check of whether content is understandable. The results in this study have not revealed any guidelines or checklists available to support this measure in either DF or FS.

The demand for quality in investigations has been a top priority for many years in the yearly *Circular for priority (Prioriteringsskrivet)* from the Norwegian Director of Public Prosecutions (NDPP), and, in addition in *Kvalitetsrundskrivet*, the need for quality in investigations was concretized (6). This demand for quality seems not to have got a foothold with the management in the participating districts in this study but is, instead, being treated as a responsibility for the individual investigator.

One DFE in this study has initiated a quality evaluation project for reports in their district, where they conduct controls on the data-technical work in cases to which



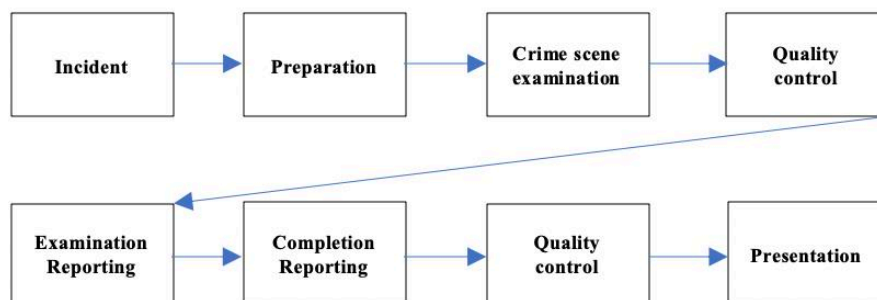
DFEs have contributed. The controls are conducted by a DFE other than the one who has done the work, from whence the report is delivered to the witness appearance in court. The DFE added this measure, on his own initiative, to increase quality in their forensic investigations, which illustrates the lack of involvement the management shows in QM in DF.

FTs work in dual-investigator pairs – although not in all cases, due to the lack of resources, especially since the reform – and follow the workflow process in the quality standard document to the extent that it is possible. I presented the process in my preliminary report and in this thesis in Chapter 2.7, Figure 2.2. To explain the process thoroughly, it is important to show it again (3, 5).

There is a detailed description of the process, explaining each step and, unlike the DF process, with quality control steps, in a document attached to the quality standard document, called *Detaljert prosessbeskrivelse (kvalitetsstandard kriminalteknikk)* (52). The process has many “sub-steps”, not all of which are relevant for describing the quality controls that are a part of the process. Below is a short description of the eight main steps in the process:

- **Preparations**, packing necessary equipment and planning for the specific forensic investigation.
- The **crime scene examination** is conducted with an evaluation when completed – of the seized material and samples
- In the forensic laboratory / at the police station, **quality control** is conducted by an equally proficient pair of eyes on the seized material and objects, before additional examinations are done locally or the material is sent to external partners, like NCIS

Fig. 2.2 Forensic Science Workflow Process



- **Examination** of the seized evidence. If examination by other experts at NCIS or external laboratory cooperators is needed, the evidence is sent with a request. Reports from the crime scene and on what is seized are created.

- **Report** continuation. After examinations are finished internally and externally, the investigator on the case is conferred with and the report written, with a conclusion.
- **Quality control** on the documentation, examination and reports by an equal peer or someone with a higher level of expertise.
- Preparing for court, eventual **presentation** in court, and possible after-work, evaluation.

The results in Chapter 4 showed that the FTs followed the quality standard to an extent. None of the districts included in the study had created updated local instructions as instructed in the document, but they said they followed the quality standard. As regards conducting quality controls as implemented in the workflow process, the results indicated that they did not conduct the controls in every case/assignment, due to lack of resources.

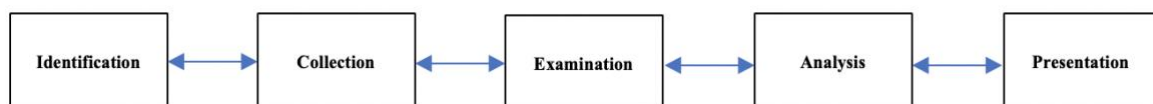
The quality controls were mainly evidence control after crime scene examinations and following peer reviews in the form of report-reading by a colleague, superior or FTC.

The process is a guide for FS but seems not to be complied with fully in the participating districts. There are no detailed specifications on the quality controls that should be conducted and by whom, only keywords on what they could be.

## The FS workflow process compared to the DF process

I have referred to Flaglien’s DF process in this study. The reasons for this are firstly that, to my knowledge, no version of the process has been developed or adopted in the Norwegian police. Secondly, Flaglien’s version is thoroughly documented, all the way from the planning and preparation stage to the final presentation stage. Thirdly, in INTERPOL’s new guideline from 2019, referred to in Chapter 2.2, the process is described with the same five stages as in Flaglien’s chapter in the book, *Digital Forensics* (21, p.16).

Figure 2.1 The Digital Forensic Process (modified by me)



Compared to the Norwegian FS process, the DF process lacks defined quality control steps and does not involve quality control by others. Going through the description of the phases in Flaglien’s chapter in the book, there are allegedly no

quality controls by others than the examiner, such as documenting evidence integrity and COC.

As referred to in Chapter 2.2, Page et al. suggest learning from the FS field, where there are established QM systems for quality assurance. Below is shown peer review in five levels for establishing quality controls, as mentioned in Chapter 2.2 (3, 24):

1. Proof check – check language for spelling and grammatical faults
2. Sense review – check whether the presentation of findings makes sense as evidence
3. Conceptual peer review – review of documentation of findings, descriptions of artefacts, if COC is actually documented
4. Verification review – validation/examination of findings on datasets, but not on all acquired data
5. Re-examination – a total new examination by another expert – enables the results of the DFE and those of the reviewer to be compared – reduces possible cognitive biases – but requires resources in time and personnel

How can these five levels of peer review be integrated in a QM system in DF? Sunde has suggested an implementation of these levels of quality controls in DF:

*Proof check, sense review and conceptual peer review* should be done by an equal peer or higher, on every report.

It is suggested that the more resource-challenging *verification review* and *re-examination* are conducted on a regular basis, to reveal possible errors in the examinations and to identify possible learning points to ensure development (25, p.23-24).

However, it is important to be aware that implementing such quality controls is not synonymous with an error-free investigation. The human-error factor is a constant vulnerability in investigating crimes, and there are, for example, several cognitive biases that can influence the human mind that are possible sources of error to be aware of in investigations (53).

### **Can DF learn something from FS, in terms of quality assurance of their work?**

Based on the findings in this study, DF can learn from FS about quality assurance in these areas:

- First and foremost, a quality standard for DF should be developed

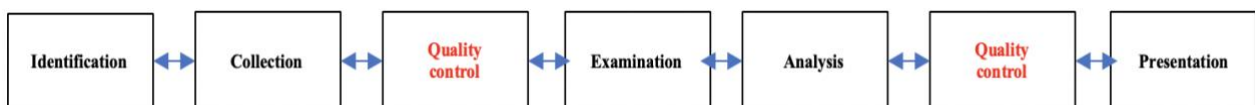
- DFEs would benefit from working in pairs. This way of working would reduce the risk of human errors because more eyes, knowledge and more responsibility are involved
- DF would also benefit from establishing a coordinator and quality assurance role, similar to that of the FTC. According to the interviewees from FS, this position has been a success in investigations regarding clarifying the forensic aspects for the tactical investigators and their leaders, in addition to being a controller for the work delivered by the FTs

In addition to this, as referred to in Chapter 2, the national FS unit at NCIS has several sections with laboratory functions in different areas. According to Police Superintendent *Morten Olsen Sandnes* at the national FS unit, contacted on May 20, 2020, they have appointed quality contacts at every laboratory/section, with responsibilities for assuring and controlling quality in their fields of study. In addition to this, the unit has a position in which a specialist's full-time function is to safeguard and assure quality for the whole unit.

Implementing similar quality assurance measures to those of the national FS unit in the Norwegian police, for the field of DF, will be important. This would raise the quality and reduce the risk of errors in the forensic investigation of digital evidence, even though it would require resources.

A modified DF process with steps of quality controls by others could be presented as Figure 5.1, taken from my preliminary report (3) but enhanced with the arrows pointing both ways, as in Figure 2.2, since I still think it is iterative, with the quality controls.

Fig 5.1 – DF Process (modified, with quality control steps)



Page et al's levels of peer reviews 1-3 (24), should, in my opinion, be conducted in every case, as Sunde suggests (25, p.23-24). As referred to earlier in this chapter, one participating DFE had developed a quality evaluation project for conducting detailed controls on each other's reports before they were submitted. The project seems to cover levels 1-3, which are quality controls on written reports. These controls are essentially conducted after the analysis phase, when the examiner is finished with the examination of the digital evidence.

Reports *can* be written at other phases of the process, often in connection with the collection and examination of the data, documenting the acquisition and verification processes.

Therefore, it would be feasible to have another peer review of the acquisition reports, as well as a control/validation of the acquired and examined data before the analysis phase.

*A figurative example:* An examiner has finished a draft of the report. The report is evaluated/controlled in cooperation with an equal peer, and a deficiency in the presentation of the digital evidence is unveiled. The measures that must be taken to complete the examination can include collection of new identified evidence or re-collection of collected evidence; re-examination and re-analysis of new, parts of or all the digital evidence; change of methods, etc. This depends on what is needed for the necessary documentation of the digital evidence in the investigation.

I believe quality controls can be conducted at all phases in the process. It is often a matter of getting a second opinion, and this can be crucial in several steps in the process, as well as which methods which will give the best and most reliable results of all handling of the digital evidence. Controls can also involve testing of methods and tools. These actions/controls should be done by, or in cooperation with, an equal or more experienced peer. Working in pairs could assure this, if the pairs are experienced. If not, a third-party senior should also be required to have a control function.

More resource-demanding peer reviews, such as levels 4-5 suggested by Page et al. (24), verification review and re-examination, are, based on my experience in DF, not feasible to conduct in every investigation. They should, however, be a part of a quality assurance regime and conducted at certain intervals.

In the introduction, I referred to an incident in Denmark in 2019, where errors in the Danish police's handling of Call Data Records resulted in new examinations/reopening of a large number of criminal cases. Without systems assuring quality, this could also occur in investigating digital evidence in DF.

Errors in investigations may lead to severe consequences for the involved parties. They can lead to miscarriages of justice, wrongful convictions of innocent people and the acquittal of guilty people. Measures and mechanisms aimed at reducing errors are highly important in every criminal investigation, and such quality measures may prevent errors before they affect the outcome of investigations (3).

## 6 SUMMARY AND FUTURE WORK

### 6.1 Summary

It is not within the scope of a qualitative study to come to conclusions that can be generalized. In this phenomenological research, by conveying the participants' experiences and, expressly, their answers to the questions, a focus is placed on the phenomenon, quality assurance, in Digital Forensics in the Norwegian police.

QM, along with addressing competence requirements, competence planning and standards in methods or tools, or instructions regarding quality assurance measures, seem not to have been prioritized in DF in the police districts represented in this study.

The management seems to have insufficient knowledge about the challenges within the DF discipline. The study suggests that the basic competence level for a DFE is insufficient to safeguard the quality of DF. It seems that DFEs do not get training in the tools they use because the district's economic situation is poor, and they are worried about the impact this can have on the rule of law.

There seems to be a culture in DF, not only in Norway but in the field as a whole, of excessive belief in competence and of overlooking the need for quality assurance with control measures.

Unlike DF in the Norwegian police, FS has a quality standard which sets out detailed requirements for how the FS work should be conducted, making the management responsible for establishing a QM system. The detailed work process in FS is an example of how to implement quality control measures in a standard, even if it seems not to be fully implemented in the districts in this study. The DF process referred to in this study has not implemented similar measures.

### 6.2 Future work

Based on this study, a national quality standard for DF appears to be an important step in ensuring that quality work is clearly rooted in the management. This would probably have contributed to a better structure for the implementation of quality assurance measures, as well as a standardized and equal approach to quality for the whole country.

A further scrutiny of the dual-investigator work form would be important, since all the participating FTs said they essentially worked in pairs, and this measure is not mentioned in the quality standard.

- What instructions do the pairs follow?
- What considerations are taken into account when it comes to conclusions?

- Is this way of working measured in relation to the time spent on a case assignment versus working alone?
- Is it possible to implement this in DF in Norway, with the available resources, without loss of capacity?

It would be valuable to examine further the report evaluation project that the DFE in the participating district in this study has established, to see whether it could be transferable to the whole DF discipline in the Norwegian police.

A preventive measure to investigate further is the possibility of accrediting workflows, procedures and guidelines in DF in Norway.

Countermeasures to prevent miscarriages of justice are crucial to maintain confidence in the police and the judicial system; if only one mistrial is prevented, it would be worth implementing all actions mentioned in this study.

## 7 BIBLIOGRAPHY

1. The Justice Department, (2015), "Nærpolitireformen", Det kongelige justis og beredskapdepartement, Oslo, URL: <https://www.regjeringen.no/no/tema/lov-og-rett/kriminalitet-og-politi/innsikt/narpolitireformen/id2398914/>, Accessed: July 19, 2020
2. Grut, S. (2019), "Over 10.000 rettssaker må gjennomgås etter teledata-skandale hos dansk politi», NRKBeta, URL: <https://nrkbeta.no/2019/08/23/over-10-000-rettssaker-ma-gjennomgas-etter-teledata-skandale-hos-dansk-politi/>, Accessed: June 21, 2020
3. Jahren, J .H, (2019), "Quality Assurance in Digital Forensics in The Norwegian Police, is It Good Enough?", NTNU I Gjøvik
4. Årnes, A. (2018), "Introduction", in: "Digital Forensics", Årnes, A. (editor), Wiley
5. National Police Directorate (2012), «Kvalitetsstandard for kriminalteknisk etterforskning», Oslo, Politidirektoratet, URL: <https://docplayer.me/5070229-Kvalitetsstandard-for-kriminalteknisk-etterforskning.html>, Accessed: May 7 2019
6. Norwegian Director of Public Prosecutions (2018), «Kvalitetsrundskrivet 03/2018», Riksadvokaten, Oslo, URL: <https://www.riksadvokaten.no/document/nytt-kvalitetsrundskriv/>, Accessed: July 19, 2020
7. Watson, D., Jones, A. (2013), "Digital Forensics Processing and Procedures, Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements", Syngress Media US
8. Årnes, A., (2019), "Introduction" p.1, in: "Cyber Investigation", Årnes, A., (editor), a draft for class use only, NTNU, Feb. 2019
9. Tilstone, W., Hastrup, M. L., & Hald, C. (2013). Fischer's Techniques of Crime Scene Investigation, CRC Press, Boca Raton
10. Pollitt, M., (2010), "A History of Digital Forensic"s. 6th IFIP WG 11.9 International Conference on Digital Forensics (DF), Hong Kong, China. pp.3-15, 10.1007/978-3-642-15506-2\_1. hal-01060606
11. UK Government (2020), Forensic Science Regulator Institution, URL: <https://www.gov.uk/government/organisations/forensic-science-regulator>, Accessed: May 30, 2020



12. UK Government (2020), " Forensic Science Providers: Codes of Practice and Conduct", URL: <https://www.gov.uk/government/publications/forensic-science-providers-codes-of-practice-and-conduct-2020>, Accessed: May 30, 2020
13. "The Netherlands Register of Court Experts (NRGD), (2016)", URL: <https://english.nrgd.nl/>, Accessed: June 2, 2020
14. Sommer, P. (2018,) "Accrediting Digital Forensics: What are the Choices?" URL: [https://www.researchgate.net/publication/324679791\\_Accrediting\\_digital\\_forensics\\_what\\_are\\_the\\_choices](https://www.researchgate.net/publication/324679791_Accrediting_digital_forensics_what_are_the_choices), Accessed: May 30, 2020
15. Borhaug, T. S. (2019), "The Paradox of Automation in Digital Forensics", NTNU i Gjøvik, URL: <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2617753>, Accessed: June 2, 2020
16. Netherlands Forensic Institute, (NFI), (2010), "Hansken", URL: <https://www.forensicinstitute.nl/products-and-services/forensic-products/hansken>, Accessed: July 19, 2020
17. Heitmann, O. (2019), "Digital Investigation: The Malnourished Child in the Norwegian Police Family?", NTNU i Gjøvik, URL: <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2617759>, Accessed: June 2, 2020
18. Erlandsen, T.E. (2019), "Fallacies when Evaluating Digital Evidence Among Prosecutors in the Norwegian Police Service", NTNU i Gjøvik, URL: <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2617771>, Accessed: June 2, 2020
19. Sunde, N. (2017), "Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation", NTNU i Gjøvik, URL: <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2450280>, Accessed: June 2, 2020
20. INTERPOL Global Guidelines for Digital Forensics Laboratories, (2019), INTERPOL, Lyon, URL: [https://www.interpol.int/content/download/13501/file/INTERPOL\\_DFL\\_GlobalGuidelinesDigitalForensicsLaboratory.pdf](https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf) , Accessed May 9, 2020
21. Flaglien, A (2018), "The Digital Forensic Process", p. 16, in: "Digital Forensics", Årnes, A (editor), Wiley

22. Dilijonaite, A, (2018), "Digital Forensic Readiness", chapter 4, in: "Digital Forensics", Årnes, A (editor), Wiley
23. Norwegian Accreditation (2020), «Norges nasjonale organ for teknisk akkreditering og god laboratoriepraksis», Lillestrøm, Norsk Akkreditering, URL: <https://www.akkreditert.no/akkrediterte-organisasjoner/akkrediteringsomfang/?AkkId=519>, Accessed: May 15, 2020
24. Page, H., Horsman, G., Sarna, A., Foster, J. (2018), "A review of quality procedures in the UK forensic sciences: What can the field of Digital Forensics learn? Helen, P., Science & Justice, URL:<https://www.sciencedirect.com/science/article/abs/pii/S1355030618302211?via%3Dihub>, Accessed: May 7, 2020
25. Sunde, N, (2019), "Cyber Investigation Process" p.23-24, in "Cyber Investigation", Årnes, A., (editor), a draft for class use only, NTNU, Feb. 2019
26. ACPO Association of Chief Police Officers of England, Wales and Northern Ireland, "Good Practice Guide for Digital Evidence", (2012), URL: [https://www.digital-detective.net/digital-forensics-documents/ACPO\\_Good\\_Practice\\_Guide\\_for\\_Digital\\_Evidence\\_v5.pdf](https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf), Accessed: May 10, 2020
27. Horsman, G. (2020), "ACPO Principles for Digital Evidence: Time for an Update?", School of Health & Life Sciences, Teesside University, Middlesbrough, North Yorkshire, United Kingdom, URL: <https://www.sciencedirect.com/science/article/pii/S2665910720300220#bib0005> , Accessed: May 10, 2020
28. National Police Chiefs Council, (NPCC), (2020), "Transforming forensics", URL: <https://www.npcc.police.uk/NPCCBusinessAreas/ReformandTransformation/Specialistcapabilitiesmain/SpecialistCapabilitiesProgrammeTransformingForensics.aspx>, Accessed: May 10, 2020, UK
29. The Justice Department, (2012), NOU 2012:14, «Rapport fra 22.julikommisjonen», Oslo, Det kongelige justis og beredskapsdepartement, URL: <https://www.regjeringen.no/no/dokumenter/nou-2012-14/id697260/>, Accessed: May 2 2020
30. The Justice Department, (2013), NOU 2013:9, «Ett politi – rustet til å møte fremtidens utfordringer Politianalysen», Oslo, Det kongelige justis og beredskapsdepartement URL:

<https://www.regjeringen.no/no/dokumenter/nou-2013-9/id730815/?ch=1>,  
Accessed: May 2 2020

31. National Police Directorate (2016), "Handlingsplan for løft av etterforskningsfeltet", Politidirektoratet, Oslo, URL: <https://www.politiet.no/globalassets/05-om-oss/03-strategier-og-planer/handlingsplan-for-loft-av-etterforskningsfeltet.pdf>, Accessed: July 19, 2020
32. National Police Directorate, (2016), «Rammer og retningslinjer for etablering av nye politidistrikter», Politidirektoratet, Oslo, URL: <https://docplayer.me/53387738-Rammer-og-retningslinjer-for-etablering-av-nye-politidistrikter.html> Accessed: July 19, 2020
33. National Police Directorate (2019) «Nasjonale rolledefinisjoner med kompetansekrav - etterforskningsfeltet», Politidirektoratet, Oslo
34. Norwegian Police University College (2019), Etter og videreutdanning i etterforskning og kriminalteknikk, Politihøgskolen, Oslo URL: <https://www.phs.no/studietilbud/etter--og-videreutdanning/utdanninger/etterforskning-og-kriminalteknikk/>, Accessed: May 5 2020
35. Norwegian University of Science and Technology (NTNU), (2019), "Erfaringsbasert master I informasjonssikkerhet, MISEB", NTNU, Gjøvik, URL: <https://www.ntnu.edu/studies/miseb> , Accessed: May 5 2020
36. National Police Directorate (2012), "Politiet I det digitale samfunn, en arbeidsgrupperapport om: Elektroniske spor, IKT-kriminalitet og politiarbeid på internett", Politidirektoratet, Oslo, URL: <https://medlem.ntl.no/Content/103500/cache=20122109105334/Politiet%20i%20det%20digitale%20samfunn%20juli%202012.pdf> Accessed: May 5 2020
37. National Police Directorate (2010), "Rundskriv 2010/007, Behandling av beslag I straffesaker", Politidirektoratet, Oslo, URL: <https://www.riksadvokaten.no/wp-content/uploads/2019/03/Behandling-av-beslag-i-straffesaker.pdf>, Accessed: May 5 2020
38. Norwegian Director of Public Prosecutions,(NDPP), (2019), Forvaltningsapparat-for-etterforskningsfeltet-Riksadvokatembetets-rolle-som-fagmyndighet.pdf, at <https://www.riksadvokaten.no/document/riksadvokaten-som-fagmyndighet/>, Accessed: May 12, 2020

39. The Justice department, (2015), «Justis -og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet», Det kongelige justis og beredskapsdepartement, Oslo, URL: <https://www.regjeringen.no/no/dokumenter/justis--og-beredskapsdepartementets-strategi-for-a-bekjempe-ikt-kriminalitet/id2413705/>, Accessed: July 19, 2020
40. Kripos (NCIS) (2020), "Kripos-hovedarbeidsområder", URL: <https://www.politiet.no/om/organisasjonen/sarorganene/kripos/kripos-hovedarbeidsomrader/>, Accessed: May 12, 2020
41. Kvale, S., Brinkmann, S. (2015), Det kvalitative forskningsintervju, Gyldendal Norsk forlag
42. Creswell, J. W. (2013), Qualitative Inquiry & Research Design, Sage Publications
43. Leedy, P. D., Ormrod, J. E. (2015), Practical Research - Planning and Design, Pearson Education Limited
44. Norwegian Centre for Research Data (2020), Norsk senter for forskningsdata (NSD), Bergen, URL: <https://www.nsd.no> Accessed: July 23, 2020
45. Malterud, K, (2017,4), «Kvalitative forskningsmetoder for medisin og helsefag», Universitetsforlaget
46. Johannessen, A., Tufte, P. A., Christoffersen, L. (2010,4), "Introduksjon til samfunnsvitenskapelig metode", Abstrakt Forlag
47. Glomseth, R., (2020), «Toppledere og toppledelse i politi og påtalemyndighet med fokus på utviklingstrekk, barrierer for læring og utvikling, endringer i ledelse, ledelsesprosesser og styring samt utfordringer.», Politihøgskolen, Oslo, URL: [https://pfs.brage.unit.no/pfs-xmlui/bitstream/handle/11250/2649879/toppledere\\_og\\_toppledelse.pdf?sequence=1&isAllowed=y](https://pfs.brage.unit.no/pfs-xmlui/bitstream/handle/11250/2649879/toppledere_og_toppledelse.pdf?sequence=1&isAllowed=y) Accessed: May 21, 2020
48. Direktoratet for forvaltning og økonomistyring, (DFØ), (2020), «Følgeevaluering av nærpolitireformen – statusrapport for 2019», URL: [https://dfo.no/filer/Fagomr%C3%A5der/Rapporter/2020/Statusrapport-naerpolitireformen\\_DFO-rapport-2020\\_4.pdf](https://dfo.no/filer/Fagomr%C3%A5der/Rapporter/2020/Statusrapport-naerpolitireformen_DFO-rapport-2020_4.pdf), Accessed: May 11, 2020, Oslo
49. Sunde, N, Bergum, U (2019), «Dataetterforskning – en ungdom med voksesmerter», Oslo, Norges Politilederslag, URL:

<https://www.parat.com/npl/dataetterforskning-en-ungdom-med-voksesmerter-5410-406272>, Accessed: May 5 2020

50. Hansen, H., Andersen, S., Axelsson, S., Hopland, S., (2017), "Case Study: A New Method for Investigating Crimes against Children", , NTNU, Oslo Police district, URL: [https://www.researchgate.net/publication/333609682\\_Case\\_Study\\_A\\_New\\_Method\\_for\\_Investigating\\_Crimes\\_Against\\_Children](https://www.researchgate.net/publication/333609682_Case_Study_A_New_Method_for_Investigating_Crimes_Against_Children), Accessed: June 27, 2020
51. Oslo Police District, Oslo Politidistrikt (2018), Digital Forensics Digitalt Politiarbeid, Recommendation - Anbefaling (18.04.18), Oslo 2018
52. National Police Directorate, (2012) «Detaljert prosessbeskrivelse (kvalitetsstandard kriminalteknikk)», Politidirektoratet, Oslo
53. Sunde, N., Dror, I., (2019), "Cognitive and Human Factors in Digital Forensics: Problems, Challenges, and the Way Forward", 10.1016/j.diin.2019.03.011, URL: [https://www.researchgate.net/publication/332014667\\_Cognitive\\_and\\_Human\\_Factors\\_in\\_Digital\\_Forensics\\_Problems\\_Challenges\\_and\\_the\\_Way\\_Forward](https://www.researchgate.net/publication/332014667_Cognitive_and_Human_Factors_in_Digital_Forensics_Problems_Challenges_and_the_Way_Forward), Accessed: June 25, 2020
54. The International Organization for Standardization (2020), Geneva, Switzerland, URL: <https://www.iso.org/standards.html>, Accessed: May 14, 2020

## 8 APPENDIXES

Appendix 1: NSD approval

Appendix 2: NPD approval

Appendix 3: Information and Consent form

Appendix 4: Interview guide

Appendix 5: Jahren, J .H, (2019), "Quality Assurance in Digital Forensics n The Norwegian Police, is It Good Enough?", MISEB, NTNU, Gjøvik

### 8.1 Appendix 1

14.4.2020

Meldeskjema for behandling av personopplysninger



#### **NSD sin vurdering**

##### **Prosjektittel**

Quality management/assurance in Digital Forensics in the Norwegian Police, is it good enough? What lessons can be learned from quality control in Forensic Science in the Norwegian Police?

##### **Referansenummer**

432511

##### **Registrert**

09.10.2019 av Jørn Helge Jahren - jornhja@stud.ntnu.no

##### **Behandlingsansvarlig institusjon**

Norges teknisk-naturvitenskapelige universitet NTNU / Fakultet for informasjonsteknologi og elektroteknikk

(IE) / Institutt for datateknologi og informatikk

**Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)**

Katrin Franke, katrin.franke@ntnu.no, tlf: 90215425

**Type prosjekt**

Studentprosjekt, masterstudium

**Kontaktinformasjon, student**

Jørn Helge Jahren, jorn.jahren@gmail.com, tlf: 97552421

**Prosjektperiode**

01.09.2019 - 01.06.2020

**Status**

25.11.2019 - Vurdert

**Vurdering (1)**

---

**25.11.2019 - Vurdert**

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med

personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 25.11.2019, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

**MELD VESENTLIGE ENDRINGER**

Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD 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://nsd.no/personvernombud/meld\\_prosjekt/meld\\_endringer.html](https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html)

Du må vente på svar fra NSD før endringen gjennomføres.

## TYPE OPPLYSNINGER OG VARIGHET

Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 01.06.2020.

## 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

NSD 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: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).

NSD 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

NSD 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).

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

## OPPFØLGING AV PROSJEKTET

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

Lykke til med prosjektet!

Kontaktperson hos NSD: Karin Lillevold

Tlf. Personverntjenester: 55 58 21 17 (tast 1)

<https://meldeskjema.nsd.no/vurdering/5d7f83d9-24f4-4bf3-910b-a5bf48aa7fd0>

2/2

## 8.2 Appendix 2



**POLITIET**  
POLITIDIREKTORATET

Jørn Helge Jahren  
E-post: [jorn.jahren@politiet.no](mailto:jorn.jahren@politiet.no)

**NATIONAL POLICE DIRECTORATE**

Deres referanse:  
Jørn Helge Jahren

Vår referanse:  
19/36819

Sted, Dato  
Oslo, 25.11.2019

### **DATAINNSAMLING TIL MASTEROPPGAVE VED NTNU INNENFOR FAGOMRÅDET DIGITAL FORENSICS AND CYBERCRIME INVESTIGATIONS**

Det vises til søknad mottatt 14. november 2019 med vedlegg i forbindelse med gjennomføring av masteroppgave ved NTNU innenfor det erfaringsbaserte masterstudiet "Digital forensics and cybercrime investigations".

Navnet på oppgaven er opplyst å være "Kvalitetssikring i datatekniske undersøkelser, er den god nok? Kan man lære noe av fagområdet Kriminalteknikk?". Formålet med prosjektet er å undersøke hva slags kvalitetskontroller som gjøres av arbeidet til dataetterforskere og kriminalteknikere for å kunne sammenlikne og finne ut om det er læringspunkter mellom fagområdene.

For å belyse problemstillingene planlegges det med å foreta kvalitative intervjuer med tre dataetterforskere og tre kriminalteknikere i tre politidistrikt med ulik størrelse. Det er presisert at det ikke etterspørres opplysninger om eller fra konkrete straffesaker. Videre legges det til grunn oppgaven ikke skal etterspørre eller omtale taushetsbelagt informasjon.

Politidirektoratet vurderer saken etter politiregisterloven § 33, jf. § 23. Politidirektoratet forstår søker slik at det ikke bes om innsyn i politiets registre eller i straffesaksdokumenter. Når det gjelder personlige forhold knyttet til de som ønskes intervjuet synes dette uproblematisk idet innhenting vil basere seg på samtykke. Gjennomføringen av masteroppgaven synes ikke å reise øvrige personvernutfordringer. Gjennomføringen av oppgaven – og de tema som er valgt – er innrettet slik at det ikke er behov for å omtale taushetsbelagt informasjon. Politidirektoratet legger etter dette til grunn at det ikke vil bli behandlet taushetsbelagt informasjon i spørreundersøkelsen og at det således ikke er nødvendig med fritak fra taushetsplikt etter politiregisterloven § 33.

Politiets ansatte som deltar i studien må iakttas sin taushetsplikt, og de ansatte som blir forespurt om å delta i studien må bli gjort kjent med de føringer direktoratet gir i dette brevet. Under denne forutsetning gir Politidirektoratet tillatelse til at studien kan gjennomføres. Det tas forbehold om at det eller de aktuelle politidistrikt som det ønskes bistand fra, avsetter tid og personell for gjennomføring av studien.

#### **Politidirektoratet**

Tlf: 23 36 41 00

Org. nr.: 982 531 950

Post: Postboks 8051 Dep., 0031 Oslo  
Besøk: Fridtjof Nansens vei 14/16

Faks: 23 36 42 96  
E-post: [politidirektoratet@politiet.no](mailto:politidirektoratet@politiet.no)

Giro: 7694.05.02388  
[www.politi.no](http://www.politi.no)

Med hilsen

## 8.3 Appendix 3

# VIL DU DELTA I FORSKNINGSPROSJEKTET

*“ Kvalitetssikring i datatekniske undersøkelser, er den god nok? Kan man lære noe av fagområdet Kriminalteknikk”?*

### Formål

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke om hva slags kvalitetskontroller som gjøres av arbeidet til dataetterforskere og kriminalteknikere i Norge, for å sammenligne og se om det er læringspunkter mellom fagområdene.

**Hvem er ansvarlig for forskningsprosjektet?**

NTNU - Gjøvik

## Hvorfor får du spørsmål om å delta?

Jeg har valgt å intervju dataetterforskere og kriminalteknikere fra et lite, et mellomstort og et stort distrikt, fordi det kan være forskjeller i organisering, sammensetning og oppgaveløsning.

## Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet, innebærer det at du deltar i et videointervju på Skype. Det vil ta deg ca. 30 minutter. Jeg tar opptak og notater fra intervjuet.

## 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 opplysninger om deg vil da bli anonymisert. 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.

- Det er kun student og veilederne **Nina Sunde** og **Katrin Franke** som vil ha tilgang til de lagrede opptakene/personopplysningene
- Navnet og kontaktopplysningene dine vil jeg erstatte med en kode som lagres på egen navneliste adskilt fra øvrige data,

som lagres kryptert på et serverområde til forskningsstedet, NTNU.

Deltakernes identitet vil bli anonymisert i prosjektet.

### **Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?**

Prosjektet skal etter planen avsluttes 1.6.2020. Opptak og personopplysninger slettes etter at prosjektet er fullført.

### **Dine rettigheter**

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

- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

### **Hva gir oss rett til å behandle personopplysninger om deg?**

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

### **Hvor kan jeg finne ut mer?**

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

- NTNU - Gjøvik ved prosjektansvarlig professor Katrin Franke, [katrin.franke@ntnu.no](mailto:katrin.franke@ntnu.no)
- Veileder fra Politihøgskolen politioverbetjent Nina Sunde, [nina.sunde@phs.no](mailto:nina.sunde@phs.no)
- Vårt personvernombud: Thomas Helgesen, [thomas.helgesen@ntnu.no](mailto:thomas.helgesen@ntnu.no)
- NSD – Norsk senter for forskningsdata AS, på epost ([personverntjenester@nsd.no](mailto:personverntjenester@nsd.no)) eller telefon: 55 58 21 17.

Med vennlig hilsen

Prosjektansvarlig  
(Forsker/veileder)

*Eventuelt student*

---

---

## Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet, **«Kvalitetssikring i datatekniske undersøkelser, er den god nok? Kan man lære noe av fagområdet Kriminalteknikk?»**, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. 1.6.2020

---

---

(Signert av prosjektdeltaker, dato)

## 8.4 Appendix 4

# **INTERVJUGUIDE**

*” Kvalitetssikring i datatekniske undersøkelser, er den god nok? Kan man lære noe av fagområdet Kriminalteknikk”?*

Informasjon til informanten om at intervjuet blir tatt opp på lyd/video, og at opptaket blir lagret på sikkert/kryptert område, og slettes etter at analysen/forskningen er gjennomført. Avklarer om informanten synes dette er greit.

### **Innledning:**

I innledningen spørres informanten om navn, stilling, utdanning, bakgrunn og erfaring som kriminaltekniker/dataetterforsker.

### **Hoveddel:**

#### **Kvalitet i etterforskningen**

- *Politireformen – kvalitetsreformen er gjennomført – med sammenslåing og større enheter - hvordan har denne påvirket*



*arbeidet i din enhet i det nye politidistriktet? Er det fokus på kvalitet? Har ledelsen i ditt distrikt mer fokus på kvalitet knyttet til ditt fagområde?*

- *Kvalitetssikring/styring i kriminalteknikk/datatekniske undersøkelser før politireformen – fortell om eventuelle etablerte systemer for dette?*
- *Etterforskningsløftet – beskriv om det hittil ført til økt fokus på kvalitet, kvalitetssikring og kvalitetsstyring i ditt fagområde?*

### **Utdanning, kompetanse, sertifisering og standardisering**

- *Fortell litt om hvilke retningslinjer for hva slags utdanning/kompetanse en dataetterforsker/kriminaltekniker skal inneha i ditt distrikt?*
- *Kan du forklare litt om distriktets kompetanseplaner for dataetterforskere/kriminalteknikere?*
- *Beskriv eventuelle standardiserte, akkrediterte metoder som er etablert i distriktet innenfor ditt fagområde?*

### **Kvalitetssikring av arbeidet til dataetterforsker/kriminaltekniker**

- *Beskriv hvilke rutiner som er etablert for å kontrollere kvaliteten i arbeidet med den kriminaltekniske etterforskningsprosessen?*
  - *Hva slags kvalitetskontroller?*
  - *Hvordan gjennomføres kvalitetskontrollen?*
  - *Hvem gjennomfører kvalitetskontrollen?*

- *Beskriv hvilke rutiner som er etablert for å kontrollere kvaliteten i arbeidet med den datatekniske etterforskningsprosessen?*
  - *Hva slags kvalitetskontroller?*
  - *Hvordan gjennomføres kvalitetskontrollen?*
  - *Hvem gjennomfører kvalitetskontrollen?*

### **Kvalitetssikring og styring – status og behov**

- *Kvalitet – hva betyr det for deg i ditt arbeid?*
- *Kan du si din mening om kvalitetskontrollen av arbeidet til kriminaltekniker/dataetterforsker tilfredsstillende?*
- *Hvilke kontrolltiltak bør gjennomføres og hvem bør ha ansvaret for dette?*

Jørn Helge Jahren

Student v/MISEB, NTNU

## 8.5 Appendix 5



QUALITY ASSURANCE IN DIGITAL FORENSICS IN  
THE NORWEGIAN POLICE  
Is it good enough?

Jørn Helge Jahren

Contents

CONTENTS .....	1
1 REVISION HISTORY .....	2
2 ABSTRACT .....	3
3 ACKNOWLEDGEMENTS .....	4
4 INTRODUCTION AND PROBLEM DESCRIPTION .....	5
5 METHODOLOGY .....	7
6 BACKGROUND AND THEORY .....	8
7 RESULTS AND DISCUSSION .....	11
8 CONCLUSION .....	17
9 BIBLIOGRAPHY: .....	18

## 1 Revision history

Version	Changes
0.1	Created a chapter called Background and theory to explain about the police organization 26.5
0.2	Created a list of abbreviations explaining some terms 29.5
0.3	Added reference 15 – role descriptions for the police – and in list of abbreviations added Digital Forensic Examiner – added reference 16 article about DFI role and competence 31.5

## 2 Abstract

Digital Forensics (DF) is a relatively new field in forensics but may still be the fastest growing in complexity and extent. I have worked within the field of DF since 2003 both in the police and in the Norwegian Tax Administration, both as an operative digital forensic examiner and as a manager or team leader. The evolution I have experienced in those 15 years has been enormous when it comes to the amount of cases Digital Forensic Investigators (DFI) are being involved in today, compared to 2003. Other issues like the amount of data, platforms, handhelds, internet cloud storages and the number of providers of services, have done the work of the DFI's far more complex today than 15 years ago. As no quality management measures or peer review or other quality systems were undertaken prior to the court proceedings, the responsibility on me as a witness was considerable. The total absence of quality system should be cause for concern.

In this project I wanted to explore to what extent digital forensic examinations within Norwegian law enforcement was subject to quality management (QM). I wanted to find out whether there was any standardization of methods, accredited labs, certifications of personnel or standards/guidelines for how DF examinations should be carried out. I also wanted to compare the status of QM in digital forensic examinations with how this was conducted within Forensic Science (FS) (Norwegian: Kriminalteknikk) undertaken by Norwegian law enforcement. Due to my extensive experience from the DF field, the results were not overwhelming or shocking in any way. There are no formalized guidelines or standards governing DF examinations in Norwegian law enforcement. In the FS field, a quality standard was released from the National Police Directorate (NPD) in 2013, which gives guidance for a forensically sound processes in FS examinations. There are some newly established and promising initiatives within both DF and FS. In 2018, several national groups of experts for professional development and improvement of quality were established, including DF and FS.

### 3 Acknowledgements

Thanks to my supervisors Ulf Bergum and Nina Sunde at the Norwegian Police Academy for putting me on the idea and on track to get started, and for guidance and advices during my writing.

I want to thank my informants in the Forensic Science sections in Kripos(NCIS) and Sør-Øst police district, Assistant Chief of Police Morten Olsen Sandnes at NCIS, Police Superintendent Trond Sandsbråten and in Digital Forensics, Special Investigator Roy Evensen from Sør-Øst police district.

## 4 Introduction and problem description

The motivation for this research is very clear. I have worked as a DF investigator in the Norwegian police, in Vestfold district and later Sør-Øst district for 15 years. During this period, I have experienced a demand for efficiency, but no one seems to be concerned about the quality of the work that I have done, or the digital evidence I have provided. The “quality control” if one can call it so, has been done occasionally when I have asked my colleagues to review my reports or presentations. Otherwise – the quality control has been left with the judge when I presented digital evidence in court. In general, my experience has been that the work has been accepted as good and solid, often with few or little questions asked from the parties, when presented in court.

When I started working with DF in law enforcement, my technology competence was from a part time education in computer science. I had no preliminary training in DF before I went ahead and did live examinations of digital evidence in the police. When I started doing DF, there were no competence requirements, and no standardization of procedures, methods or tools. Except a newly defined competency requirement for DF, the situation is pretty much the same today. There is a lot more focus on digital forensics and the importance of digital evidence today due to the fact that people literally live digitally, because of the rapid technologic development which again has given an enormous amount of data on different data carriers. Because of this, the demand for digital evidence in criminal investigations is increasing, and increasingly more people are working with DF. While the demand for digital evidence is growing, it is worrying that there still are no standards or requirements for processes, tools, methods or quality management

### Problem description

In this project, I focus on the quality management of the work of Digital Forensic Investigators (DFI). I compared it to the work of Forensic Science Technicians (FST), whose field has a longer history in criminal investigations, and assumingly have better quality management. The research questions are:

- In Norwegian law enforcement, what is done to ensure quality in DF examinations, and how is this done?
- Can DF learn something from the FS in terms of quality management of their work?



The question(s) will be answered to an extent, getting an overview, with status and some of the ongoing projects for future development of the two disciplines.

#### Delimitations

I will only focus on DF the police organization and not the private sector and will concentrate on the role of the digital forensic investigator and no other roles.

#### List of abbreviations:

##### DE – Digital Evidence

- “Digital Evidence is defined as any digital data that contains reliable information that can support or refute a hypothesis of an incident or crime” (2)

##### DF - Digital forensics

- “Digital Forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation 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” (2)

##### DFI - Digital Forensic Investigator

- A police educated or civilian with relevant competence who preserves, collects, validate, identifies, analyzes, interprets and presents digital evidence acquired from digital sources

##### DFE – Digital Forensic Examiner

- A police or civilian with basic competence, primarily to conduct examinations on material acquired and prepared by DFI’s – a support and “middleman/woman” for DFI’s and investigators

##### FS – Forensic Science

- Forensic Science definition would, in my opinion, be the same as DF besides “digital evidence derived from digital sources” but instead physical evidence at crime scenes or from other possible sources relevant to the investigation

FST - Forensic Science Technician

- An investigator who preserves, collects, validates, identifies, analyzes, interprets and presents evidence from a crime scene, like any kind of object or fluid found that can contain possible evidence, but it can also be a lab-technician analyzing content of drugs, firearms ballistics, blood, fingerprints etc. but not forensic autopsies and DNA-analyses.

NPUC – Norwegian Police University College

NPD – National Police Directorate (Politidirektoratet)

NDPP - Norwegian Director of Public Prosecutions (Riksadvokaten)

NCIS – National Criminal Investigation Service (Kripos)

SDP – Section for Digital Policing

NCFI – Nordic Computer Forensic Investigator

Structure of this report

The methods I have used is explained in chapter 5. I will present the background and theoretical basis of my project in chapter 6. In chapter 7 the results will be presented and discussed in chapter, followed by a conclusion in chapter 8.

## 5 Methodology

I have been working in the Norwegian police for nearly 30 years and have gotten a lot of experience in many disciplines in policework, like patrolling, SWAT-officer, investigator in a police station, financial crime investigator and for the last 15 years, digital forensics. This has given me detailed insight of how “things work” in the Norwegian police, and much of the descriptions of the DF field in this paper is obtained from my background knowledge and therefore biased by my opinions being an insider. To solve my research problem, I have studied government publications that discusses the status and the future development of DF and FS. I have also obtained information from colleagues in the two milieus in Sør-Øst police district and on National Criminal Investigation Service (NCIS).

Finally, I have read scientific papers about QM in DF and FS, to get an insight on how the quality is governed in other countries.

Due to the scope of this project, I have not obtained a complete oversight over the QM situation in DF and FS work in Norway. To get a more complete picture of the situation, more research is necessary. Therefore, the results presented in this report only provides general overview of the status of QM in DF and FS in law enforcement in Norway based on a limited number of informants and information sources, with inputs from colleagues in both fields at NCIS and Sør-Øst police district, in addition to reading official documents and publications.

## 6 Background and theory

After the terrorist-attacks in Oslo and Utøya in 2011, the Norwegian police were criticized for how they handled the situation. This resulted in a thorough examination of the involved police forces by a government appointed commission. As a result, several challenges were uncovered concerning how the organization of the police, and their emergency readiness. This resulted in a demand to make the police more robust all over the country and therefore to reform the organization.

This re-organization of the police has just been completed, at least for the local districts. The national investigation units will have their re-organization starting from 2019. The re-organization was named "*Nærpolitireformen*", which may be translated to "*Police reformed to be more present*" (1). The police districts were reduced from 27 to 12. The main goal with the reform has been to make more robust units who are capable of handling large scale investigations and crises. The reform has been heavily criticized and disputed, mostly by the local communities and for minimal funding and too heavy centralization of units, but the new districts are now operational.

In the reform-proposition it was also pointed at the fact that the police have to be better organized and coordinated digitally to be able to meet the future demands, both in investigating digital related crimes, and in general get a more modern digital infrastructure. The new districts were given a set of measures and guidelines on how to conduct the reform in "*Rammer og retningslinjer for etablering av nye politidistrikter, 2016*," which may be translated to "*Guide and guidelines for establishing new police districts*" (3), when the reform started in January 2016. The document describes in detail how the new districts should re-organize into new centralized bigger units, sections and groups.

## The new organization of DF in Norway

Before the “Nærpolitireformen”, there were DF units in all the 27 police districts. After the re-organization of the police, they were merged into larger units, named “*Seksjon for Digitalt Politiarbeid*” or Section for Digital Policing (SDP). All SDPs had a similar internal structure and were given guidelines for how they should be formed and rigged for the future. Each of the 12 districts now has its own SDP, that should in time, be more robust to handle large scale and complex investigations on their own.

Some districts, like Sør-Øst were merged from 4 of the old districts. DFI’s were moved to new locations to comply with the demand to create more robust units, which for some people implied a longer travel route to work. This again, has to my knowledge, led to some loss of qualified DFI’s to other police districts, national investigations services or competing businesses in private sector

Oslo is the largest police district in Norway, with over 3000 employees. Their SDP got a mandate from the Department of Justice as one of the measures in their strategy document from , “*Justis -og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*”, which may be translated to “*The Justice departments strategy to fight Cybercrime, 2015*” (4), to create and deliver a pilot-project for how the 12 districts could evolve in the best way to be able to investigate and prevent digital-related crimes. The report has been sent to the NPD in 2018, but there has, to my knowledge, not resulted in any new measures or instructions to the districts yet.

Another measure introduced by the above-mentioned strategy document was to create a National Cybercrime Center (NC3). This was established in January 2019, currently consisting of 4 sections transferred from the NCIS. The center is planned to increase in the number of employees, but the composition and interface against the districts, and what task/duties they will deliver and what the districts should handle themselves is not yet clear

## Quality in criminal investigations

The term quality is frequently used when Norwegian politicians and police leaders talk about the necessity of the major reform of the police. In May 2016 the NPD released a strategy

aimed at better quality in the investigations and the overall criminal case work all over the country. The plan is called "*Handlingsplan for løft av etterforskningsfeltet*" may be translated to "*Strategic plan to raise competence in the field of investigation*" (5). The plan is a part of the reform and is a result of a cooperation with the Norwegian Director of Public Prosecutions (NDPP), who for a long period of time has called for a general increase of competence in criminal investigations.

In the strategic plan NDPP has listed a set of quality markers which represents what he sees as necessities for assuring the best quality in a criminal investigation. One of the markers refers to that the quality concept in an investigation not only should focus on the results, but also to the dedication and execution of the task. This is a very important concept that should be emphasized, because the dominating focus has been on the results in the Norwegian police. Time spent per investigation is one of the most measured entities in the criminal justice system, and probably the most important one, both for the people involved and for the police.

In "*Kvalitetsrundskrivet*" (NDPP, 2018) may be translated to "*Quality circular for criminal case processing for the police and the district attorney's office*" (6), the NDPP describes how quality should be understood and assessed in criminal investigations. The NDPP emphasizes the requirement to be objective in all parts of the criminal justice chain to avoid errors of justice and to secure the rule of law. An objective and transparent investigation process is necessary to be perceived as trustworthy to the society.

Errors in criminal investigations may have severe consequences for the parties involved. They may lead to miscarriage of justice, such as conviction of innocent people, and that guilty people are acquitted. Therefore, measures and mechanisms aimed at reducing errors in any criminal investigation are very important. Quality measures may prevent errors to occur or may detect errors before they affect the outcome of the investigation. One of these mechanisms should be quality assurance/management of some kind to reduce the risk of faults which lead to wrong acquittals and in worst case miscarriages of justice.

So, about quality in DF, why is it important to look in to?

There is digital evidence in nearly every criminal investigation today. This can be messages on a phone, internet related evidence from a weblog, the content of a memory stick, etc. To

securely identify, collect/acquire, examine and analyze this evidence, special competence and experience is necessary. In my opinion, there is also a need to define and standardize competency requirements, to accredit or acknowledge methods, and require certifications to perform advanced digital forensics in criminal investigations. This will be important to ensure sufficient quality, and the same level of quality all over the country. A transparent handling of digital evidence will enable the necessary scrutiny of the methods and tools used and is important for a fair administration of justice and the rule of law.

Why compare DF to FS?

A Forensic Science Technician (FST) preserves, collects, validates, identifies, analyzes, interprets and presents findings of physical objects on a crime scene. These work-processes seems to be quite similar and transferable to the work-processes of the Digital Forensic Investigator (DFI), except that the DFI handles digital evidence.

Page (et al 2018) point to this in the article “A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn?”, where the situation in the UK seems to be similar to the situation in Norway, and there seems to be “an apparent lack of quality management in DF”. In this article, experiences from quality management in Forensic science disciplines in fingerprint examinations, DNA-analysis are explained, and the authors recommend establishing similar quality management for DF. This will be further discussed in chapter 7. (7)

## 7 Results and discussion

An overview of the quality in DF in Norway – competence/education, standardization, accreditation, certification – what is the current status?

Competence/education

The first education within DF at Norwegian Police University College (NPUC) was offered in 2004, and since then NPUC has developed a broad portfolio of educations in DF.

Currently, the educations are divided in three levels. At the basic level, we find NCFI Module 1, Core Concepts. These educations are included in the competency requirements for DFIs in Norway as of January 2019(15).

At the second level, Module 2, there are several educations aimed at development of more specialized competencies within DF, such as advanced computer forensics, online investigation and network forensics/cybercrime investigations. At the third level, Module 3, there are more advanced and specialized educations at master level. These are included in the experience-based master program offered by NPUC and Norwegian University of Science and Technology (NTNU), Gjøvik. (8,9)

The NPUC offer, to my knowledge, one of the best educations for Digital Forensic personnel in Europe. NPUC and has in the later years established relationships with police academies from many European countries, like all the Nordic countries, Germany and Poland. NPUC educations are offered to DFIs from these countries. All of these educations are aimed at giving the attending DFIs sufficient knowledge and skills to conduct DF work with the highest level of quality.

Knowing this, there should be a solid base for DF personnel in these countries to conduct and deliver forensic work and examinations with high quality, if they do attend the studies.

NDP recently published role definitions for the different professions, like the DFI, and what qualifications they should have. To be a DFI the NPD has set the qualification level to NCFI Module 1 Core Concepts. This is basic level education meant for investigators who should operate as a “helper” in investigations as a Digital Forensic Examiner (DFE). This role was recently introduced in the police, and should conduct simple securing and analysis tasks, to reduce the workload for the DFI. This would enable the DFI to concentrate on the more advanced digital forensic tasks.

To set the qualification level to the DFI to NCFI Module 1 Core Concepts is in my opinion insufficient, due to the complexity of handling digital evidence today. The entry level qualifications should at least be at NCFI level 2 or similar, which also is the opinion of the staff providing DF educations at NPUC (16).

#### Standardization/certification/accreditation

The NDP released a circular in 2010, "*Circular 2010/007, Behandling av beslag I straffesaker*", translated to "*Handling seized evidence in criminal cases*". (10)

In general, the circular describes what objects that can be seized, how the seized objects should be handled/preserved and by whom. Section 3 of the document describes what Digital Evidence (DE) is or could be, how and what data/information that can be seized, and most important, that DE only can be seized by qualified personnel with special and adequate training, equipment and software.

The circular is, to my knowledge, still the leading official governing "quality document" for the police to handle seized digital evidence. There are not specifications on what kind of education/training, certification or standards for the personnel that handles DE, should possess, in the document.

"Politiet I det digitale samfunn, 2012", translated to "*The Police in the digital society*" (11), describes the situation prior to the reform, and concludes that there are needed standards in methods, tools and competence, to meet the challenges in the DF field, and handle DE in investigations with good quality.

Now, in 2019, there is, to my knowledge, still no standardizations of tools/equipment, accredited methods or certifications in DF in Norway. There are though, by orders from the NPD in 2018, created national groups within special disciplines in the investigation field. These groups were tasked to develop and identify the needs to enhance the quality in their respective disciplines. This measure is a part of the reform of the police and the DF and FS are two of the disciplines, and both are led by NCIS, with competent participants from the districts.

According to one of the members in the national DF-group, Special Investigator Roy Evensen in Sør-Øst district, the group has just started to obtain an overview of how the current situation is in the districts in terms of equipment, human resources, competence and the needs for the future. According to Evensen, there are huge differences in how the districts have prioritized and organized the function handling DF, the SDP.



An overview of the quality in FS in Norway – competence/education, standardization, accreditation, certification – what is the current status?

#### Competence/education

There are several specialized educations for the FS, and there are 4 levels/modules of education, where one can specialize on different subjects like fire related crime scenes and investigations, severe accidents, blood traces, explosions etc.

The newest, and highest level 4, released in 2018, is the education for Forensic Science Coordinators, which focuses on the cooperation between the Forensic Science Technicians (FST) and the investigators in criminal investigations. According to the education program, the education is aimed at ensuring that the forensic science work is being done with the highest quality. (8)

In areas like fingerprint identification and DNA analysis, districts send samples collected in the daily service for registration and possible identification of suspects in criminal cases. The quality control of these collected samples is done at the forensic labs at (NCIS) or their cooperatives.

The forensic science field is associated with several lab functions, like labs for ballistic research of firearms, chemical labs for different analyzes like identifying and registration quantity of drugs, handwriting examinations, fingerprints, fire-related examinations etc. Most of these lab functions does NCIS have the sole national responsibility for. The districts send material for lab examination to NCIS and get reports back with the results, when the examinations have been conducted.

#### Standardization/certification/accreditation

According to Assistant Chief of Police Morten Sandnes Olsen at NCIS the different lab functions and methods are accredited by Norsk Akkreditering. (12) Forensic work on crime scenes is still not accredited but there is ongoing work in other countries in Europe developing accredited methods for this.

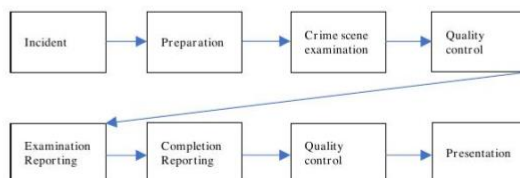
NCIS has the national responsibility for development and implementation of new technology and methods in the FS field in Norway. This is expressed specifically in a document from the NPD, “Kvalitetsstandard for kriminalteknisk etterforskning, 2013” may be translated to “Quality standard for Forensic Science (Technical) investigations”, (13) which came out in 2013”. Although Digital Forensics is included as a discipline under the umbrella term Forensic Science, this document states explicitly that Digital Forensics is excluded from the requirements of the document.

Some highlights from the document:

- The document defines a standard for all work in the FS field with areas of responsibilities set to the local districts, the NPUC, NCIS and NPD in order to assure that the guidelines within are followed and maintained.
- Quality management is defined as a responsibility for the leaders in the districts, to further create routines that assures quality in every part of the forensic work, so that processes are documented, and can be verified. The responsibility also includes having a system for following up faults/mistakes and for identifying, documenting, analyzing and reporting them with what measures that has been taken.
- Review of all reports and verification of the documentation in the examinations should be conducted by at least one qualified person.

The forensic science work process in FS, (13),

Figure 1. recreated and text translated by as good as it may, by me.



I have not found the detailed description of the forensic process in the document, but it seems to be an adequate process preserving quality control after collecting and preserving possible evidence at a crime scene, and a new quality control when finished utterly examination and

start and complete reporting, before an eventual presentation in court. This process seems to be a really good standard for quality assurance, if followed. It also depends on what kind of control measures that are conducted.

According to Police Superintendent in Sør-Øst district, Trond Sandsbråten, who is an FST, the quality standard is followed in their district. In Sør-Øst the FST's work in pairs of two, as dual-investigators on every case/incident, they conduct the whole forensic process together and review each other's examinations, documentations and reports.

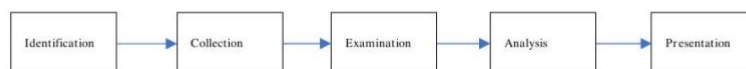
This way to work is commented by Page (et al 2018) {7} as a good sound way to reduce errors in investigations because they both will have the responsibility for the all work, and more eyes and knowledge probably gives better results.

Sandsbråten also commented that they have, according to the standard, created local guidelines on how to conduct the forensic process locally. He is also a member in the national development group for the FS field, and similar to DF, they have just started to get an overview and status of FS work in the districts. Like for DF there are huge differences in organizations and how they work locally.

#### The Digital Forensic Process

To compare the FS process to the digital forensic process in the book "Digital Forensics, 2018, Wiley, edited by Andre Årnes, Flaglien, p. 16," (14), the process has these steps:

Figure 2 recreated by me

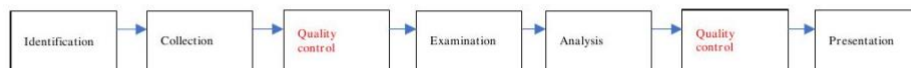


The process is well known to most DFI's and is aimed at preserving evidence integrity and the chain of custody (COC), which are the base for all digital forensic work to handle DE in a forensically sound manner. Evidence integrity is to keep the evidence in the original form, and not change it in any way. COC is the process of documenting every step of the work done in a case, to be transparent.

In short terms, explaining the steps, identification of possible digital evidence, collection is some kind of copying data, examination is processing and structuring the collected data, analysis to seek and find possible evidence in the data, presentation of the findings in reports or in courts or other interests. The process enhances quality control by ensuring integrity and chain of custody – but the control is conducted by the DFI him/herself.

Compared to the FS process the DF process has an obvious shortage/lack. There are no quality control measures conducted by others in it! Looking at the FS process it should naturally be a control after the collection phase to among other things verify the data before examining it, and another one before presenting a report or presentation.

Figure 3. created by me to illustrate my statement



Quality assurance – other methods?

Page (et al 2018 (7), suggests some good methods of quality control in 5 levels of peer review for DF:

1. Re-examination – being a total new examination by another expert being able to compare the results of the DFI and the reviewer – reduces possible cognitive biases – but requires resources in time and personnel
2. Verification review – Validation of findings on datasets and not all acquired data to check traces, hypotheses etc
3. Conceptual peer review – Review of documentation of findings, descriptions of artefacts, acutally if COC is documented.
4. Sense review – check if the presentation of findings make sense as evidence
5. Proof check – check language for spelling and grammatical faults

With my experience from the police I know that a re-examination of every case is impossible due to lack of resources, however, it should be done at an interval, maybe once pr 6 months or so.

A verification review should be feasible in more frequent intervals, and the three next reviews should be done in all delivered work in DF.

## 8 Conclusion

Quality of the work in DF in Norway seems to lack systems for quality management and quality assurance. There are few, or more correct, no governing instructions or standards in how the work in DF should be conducted in the Norwegian police, few (and insufficient) demands in competence/certification for DFI's, no standardizations or accreditation of methods, tools or equipment. There is a great need for systems to increase the quality in DF, to reduce the risks of errors and misleading evidence resulting from poor DF work. After comparing the processes in FS and DF, I have suggested some quality control steps to the DF process. The effects of such measures should be investigated in further research.

In this report I have documented, to some extent, that the Forensic Science (FS) field in Norway has a far more developed system for quality management and control and has a national standard for this. The FST's in Sør-Øst police district work in pairs securing a quality control in the whole forensic process.

Future work will be to look closer into the FS field to see in detail and to experience how the quality control of the forensic processes are conducted.

## 9 Bibliography

1. The Justice department, (2015), "Nærpolitireformen", URL: <https://www.regjeringen.no/no/tema/lov-og-rett/kriminalitet-og-politi/innsikt/narpolitireformen/id2398914/>, Oslo, Det kongelige justis og beredskapsdepartement
2. Årnes, A. (2018), Introduction. In: "Digital Forensics", Årnes, A. (editor), Wiley
3. National Police Directorate, (2016), «Rammer og retningslinjer for etablering av nye politidistrikter», Oslo, Politidirektoratet
4. The Justice department, (2015), «Justis -og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet», URL: <https://www.regjeringen.no/no/dokumenter/justis--og-beredskapsdepartementets-strategi-for-a-bekjempe-ikt-kriminalitet/>

- [beredskapsdepartementets-strategi-for-a-bekjempe-ikt-kriminalitet/id2413705/](#), Oslo, Det kongelige justis og beredskapsdepartement
5. National Police Directorate (2016), "Handlingsplan for løft av etterforskningsfeltet", Oslo, URL: <https://www.politiet.no/globalassets/05-om-oss/03-strategier-og-planer/handlingsplan-for-loft-av-etterforskningsfeltet.pdf>, Oslo, Politidirektoratet
  6. Norwegian Director of Public Prosecutions (2018), «Kvalitetsrundskrivet 03/2018», URL: <https://www.riksadvokaten.no/document/nytt-kvalitetsrundskriv/>, Oslo, Riksadvokaten
  7. Page, Horsman, Sarna and Foster (2018), "A review of quality procedures in the UK forensic sciences: What can the field of Digital Forensics learn ?", Helen, P., Science & Justice, URL: <https://doi.org/10.1016/j.scijus.2018.09.006> , Accessed: January 24 2019
  8. Norwegian Police University College (2019), Etter og videreutdanning i etterforskning og kriminalteknikk, URL: <https://www.phs.no/studietilbud/etter-og-videreutdanning/utdanninger/etterforskning-og-kriminalteknikk/>, Oslo, Politi høyskolen, Accessed: May 30 2019
  9. Norwegian University of Science and Technology (NTNU), (2019), "Erfaringsbasert master I informasjonssikkerhet, MISEB", URL: <https://www.ntnu.edu/studies/miseb> , Accessed: May 30 2019, Gjøvik NTNU
  10. National Police Directorate (2010), "Rundskriv 2010/007, Behandling av beslag I straffesaker", URL: <https://fido.nrk.no/0f9e97f92048ab8ee84d28411b7d5399bf32998537b841582648e891b1818aac/Rundskriv%202010-007.pdf>, Accessed: May 28 2019, Oslo, Politidirektoratet
  11. National Police Directorate (2012), "Politiet I det digitale samfunn, en arbeidsgrupperapport om: Elektroniske spor, IKT-kriminalitet og politiarbeid på internett", URL: <https://medlem.ntl.no/Content/103500/cache=20122109105334/Politiet%20i%20det%20digitale%20samfunn%20juli%202012.pdf> Accessed: May 30 2019, Oslo Politidirektoratet

12. Norwegian Accreditation (2019), «Norges nasjonale organ for teknisk akkreditering og god laboratoriepraksis», URL: <https://www.akkreditert.no/om-oss/>, Accessed: May 25 2019, Norsk Akkreditering, Lillestrøm
13. National Police Directorate (2013), «Kvalitetsstandard for kriminalteknisk etterforskning», URL: <https://docplayer.me/5070229-Kvalitetsstandard-for-kriminalteknisk-etterforskning.html>, Accessed: January 24 2019, Politidirektoratet, Oslo
14. Flaglien, A (2018), «The Digital Forensic Process», p. 16, in: «Digital Forensics», Årnes, A (editor), Wiley
15. National Police Directorate(2018) «Nasjonale rolledefinisjoner med kompetansekrav - etterforskningsfeltet», URL: <https://www.politilederen.no/dokumenter/POD/Nasjonale%20rollebeskrivelser%20med%20kompetansekrav%20v0.7.pdf>, Accessed: May 31 2019, Politidirektoratet, Oslo
16. Sunde, N, Bergum, U (2019), «Dataetterforskning – en ungdom med voksesmerter», URL: <https://www.parat.com/npl/dataetterforskning-en-ungdom-med-voksesmerter-5410-406272>, Accessed: May 31 2019, Norges Politilederslag, Oslo

