NTNU

Norwegian University of
Science and Technology

Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation

Nina Sunde

Information Security
Submission date: August 2017
Supervisor: Carl Stuart Leichter, IIK
Co-supervisor: Inger Marie Sunde, IIK

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Master's thesis

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

Author:
Nina Sunde

Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation

Supervisor:
Inger Marie Sunde

Oslo, 01.06.17

Experience-based Master in Digital Forensics and Cybercrime Investigation (MISEB)
30 ECTS
A program in cooperation with the Norwegian Police University College

POLITIHØGSKOLEN

NTNU
Norwegian University of Science and Technology

Acknowledgements

I would like to thank the Norwegian University of Science and Technology and the Norwegian Police University College for three challenging and interesting years as a master student.

I want to thank my supervisor, Professor Inger Marie Sunde for guidance, inspiration, encouragement and constructive criticism.

I am grateful for the cooperation of my informants from the Oslo Police District, and want to thank them for their honesty, engagement and time.

I want to thank my colleagues, Kristina K. Jakobsen and Patrick U. Risan for their involvement and valuable input.

And eventually, I want to thank my husband for proof reading, support and patience. I want to thank my sons for laughter and convenient interruptions, which brought me up to the surface when I dove too deep into the thesis.

Abstract

Digital evidence is relevant to almost every criminal case. Like other lines of evidence, they serve the purpose of establishing the indisputable facts, and they also shed light on the suspects' motivation and purpose of committing the crime under investigation. The spectrum of technical errors and uncertainties with digital evidence is thoroughly covered in literature. This study aims at the non-technical sources of errors that might impact the potential digital evidence in the investigation of a criminal case.

In the thesis the research problem addressed is: When handling digital evidence in a criminal investigation, do the non-technical sources of errors pose a threat towards the required quality, and eventually the rule of law?

The Digital Forensics Process and The Investigative Cycle is the fundament for the analysis in this study, and is discussed in relation to relevant theory and methodologies from a criminal investigation point of view. Theory from law, criminal investigative methodology, forensic psychology and digital forensics is used to solve the research problem. This study employed a qualitative methodological approach, and built on a hermeneutic–phenomenological theoretical framework. 6 detectives from the Oslo Police District were interviewed in semi-structured interviews. The analysis was performed with The Step-by-step Deductive Inductive approach (SDI-model).

The data analysis showed that criminal investigation was conducted within the phases of the Digital Forensics Process. Investigative competence was needed in the identification-, analysis-, and presentation phases. The investigation of digital evidence was carried out by digital forensic detectives with police or civil background. The participants without police background had only a one-day course in subjects relevant to criminal investigation.

The cooperation when investigating digital evidence was regarded most successful when the digital forensic detective was involved in the investigation at an early stage, or fully included in the investigation team. The examples from the participants showed that other important

factors for good cooperation in investigation of digital evidence were clear leadership and adequate allocation of resources.

The literature review and the interviews led to identification of several non-technical sources of errors in relation to investigation of digital evidence, and they were divided into four main themes: The individual detective does not possess the sufficient competence, absence of the right type of competence at the right time during the investigation, bias and heuristics and organisational challenges, such as missing competency requirements and large backlogs. This resulted in the development of a concept where the necessary technological and investigative competence in relation to the Digital Forensics Process was described.

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. Countermeasures towards the sources of errors on an individual level, a cooperation level or an organisational level are suggested.

Keywords

Digital forensics, Digital Forensics Process, The Investigative Cycle, analysis sub-phases, criminal investigation, digital evidence, errors, sources of errors, technological competence, investigative competence, bias, heuristics.

Sammendrag

Digitale bevis er relevante i så godt som alle straffesaker. I likhet med andre typer bevis, tjener de hensikten å etablere sakens udiskuterbare fakta. De belyser også mistenktes motivasjon og hensikt med å begå den kriminelle handlingen som etterforskes. Spektret av tekniske feil og usikkerhetsmomenter med digitale bevis er grundig behandlet i litteraturen. Dette studiet retter seg mot de ikke-tekniske feilkildene som kan påvirke det potensielle digitale beviset som etterforskes i en straffesak.

Forskningsspørsmålet som søkes besvart i denne masteroppgaven er: Når digitale bevis inngår i etterforskningen av straffbare forhold, utgjør de ikke-tekniske feilkildene en trussel mot den nødvendige kvaliteten, og til sist rettssikkerheten?

Dataetterforskningsprosessen og etterforskningssyklusen danner fundamentet i dette studiet, og diskuteres i relasjon til relevant etterforskningsfaglig relevant teori og metodikk. Juridisk teori, samt teori fra etterforskningsmetoder, rettspsykologi og dataetterforskning blir brukt for å besvare forskningsspørsmålet. Dette er en kvalitativ studie som bygger på et hermeneutisk-fenomenologisk teoretisk rammeverk. 6 etterforskeren fra Oslo Politidistrikt ble intervjuet i semistrukturerte intervjuer. Analysen ble gjennomført med Steg-for-steg deduktiv induktiv metode (SDI-modellen).

Analysen av de innsamlede data viste at straffesaksetterforskning skjedde innenfor Dataetterforskningsprosessen. Det var behov for etterforskningsfaglig kompetanse i identifikasjons-, analyse- og presentasjonsfasen. Etterforskning av digitale bevis ble gjennomført av dataetterforskere med politi- eller sivil bakgrunn. Deltakerne i studiet uten politibakgrunn hadde et en-dags kurs i tema som var relevant for straffesaksetterforskning.

Samarbeidet under etterforskning av digitale bevis ble regnet som mest vellykket når dataetterforsker ble involvert på et tidlig stadium i etterforskningen, og inkludert i etterforskningsteamet. Eksemplene fra deltakerne viste at andre viktige faktorer for godt samarbeid i etterforskning av digitale bevis var klart lederskap og adekvat allokering av ressurser.

Litteraturstudiet og intervjuene førte til at flere ikke-tekniske kilder til feil i relasjon til etterforskningen av digitale bevis, og de ble inndelt i fire hovedtema: Den enkelte etterforsker har ikke nødvendig kompetanse, fravær av riktig kompetanse til riktig tid under etterforskningen, bias og heuristikker og organisatoriske utfordringer, som manglende kompetansekrav og store restanser. Dette resulterte i utviklingen av et konsept hvor den nødvendige teknologiske og etterforskningsfaglige kompetansen i relasjon til Dataetterforskningsprosessen ble beskrevet.

Feil kan føre til dårlig kvalitet og effektivitet i etterforskningen, som igjen kan føre til en utilstrekkelig beskyttelse av rettssikkerheten i form av feilaktige dommer eller frifinnelser. Mottiltak mot feilkildene er foreslått på individ-, samarbeids- og organisasjonsnivå.

Nøkkelord

Dataetterforskning, Dataetterforskningsprosessen, Etterforskningssyklusen, feil, feilkilder, teknologisk kompetanse, etterforskningsfaglig kompetanse, bias, heuristikker.

List of abbreviations

BL – Basis Løsninger

CD – Criminal detective

DFD – Digital forensics detective

CFFTPM – Cyber Forensic Field Triage Process Model

ECHR – European Convention on Human Rights

ICCPR – International Covenant on Civil and Political Rights

NSD – Norsk Samfunnsvitenskapelig Datatjeneste

SDI-model – The Step-by-step Deductive Inductive approach

UNODC – United Nations Office on Drugs and Crime

5WH – What, when, why, who, where and how

List of figures

1. INTRODUCTION

Digital devices and the Internet are important parts of many people's lives today. A vast amount of daily activities leave digital traces behind. These digital traces are often crucial pieces of evidence when the criminal investigation puzzle is laid.

The ultimate goal of any criminal investigation is to uncover and present the truth. Here, the concept of "truth" means a reconstruction of past events by the evidence uncovered in the criminal investigation. Since we cannot fully reconstruct the actual truth, it is of critical importance that the evidence used to prove or disprove a crime is relevant, detailed and reliable (N. Sunde, 2016).

Digital evidence is often considered reliable and unbiased. The reason for this is mainly that it is generated by machines, and not processed through the perception of a witness. However, there are several uncertainties and potential errors associated with data as evidence. This subject has been thoroughly covered in literature from a technical point view (e.g. Casey, 2002; Ekfeldt, 2016). The non-technical sources of errors seem to attract far less attention than the technical pitfalls (N. Sunde, 2016). My focus in the thesis was therefore directed towards the potential non-technical sources of errors concerning the digital evidence during the Digital Forensics Process.

1.1 Justification, motivation and benefits

The area of research was digital forensics within criminal investigation, with focus on cooperation between different professional groups, digital forensic detectives (DFD) and criminal detectives (CD).

I chose this topic because, over many years, I have witnessed detectives being assigned to tasks they probably lacked the sufficient competence to conduct in an adequately manner.

However, I have also experienced examples of cooperation between CDs and DFDs that have resulted in high quality and rapid solving of the criminal case. My motivation was to contribute to a more solid knowledge foundation that could lead to a better and more systematic use of the competence of those involved in a criminal investigation. This could hopefully lead to improved quality and efficiency in investigations where digital evidence is involved.

I hoped to identify the necessary competence components, and to find out whether these knowledge components were available at the time they were needed during an investigation. Finally, I sought to identify measures beyond solely raising the competence of the involved detectives.

Theory, approaches and methodologies from criminal investigation was discussed in relation to the Digital Forensics Process to bring new perspectives to the list of possible sources of errors when handling digital evidence – as well as possible countermeasures.

This study had a 'what works' focus. The objective was not limited to merely extending the list of sources of error, but also to highlight examples of fruitful cooperation between the two professions that might inspire others within the law enforcement. From a 'what works' perspective, this is just as important as pointing out errors.

1.2 Research problem

The research problem of the thesis was:

When handling digital evidence in a criminal investigation, do the non-technical sources of errors pose a threat towards the required quality, and eventually the rule of law?

This was based on the research problem in the preliminary study that was conducted in advance of the thesis (N. Sunde, 2016, see appendix 4). There were some adjustments. I did not only focus on the errors, but paid more attention to their *sources.* The reason was that the sources needed to be identified and countered in order to prevent the errors from occurring. I also brought in the term *rule of law* in relation to these errors. This was due to the fact that it's not very useful to identify all possible errors that may occur during an investigation, without

regard to their possible impact to the outcome of the case. Those that might pose a threat towards the rule of law should therefore have a major attention, since they may have serious consequences for the parties involved.

1.3 Research questions

To be able to answer to my research problem, some sub-problems were defined:

- Which non-technical sources of errors relevant to a criminal investigation may be identified?
- What are the consequences if these errors occur?
- How can the errors be prevented or countered?
    - At a personnel level, by the individual detective?
    - At an interpersonal level, through cooperation between detectives?
    - At an organisational level?
- Are there real-life examples which may illustrate cooperation with positive impact on the quality of the investigation?

1.4 Target group

The thesis might be relevant to detectives who have special interest towards digital evidence, or have digital forensics as their main task. The thesis might also be relevant for the CDs and DFDs, as well as the managers at the departments in the Oslo Police District, from where the participants of this study were recruited. In addition, the thesis may be relevant for students on master programs in Investigation and Police Science at the Norwegian Police University College, as well as relevant master programs at the Norwegian University of Science and Technology.

1.5 Scope of the thesis

Topics relevant to criminal investigations carried out by the police in Norway were included in the thesis. Only *open investigation* of criminal cases was part of the scope, and covert police methodologies, like covert interception of communication were left out.

The investigation tasks may be conducted until the case has received the final verdict in court. However, due to the lack of experience with presentation of evidence in court among the participants of this study, the investigation during trial proceedings or presentation of evidence in court was not included in the thesis.

I focused on the *cooperation between the DFD and the CD* during the Digital Forensics Process. Cooperation with other parties such as the forensic crime scene detective or prosecutor was not covered in depth.

1.6 Research method in brief

A qualitative research design was used, with hermeneutical-phenomenological approach. Data was gathered by interviewing 6 detectives from the Oslo Police District.

Digital Forensics Process integrated with The Investigative Cycle was used as the subject specific theoretical framework when analysing the result of the interviews in relation to relevant theory. The main theoretical subjects for the analysis were evidential requirements, criminal investigative methodology, forensic psychology and digital forensics.

1.7 Thesis outline

Chapter 2 presents the state of the art and relevant theory, such as the Digital Forensics Process, The Investigative Cycle and corresponding investigative methodologies. The evidential requirements are described, as well as biases and heuristics relevant to a criminal investigation. Finally, some organisational challenges in relation to digital forensic readiness are outlined.

Chapter 3 presents the research design and methodological approaches in this thesis. My role as a researcher, my preliminary knowledge and ethical considerations are also described and discussed.

Chapter 4 describes the results of the data collection and analysis. In chapter 5, these results are discussed in relation to the theory presented in chapter 2. The conclusions are presented in chapter 6, and relevant future work in relation to the topics subject to this thesis is presented in chapter 7.

2. STATE OF THE ART

2.1 Background and terminology

The master thesis is a continuation of my preliminary study (N. Sunde, 2016), of which chapters 1.3 (Terminology and background), 2 (The journey from information to evidence) and 3 (Evidential requirements), are included. The chapters are developed further by adding new or updated theory and references. The interviews directed my attention towards additional topics, and did also lead to further literature review, updates and additional chapters to this part of the thesis. One addition that is worth mentioning is the inclusion of the identification phase of the Digital Forensics Process, which was not a part of the preliminary study. The interviews revealed a significant amount of interesting aspects in relation to this phase, and this led to the decision of including it in the thesis.

2.1.1 Criminal investigation

The purpose is the main feature that distinguishes a criminal investigation from other police activities. In the words of Myhrer, *criminal investigation* is described as: “Criminal investigation is a purpose-oriented process with the aim of collecting information in order to clarify whether there is basis for a criminal reaction against somebody for an act that has been committed” (Myhrer, 2014, p. 14, my translation from Norwegian).

The Attorney General has set three key objectives for the criminal proceedings in the annual circular regulating the objectives and priority of criminal cases from year 2000 and up until today (e.g. Riksadvokaten, 2016a). These objectives are high clearance rate, rapid case

processing and adequate penalty. Together, these three objectives form the basis for high quality in a criminal investigation.

The objectives have been discussed by Myhrer (2014, p. 197), who somewhat disagrees with the Attorney General. Myhrer claims that high clearance rate, procedural correctness and objectivity are the three most important requirements of an investigation of high quality, and argues that as quality indictors they are clearly more important than e.g. the speediness of the criminal proceedings. This latter point is of particular interest to digital evidence, where large backlogs have been highlighted as a problem (see chapter 2.4.4).

The collection and analysis of the digital evidence is part of the investigation, and must be carried out in accordance with the Criminal Procedure Code. This means that the DFD, regardless of educational background, must comply with the same requirements as the CD when handling tasks in the criminal case. Each one of the detectives has an individual obligation to safeguard the procedural objectivity requirement stated in Criminal Procedure Code § 226, 3rd subsection.

2.1.2 Digital Forensics

An important term in this study is *digital forensics*. According to United Nations Office on Drugs and Crime (UNODC) (2013, p. 159), digital forensics can be described as "the branch of forensic science concerned with the recovery and investigation of material found in digital and computer systems". When the term 'digital forensics' is used in this thesis, it is only in relation to investigation of criminal cases carried out by the police.

The forensic standard when handling digital evidence is the Digital Forensics Process. This process is described in further detail in chapter 2.2.2.

UNODC (2013) divides digital forensics in three categories, depending on the source of the potential evidence. *Computer forensics* focuses on collecting and analysing desktop computers and laptops fond in homes or in businesses. *Mobile device forensics* is collecting and analysing low-powered mobile devices. *Network forensics* is described as collecting and

analysing evidence from online services and cloud storage, and gathering information about network traffic.

For the purpose of the analysis of this thesis, it is not necessary to distinguish between these categories, and the term ‘digital forensics’ will be used further in the thesis.

2.1.3 Law enforcement – categories and roles

According to a report by the Norwegian Police Directorate (Norwegian: Politidirektoratet), the investigation of digital evidence in Norway is handled by police officers with technological competence, or by civil engineers employed within the police (Politidirektoratet, 2012). Regardless of background, they will handle many of the same tasks concerning the investigation of digital evidence. Several of the civil engineers are also issued with *limited police authority* (Norwegian: begrenset politimyndighet). They are thus legally empowered to carry out coercive measures during the investigation, e.g. search and seizure of digital evidence.

In extraordinary situations, there is a need for extraordinary tools, software or competence. The Norwegian Criminal Investigation Service has a specialized unit of engineers that can provide assistance in such cases (Politidirektoratet, 2012).

The Norwegian Police University College has delivered interdisciplinary training within the subjects law, psychology and police methodologies since 1998 (Myklebust, 2010, p. 87). This implicates that the DFDs with police background have a basic investigative competence. The DFDs without police background would need training to gain a basic level of investigative competence.

Pursuant to Norwegian procedural law, the formal responsibility for a criminal case lies with the prosecutor, whilst the responsibility for the progress and implementation of the investigative tasks lays with the CD and his/her superior – the senior investigating officer. The CD normally has a bachelor degree from the Norwegian Police University College as a minium. The prosecutor, the CD and the DFD each have independent responsibility to act in

compliance with legal requirements and limitations. They are also responsible for contributing to an adequate progress of the investigation, and an efficient use of resources when investigating a criminal case.

A police detective, regardless of civil or police educational background, who has digital evidence handling as his/her main task will be named DFD further in this thesis.

The detective in charge of conducting the general criminal investigation will be referred to as the CD. The handling of digital evidence will often be part of the tasks of the general investigation, but not the main task of the CD.

2.1.4 Evidence – Digital evidence

UNODC defines *evidence* as well as *electronic evidence* in the aforementioned report: "Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence is all such material that exists in electronic, or digital form." (UNODC, 2013, p. 157).

Evidence is in Norwegian evidence theory described by Kolflaath (2015, p. 508) as any type of information that directly or indirectly sheds light on one of the themes of proof, or elucidates the reliability of the information or the credibility of the source of information. In this definition, evidence is related to the trial. The definition does not mention evidence that is seized during investigation, which is the focus in the thesis. Importantly, evidence can have different evidential value, depending on the reliability of the information and the credibility of the source. However, in this thesis the term 'evidence' will be used about items or data collected during the investigation, with the potential to be presented as evidence in court.

This is in line with the more general definition presented by Carrier & Spafford as "any digital data that contain reliable information that supports or refutes a hypothesis about the incident" (B. Carrier & Spafford, 2004, p. 2).

Legally, the physical storage medium and the computer data are different objects. For this reason a distinction between *seized devices* and *seized data* is made. In relation to coercive measures, the collection of the data is part of a *search* (of a physical location or a computer system),whereas *seizure* of data takes place when relevant information is uncovered and documented (I. M. Sunde, 2015, referring to Rt. 2011 p. 296 and p. 1188). In relation to the Digital Forensics Process, seizure of devices - in its legal meaning - is done in the identification phase and seizure of data, in the analysis phase. Both are coercive measures regulated by the Criminal Procedure Code.

2.1.5 Errors

The errors addressed in this thesis origin from non-technical sources, and are of a different kind than technical. They might be found in many different forms. Examples of errors that may occur in a criminal investigation are misinterpretations of the meaning, value or reliability of a piece of evidence, a biased decision, or essential evidential information being overlooked.

Errors that occur in a criminal investigation might alone, or in junction with other circumstances constitute *errors of justice*. Errors of justice are described as “any departure from an optimal outcome of justice for a criminal case” (Forst, 2004, p. 4). This is a very general and broad definition of errors. In this thesis, the focus will be on the errors that may conflict with the principle of *fair trial* stated in the European Convention on Human Rights (ECHR) (see chapter 2.2.1) or may lead to such poor quality of the investigation that the rule of law is at stake in the form of both wrongful convictions and acquittals.

In order to detect, avoid or prevent the errors from occurring, the sources of these errors must be uncovered during the investigation. If they stay undetected they might eventually pose a risk towards the rule of law, since there is no guarantee that the errors will be uncovered

during trial. In the thesis, a number of non-technical sources of errors that may occur during the investigation will be described and discussed, as well as several countermeasures.

2.1.6 Competence

The terms *knowledge*, *skill*, *expertise* and *competence* will be used to a great extent in the thesis. To distinguish between the meanings of these terms in relation to this thesis, they should be explained in further detail.

In this thesis, *knowledge* refers to theoretical competence. The term *skill* refers to the cognitive or physical ability to carry out a task with pre-determined results. *Expertise* is characterized by "special abilities that only some people possess, in contrast to others who are not experts – the novices – who cannot perform to the levels of experts" (Dror, 2011, referring to Dror et al., 1993). This definition is quite general, so in the thesis, the term expertise refers to the combination of knowledge and skills on a higher level due to extensive experience in addition to the other components. The term *competence* is used as a general umbrella term for the terms knowledge, skills and expertise, in situations where distinction is irrelevant. So, when the term *technological competence* is used, the competence is of technical type, but of undefined "size". The reason being that distinguishing between different levels of technological competence is not relevant to solve the research problem of the thesis.

2.2 The journey from data to evidence

Integration of the human:computer aspects in a criminal investigation with digital evidence requires a combined application of the Digital Forensics Process and The Investigative Cycle.

The Digital Forensics Process is the forensic standard to obtain and use data as evidence. It is a series of steps to handle data in compliance with important principles with the purpose to present the data as evidence in court.

Data can be understood as an object. To make sense as evidence, this object is dependent of the human factor, which allows the data to be discovered, interpreted and related to a meaningful context, and thus be understood as evidence (I. M. Sunde, 2015, p. 607).

To include the human factor in the Digital Forensics Process, the data must be analysed in the context of a criminal investigation, where The Investigative Cycle is an acknowledged process description for handling information during investigative tasks (Fahsing, 2016).

To serve as evidence, data must fulfil the *evidential requirements*, which are defined in The Penal Code.

The evidential requirements will be described in this chapter. The procedural steps of the Digital Forensics Process and The Investigative Cycle will then be outlined, in relation to research that applies to these process descriptions. The Digital Forensics Process integrated with The Investigative Cycle will later represent a subject specific theoretical framework for my analysis of the potential non-technical sources of errors when handling digital evidence in a criminal case.

2.2.1 Evidential requirements

As the thesis concerns criminal investigation in Norway, a brief description of the main evidential requirements in Norwegian law is necessary.

A criminal investigation must be conducted in accordance with human rights (ECHR) and the regulations in International Covenant on Civil and Political Rights (ICCPR, 1966). These regulations imply that a person charged for a crime is entitled to a *fair trial*. This means i.e. that the charged person should be allowed contradiction. In order to secure the right to contradiction the charged person has a right of access to the case documents. Such access must be provided at the stage of preparation of his/her defence at the latest (Kjelby, 2015).

The principle of *presumption of innocence* means that a suspect of a crime shall be considered to be not guilty unless or until guilt is proven according to the applicable legal evidentiary standard. According to this standard guilt must be *proven beyond any reasonable doubt*. This is an important principle stated ECHR article 6 no. 2, but is also implemented in the Norwegian Constitution § 96, 2nd section (Grunnloven, 1814).

In order to sentence an individual of a crime, the judge must be convinced about the question of guilt, and any reasonable doubt must be to the advantage of the defendant (Kjelby, 2015).This presupposes that the criminal case is investigated sufficiently, concerning both evidence against or to the benefit of the defendant.

In the trial the state, represented by the prosecutor, carries the *burden of proof*. The person charged for a crime has the right to remain silent through the trial (Kjelby, 2015).
The parties are entitled to present the evidence they wish, as long as it is relevant to the merits of the case. The scale and scope of the presentation of evidence shall be reasonably proportionate to the importance of the case (Kjelby, 2015).

In order to be convicted of a crime, the four general conditions for *criminal liability* must be fulfilled:

1. The objective conditions: The act must be rendered criminal according to law.
2. The subjective condition: The individual must have acted with intent. Negligence is sufficient only if the law explicitly says so.
3. The individual must be personally criminally capable, i.e., by being above the minimum age, and not be mentally incapacitated.
4. There must not be circumstances which render an otherwise criminal act lawful, such as emergency or exigent circumstances (I. M. Sunde, 2017).

Myhrer describes the purpose of criminal investigation to be “to obtain necessary information required to handle the criminal case during the prosecution stage, the adjudication stage and the stage of the execution of sentence” (2001, p. 4, my translation from Norwegian).

According to Criminal Procedure Code § 226, 3rd subsection (Straffeprosessloven, 1981), the investigation must be carried out in an *objective* manner. If the criminal investigation can conclude that a punishable offence has been committed, and the investigation has uncovered a

suspect of the crime, the investigation must seek to identify any mitigating or aggravating circumstances. These circumstances are listed in the Penal Code §§ 77 and 78 (Straffeloven, 2005).

To summarize, the principles of fair trial and presumption of innocence as well as the evidential requirements places great demands on the criminal investigation. This is because the judge cannot convict until s/he is convinced beyond any reasonable doubt about that the defendant is guilty of the crime s/he is charged for.

2.2.2 Digital Forensics Process

The Digital Forensics Process is developed over many years, and is described in several forms and degrees of detail (Casey, 2011, p. 188). I have chosen the model described by Flaglien (2017). From my experience and knowledge, the model fits well with investigation of digital evidence within the Norwegian police.

The phases of the Digital Forensics Process version I have chosen are *identification, collection, examination, analysis* and *presentation* (Flaglien, 2017).

The Digital Forensics Process supports a sound and structured investigation of digital evidence, by handling the carrier of the potential digital evidence (e.g. digital devices such as a mobile phone or a thumb drive) as well as the digital evidence itself (the data) in compliance with important principles (Flaglien, 2017). The principles are *Evidence integrity* and *chain of custody*.

The principle of *Evidence integrity* aims at preserving the evidence in its original form without any intentional or unintentional changes (Casey, 2011; Flaglien, 2017; Hamremoen, 2016). The principle of *Chain of custody* supports the former, and means that every contact with the physical and digital evidence should be accounted for to prove the authenticity and integrity (Casey, 2011; Flaglien, 2017; Kruse & Heiser, 2002). By following these principles, it is possible to prevent introduction of error, and thus generally undesirable *evidence*

dynamics (Casey, 2011). *Evidence dynamics* is "any influence that changes, relocates obscures or obliterates evidence regardless of intent between the time evidence is transferred and the time the case is resolved" (Casey, 2011, p. 27).

The Digital Forensics Process phases will be described in more detail below.

2.2.2.1 The identification phase

In the identification phase the DFD will, based on a set of preliminary hypothesis, try to identify digital devices or systems that might contain relevant information to the case. This might be potential evidential sources located on the search scene – as well as other physical or virtual locations. When the evidence has been identified, it must be preserved. This is done by isolating, securing and documenting the physical and digital evidence (Flaglien, 2017).

On the search scene, *preview* might be used for different purposes. Preview is a preliminary examination of the digital device without altering the content. To safeguard the integrity of the potential evidence under this examination, a physical or software based write blocker is used. The reason for previewing the content of the digital device may be e.g. to have a better basis for decision about seizure, or to look for specific content that might be evidence of a criminal act.

2.2.2.1.a) At the search scene – two models

The Cyber Forensic Field Triage Process Model (CFFTPM)

This model, described by Rogers, Goldman, Mislan, Wedge & Debrota (2006), is designed for the investigative processes that are performed within the first few hours of an investigation. Due to the information that needs to be obtained within a relatively short time frame, the model usually involves an on- site/field analysis of the computer system(s) in question.

The foci of the model are to find usable evidence immediately, identify victims at acute risk, guide the ongoing investigation, and accurately assess the offender's danger to society.

> The Cyber Forensic Field Triage Process Model (CFFTPM) proposes an onsite or field approach for providing the identification, analysis and interpretation of digital evidence in a short time frame, without the requirement of having to take the system(s)/media back to the lab for an in-depth examination or acquiring a complete forensic image(s). The proposed model adheres to commonly held forensic principles, and does not negate the ability that once the initial field triage is concluded, the system(s)/storage media be transported back to a lab environment for a more thorough examination and analysis. (Rogers et al., 2006, p. 27)

The model has several limitations in relation to efficiency. When the volume of the digital evidence is large, using this model might lead to a lengthier stay on the search scene. The model also requires a DFD to be performing the field triage. In addition, the full analysis would normally not be performed on the search scene, and the digital evidence would have to be transferred to a central location for continuation and completion of the analysis. An attempt to improve these limitations has been done in the model presented in the next chapter.

Digital Field Triage Member

Hitchcock, Le-Khac, & Scanlon (2016) have suggested a different approach based on the four phases of the aforementioned CFFTPM model. In this approach, the field triage should be carried out by trained front-line personnel, called Digital Field Triage Member. This approach is built on three important requirements to compensate for the knowledge gap between the Digital Field Triage Member and the forensic analyst (in relation to this thesis, the DFD): The Digital Field Triage Member:

- Cannot work in isolation and must work with a parent DFD.
- Must maintain the forensic integrity of the digital evidence.
- Should make an assessment, but it does not replace an analysis by the DFD.

In the approach the Digital Field Triage Member provides assistance as a resource person to the investigative team in the initial stages of the investigation, such as when planning a

search. The Digital Field Triage Member should therefore have access to all important case knowledge.

On the crime scene the Digital Field Triage Member should identify the potential digital evidence. After prioritizing, the Digital Field Triage Member should conduct an assessment of the digital evidence using an approved tool and methodology approved by the DFD. The approved tool; dependant of the customization; could create a list of recent attached items, user accounts, documents, preview images, determine if encryption is used, view internet history etc.

The Digital Field Triage Member should determine if the artefacts extracted and observed meet the required threshold for further analysis by the DFD, and decide upon seizing the device or not. After seizing the relevant digital devices, the Digital Field Triage Member should write an observation report, which is neutral - with no subjective opinions about the observations. This report contains the listed artefacts, a list of the searches they carried out and the Digital Field Triage Member's notes on the observations.

2.2.2.2 The collection phase

In the collection phase, *acquisition* of the data is done. Acquisition means to be copied, if possible – bit –by –bit, using appropriate methods and techniques. This is done to safeguard the integrity of the evidence. This approach also preserves information which has been deleted prior to collection of the evidence. Even though the information is not reachable from the file directory, the information can still be located and recovered on the digital device. Such information might be crucial to a criminal investigation. An important part of the collection phase is to consider the *order of volatility*. This means that data acquisition from one data source in a live computer may change the data in another, and the DFD must be able to prioritize between the potential evidence sources according to the volatility of the data (Flaglien, 2017).

2.2.2.3 The examination phase

Examination is described as “Preparation and extraction of potential digital evidence from collected data sources” (Flaglien, 2017, p. 35 referring to NFSTC, 2009; Carrier & Spafford, 2004). During this phase, the evidence is prepared for the analysis phase. The examination often involves restructuring and pre-processing of the raw data to make it “readable” for a DFD in the upcoming analysis (Flaglien, 2017).

2.2.2.4 The analysis phase

The analysis phase is “The processing of information that addresses the objective of the investigation with the purpose of determining the facts about an event, the significance of the evidence and the person(s) responsible” (Flaglien, 2017, p. 42 referring to Yusoff, Ismail, & Hassan, 2011). In this phase, the information is open and available, ready to be analysed.

2.2.2.4.a) Analysis sub-phases

The Oslo Police District (Oslo Politidistrikt, 2017, p. 8) has divided the analysis of digital evidence in two different concepts; content analysis and technical analysis. This distinction was used by the participants of this study, and will be referred to in chapter 4.

Content analysis means to identify and document information that contains potential evidence from electronically stored data. This might be to determine whether there are images of sexual abuse of children among the data, to export the relevant information and document it in reports.

Technical analysis means to examine, verify and evaluate the quality of technical data that contains relevant information to the criminal case. This might be to examine when and where the illegal image was taken, and with what camera.

Casey (2016, referring to Pollitt) refers to a model where the technical analysis is divided in two parts: technical process and evidence evaluation. The purpose is to make a clear distinction between activities that require quality management systems and an accredited lab

environment – and those which don't require such premises. This distinction could help to avoid problems associated with unqualified detectives attempting to evaluate digital evidence without the required competence.

Technical process means activities with verifiable outcomes, which implicates they can safely be performed outside an accredited laboratory. These activities may be e.g. making forensic copies of digital evidence, extracting active and deleted files, determine whether illegal material is on the evidence file with digital signature searches, decrypting data or scanning for virus.

Evidence evaluation means to determine accuracy, causation, linkages, spoliation and meaning within the seized data. This might be done by answering questions like: Who downloaded the illegal file to the computer? What camera was this digital image taken with? Was evidence on this computer deliberately destroyed? The reason for defining evidence evaluation as a sub-phase of the analysis phase is: "Addressing such questions involves interpretation and evaluation of digital evidence, which requires higher levels of knowledge specialization, process formalization, testing implementation, research foundation and quality oversight" (Casey, 2016, p. 2). Evidence evaluation should be done in an accredited laboratory with proper quality managements systems such as peer review in place.

In chapter 5, I will refer to three *sub-phases* of the analysis phase. The above distinctions between technical process and evidence evaluation by Casey will be used, since they are more accurate in relation to which tasks they refer to than the categorization from the Oslo Police District. The concept of content analysis from the Oslo Police District will be included, since it covers a task which requires a different competence than the other two by Casey. Together these will form three sub-phases of the analysis phase. For the purpose of clarification, some changes to the names have been done:

Technical analysis – which includes the activities included in the *technical process* mentioned by Casey (2016, referring to Pollitt). This sub-phase is more limited than defined by the Oslo

Police District, and includes only the technical tasks with verifiable results, e.g. comparing an image to a digital checksum, and concluding whether there is a match.

Content analysis - as described by the Oslo Police District (2017).

Digital evidence evaluation, referring to *evidence evaluation* as described by Casey (2016, referring to Pollitt). I have added the word 'Digital', to be able to make distinctions from evaluation of other lines of evidence in a criminal investigation.

2.2.2.4.b) Mandate for the analysis

When digital devices are seized, the CD and DFD must decide how the analysis should be conducted – by whom, and with what scope. This may be done by forming a mandate.

A mandate can be defined on different levels, e.g. narrow and targeted or wide and general. It may form the basis for an objective analysis approach as well as a partial one.

A mandate which is too narrow might increase the risk of tunnel vision (Ask, 2013, referring to Findley & Scott, 2006). If the DFD receives a mandate that, for instance, describes the aim of finding all evidence that could confirm that a suspect was sharing stolen credit card information, there is a risk that the DFD would not search for the opposite, or maybe overlook signs of innocence or mitigating circumstances if they occurred. Ekfeldt (2016, p. 271) warns against formulating mandates on activity level, for example to search for evidence which links a particular person to a criminal act.

On de other hand, a mandate which is too wide, may be problematic in relation to the speediness or quality of the investigation. It might lead to a lengthy and unfocused analysis phase, and pose a risk for those evaluating the evidence, e.g. the prosecutor, to interpret the mandate themselves – and consequently make a wrongful conclusion about the meaning or value of the evidence (Ekfeldt, 2016, p. 273). A wide mandate might also cause false negatives (Ekfeldt, 2016). An unfocused search for evidence might lead to conclusions about

information not being present among the data on the seized digital device. According to the Norwegian Police Directorate, a too wide mandate is not uncommon in the Norwegian police (Politidirektoratet, 2012).

After the DFD and CD have agreed upon the mandate, this should be documented in written form, and also be described in the analysis report. The mandate – and what the DFD actually did to carry it out is relevant for evaluation of the evidence (Ekfeldt, 2016, p. 271).

A working group founded by the Norwegian Police Directorate found that the DFD often performed all the steps in the Digital Forensics Process from identification to presentation, without a clear mandate about the aim of the analysis. This was not considered efficient compared to when the CD defined a specific task or purpose with the analysis (Politidirektoratet, 2012). Ekfeldt (2016, p. 272) found similar results in his study of Swedish police.

2.2.2.5 The presentation phase:

2.2.2.5.a) Reports

In the presentation phase, the findings from the analysis phase are presented in reports. These reports are available for the parties with legal interest in the case (Flaglien, 2017), who might be e.g. the CD, the prosecutor, the defence lawyer or the court.

According to the General Instructions for the Police (1990) (Norwegian: Alminnelig tjenesteinstruks for politiet) article 7-6, 2nd subsection, the detective must provide documentation of all information s/he discovers that might be of interest to the police.

Writing reports is an important part of the education at the Norwegian Police University College, and the police students practice this skill over three years (Politihøgskolen, 2016). The book “Politirapport” (Bjerknes & Williksen, 2015) does not cover how to write reports from investigation of digital evidence in particular. The post graduate education “Videreutdanning for Nordic Computer Forensic Investigators Introduction Module 1”

(Politihøgskolen, 2012), which is relevant to the background of the participants of this study, does not provide training in this skill. However, the more advanced education "Videreutdanning for Nordic Computer Forensic Investigators Module 2" (Politihøgskolen, 2013) provides various training activities towards writing reports. These educations are available to both CDs and DFDs employed by the police.

2.2.2.5.b) In court

The investigation forms the fundament for the evidence adduced at trial, and lasts, at least in principle, until the case has received the final verdict in court.

In court, evidence can be presented in different ways, depending on the type of evidence. Document evidence (e.g. exported emails, images, text documents) is handed out to the parties and read/presented by the prosecutor. If necessary, the physical device that was the source of the evidence (e.g. mobile phone, laptop) might be presented for visual inspection by the court. Witnesses – including the DFDs, give their testimony orally. Physical evidence is brought to the courtroom or presented through pictures. The DFD is often asked to present the findings documented in the analysis report orally, and might be allowed to use a presentation to visualize the findings.

To facilitate the best possible assessment of the evidential value, and a clear understanding of whether the evidence indicates guilt or innocence, it is crucial that the findings are presented in an understandable manner both in police reports and in court. The possible errors in relation to presentation of digital evidence in court will not be discussed further due to the scope of the thesis (see chapter 1.5).

2.2.3 The Investigative Cycle

The Investigative Cycle refers to the handling of information in investigation of criminal cases, and is divided into 6 steps. The aim of The Investigative Cycle is to help detectives focus on the diagnostic process and strive for accuracy through the cyclic problem solving process (Fahsing, 2016, p. 20).

The first five steps were initially described by Dean (2000), who referred to them as the 5c's of investigation: *Collect*, *check*, *consider*, *connect* and *construct*. Fahsing (2016) has suggested the modification of the model into a cyclic process, and to add a 6th C – *consult* - to Dean's model. The rationale is that, to be challenged by-, or to get a second opinion from a colleague might prevent errors of justice caused by bias (Fahsing, 2016; Riksadvokaten, 2015, p. 497). This college might play the role as the *Devil's Advocate* (see chapter 2.3.5), which is a recommended countermeasure to prevent confirmation bias (Christianson & Montgomery, 2008).

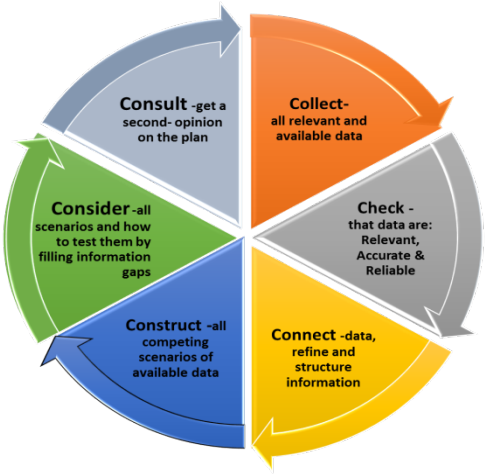


Figure 3-1: The Investigative Cycle (Fahsing, 2016)

I consider The Investigative Cycle to be relevant for discussing the need for investigative competence to prevent errors in relation to the steps of the Digital Forensics Process. The fundament of all The Investigative Cycle's procedural steps are the *5WH*: what, when, where, who, why and how, also named The Investigative Star (Tilstone, Hastrup, & Hald, 2013). The Investigative Cycle is particularly relevant to the identification, analysis and presentation phases, where investigative steps are carried out to answer the 5WH questions relevant to the investigation (N. Sunde, 2016).

The generation of hypotheses in The Investigative Cycle is based upon abductive logic, which was first described by C.S. Pierce as an addition to inductive and deductive logic in science. Abduction is carried out by forming and testing hypotheses to find the best possible guess about what the end result of the experiment or research may be (Tilstone et al., 2013). Fahsing and Rachlew (2015) state that the methodology in a criminal investigation and the quality of information obtained through this, will normally not enable a stringent falsification of theories in (deductive) scientific sense. However, they assume that the available evidence is better tested through the abductive hypotheses based approach, than through pure inductive inference.

Abductive testing of hypotheses is also referred to as "pragmatic proof testing" (Norwegian: "pragmatisk bevisprøving"), where the goal is to determine which of the hypotheses represent the best explanation of the event (Fahsing & Rachlew, 2015, p. 227 referring to Diesen, 1994). Abduction is considered the most fertile, but least secure model of inference (Tilstone et al., 2013, p. 6), and the testing is done by both seeking information that is consistent and inconsistent with the hypotheses. The best outcome from the hypothesis testing is falsification (Tilstone et al., 2013, p. 7 referring to Popper), but this result is often unachievable in an investigation.

Any investigation starts with a reason to believe that a crime has occurred, and this forms the initial hypothesis of a criminal investigation (Fahsing, 2016). This implicates that if someone is suspected of committing a crime, a guilt-hypothesis is already established. Presumption of innocence (Grunnloven, 1814, §96) commits the police to actively investigate the opposite hypothesis; the innocence hypothesis; by eliminating the explanations consistent with innocence. This strategy is proven to prevent cognitive sources of error like confirmation bias to affect the decisions of the investigation (Fahsing, 2016 referring to Lord et al., 1984).

To use a hypothesis based approach is not a new concept within digital forensic science.

> A digital investigation is a process where we develop and test hypotheses that answer questions about digital events. This is done using the scientific method where we develop a

> hypothesis using evidence that we find and then test the hypothesis by looking for additional evidence that shows the hypothesis is impossible. (Brian Carrier, 2005, p. 4)

Casey also refers to this methodology, and states: "Carrier's Hypothesis Based Approach to digital forensic investigations (Carrier, 2006) provides an initial model which bridges digital investigation practices and computer science theory, demonstrating the role of scientific method within a digital investigation" (Casey, 2011, p. 203).

The essence of each procedural step of The Investigative Cycle will briefly be described below:

Collect: Collect all available and relevant data that could shed light to the 5WH questions of the criminal case.

Check: Consider if the data is accurate, reliable and relevant. Consider whether you have the competence to make this assessment, or if specialist support is required.

Connect: Refine and structure information. Break up in smaller information pieces, organize and visualize. Consider how the information can be understood and how different pieces of information correlate, correspond, or contradict with each other.

Construct: Identify all possible explanations/hypotheses of the available information according to the 5WH. The hypotheses should involve the worst case scenarios, as well as the possibility of innocence.

Consider: Test all hypotheses by looking for information that prove or disprove the crime. Identify information gaps. Make a plan to fill the information gaps, and log all the decisions.

Consult: Always get a second opinion. The assessor should consider blind spots and whether bias has affected the investigation. The purpose of the step is to remind the detectives to get a critical view on their decisions, and/or get new declarative knowledge (Fahsing, 2013, 2016). This step is relevant to the measure 'Devil's Advocate' (see chapter 2.3.5).

2.2.4 Cooperation - The missing link between the Digital Forensics Process and The Investigative Cycle

Within a criminal investigation, every step of the Digital Forensics Process requires technological competence. However, several of the steps requires additional competence in order to safeguard the potential value of the evidence, as well as making it understandable to the prosecutor, other detectives, and other parties with legal interest in the case, like the defence lawyer.

Myhrer (2014, p. 118) states that an important factor for success in an criminal investigation is good cooperation between the CD, the DFD, the senior investigation officer and the prosecutor. The working group behind the report "Politiet i det digitale samfunnet" (Politidirektoratet, 2012) found that this way of handling the analysis was reported to be less time consuming, and provided "good evidence" (my translation from Norwegian) to the case. It was also pointed out that such a way of organizing the work increased the competence of all who were involved.

A general description of cooperation between the CD and DFD during investigation is found in the book "Etterforskningsmetoder", which is syllabus at the bachelor police education at the Norwegian Police University College:

> It is essential that there is a good information flow between those who pursue ordinary tactical and technical investigation, and the experts in analysis of digital evidence. If the person who performs an analysis of a PC does not know why the PC is analysed, important potential evidence may be overlooked. (...) However, it is equally important that the person performing the analysis manages to account for the results of the analysis in such a way that others understand what the content means. (Bjerknes & Johansen, 2009, p. 293, my translation from Norwegian)

A challenge with the Digital Forensics Process and The Investigative Cycle is that they hardly include any description of when and how cooperation with relevant competence should be carried out. The exception is the step *consult* from The Investigative Cycle. This is a general

reminder, but does not guide the DFD or the CD on when during the Digital Forensics Process these consultations should be done.

In the literature review of digital forensics science and I have not found a model describing this in a sufficient manner. The FORZA model (Casey, 2011, p. 197, referring Ieong, 2006) describes the different roles and responsibilities in a digital investigation – but does not outline when during the Digital Forensics Process the cooperation is required.

2.3 Bias and heuristics when handling digital evidence

Bias and heuristics represent a threat to the objectivity of every detective taking part in the investigation of a criminal case. Some psychological sources of errors that are particularly relevant for detectives performing criminal investigation of digital evidence will now be described.

2.3.1 Bias

Bias is "the impact of the subjective factors on our perceptions that lead to systematic errors in our judgments of the reality" (Christianson & Montgomery, 2008, p. 110, my translation from Swedish). It might lead to improper testing of hypotheses, and introduce errors into the investigation (Ask, 2013).

In relation to criminal investigation, *confirmation bias* is very relevant (Fahsing, 2016, referring to Lord et al., 1984). This is one of the most common biases, and appears in two different ways. When testing a hypothesis, a detective will have a tendency to look for information that corresponds with the hypothesis. And, when information is ambiguous and open to more than one interpretation – the detective tends to choose the interpretation that corresponds with the opinion with the hypotheses s/he believes in the most (Ask, 2013).

Bias might cause *tunnel vision*, which means that the detective solely focuses on one hypothesis or one suspect, ignoring other possible hypotheses or perpetrators (Ask, 2013, referring to Findley & Scott, 2006).

The risk of confirmation bias is influenced by situational factors like time pressure, which often can be present during a criminal investigation. The detective's emotions like confidence, frustration, sorrow and anger, personal responsibility, concern about future consequences are also factors that increases the risk of confirmation bias (Ask, 2013).

Bias is covered in relation to Digital Forensics Process by Casey (2011, p. 54), who emphasizes the importance of being unbiased and open minded, and the importance of falsification of hypotheses to reduce the risks of error. He also warns against preconceived theories based on former experience. This might cause the DFD to overlook or misinterpret the information, and lead to unfounded conclusions.

Group think is "the reluctance to think critically and challenge the theory that dominates within the group of human actors" (Fahsing, 2016, p. 30). If the DFD is working in close cooperation with the investigation team, there is a risk of this bias to occur. To avoid group think from occurring, it is necessary to be aware of the risk of this bias, but also to initiate countermeasures to prevent it.

Another important bias to be aware of during criminal investigation is *overconfidence*. Fahsing (2016, p. 29, referring to Adams & Adams, 1960) describes overconfidence as a tendency to overestimate one's own capabilities, and to have a too strong confidence in one's own knowledge and judgements. This bias might lead to poor decisions. Due to wishful thinking as a result of this bias, even highly mistaken decision-makers may remain confidently optimistic about their future decisions and remain unaware of the need to improve their thinking (Fahsing, 2016, p. 30, referring to Armor & Taylor, 1998). Overconfidence about one's own knowledge is a cognitive barrier. This has obvious parallels to the term *the illusion of explanatory depth*, which means you think you fully understand something that you actually don't (Mills & Keil, 2004). It might be relevant to relate overconfidence to the development of competence, which Burch (1970) describes to happed in four steps:

Unconscious incompetence, conscious incompetence, conscious competence and unconscious competence. Overconfidence fits well with the first step unconscious incompetence.

2.3.2 Heuristics

Heuristics are described by Ask (2013) as cognitive strategies for simplifying the handling of vast amounts of information. These strategies are helpful in the everyday life, but might also lead to systematic errors.

So-called *availability heuristic* is relevant to criminal investigation. This heuristic relates to the availability of relevant information in the long-term memory of the detective is used as a guide for determining probability. The easier we can recall examples of incidents of the same nature - the greater we consider the probability that they will occur again (Ask, 2013, p. 156). The *feature-positive effect* is a related effect to availability heuristics. It implicates that the presence of instances, more than their absence, influence our decisions, hence the saying 'out of sight, out of mind'(Fahsing, 2016, p. 25, referring to Smedslund, 1963; Jenkins & Sainsbury, 1969). This heuristic is particularly relevant during searches when decisions about seizure are done (see chapters 2.2.2.1, 4.5 and 5.2.2.2).

2.3.4 The paradox of expertise

Within the fields of digital forensics as well as criminal investigation, the detectives may develop *expertise* (see chapter 2.1.6).

Expertise is often associated with special abilities and enhanced performance, which is a correct – but one-sided presumption. There has been less attention drawn towards the downsides of expertise, which implicates that performance may be degraded, culminating in a lack of flexibility and error (Dror, 2011, p. 1).

Dror, who has done research of expertise from a cognitive neuroscientific perspective states that expertise comes with a price.

> Understanding the 'paradox' that as we become experts, we are more susceptible to contextual influences and bias because we take more 'short-cuts', rely on past experience, attend to

> information more selectively, and a whole range of cognitive mechanisms that make up expertise. (Dror, 2013, referring to Dror, 2011)

Along with the physiological changes in the brain when developing expertise, there are psychological pitfalls affecting the expert. An expert is more susceptible to confirmation bias, and over-confidence (Dror, 2011, referring to Dror, 2008; Rossmo, 2008).

Forensic analysts are during investigations routinely exposed to information that is not related to their examination of evidence. This information is not documented in their reports, but is affecting the interpretation of forensic science evidence (Edmond, Tangen, Searston, & Dror, 2015). Research has shown that contextual information about the case could sway the decision-making when forensic science evidence is produced, hence the term *contextual bias*. The contextual bias could also be relevant when investigating digital forensic evidence.

A problem with bias and heuristics is that they may cause errors in relation to the evidence produced by the detective. In addition, forensic evidence may cause an increasing snowball of bias, and thus affecting other lines of evidence in the criminal case. This is called *cross-contamination of evidence* (Edmond et al., 2015). For example, a forensic examiner looking at bite marks may be influenced and biased during the examination if they know that fingerprint or DNA evidence indicates that the suspect is guilty (Edmond et al., 2015). In a digital forensics perspective, a DFD might be influenced and biased in the examination of the suspects' computer if other evidence indicates guilt.

2.3.5 Countermeasures against bias, heuristics and expert limitations:

Whether you gain theoretical knowledge about bias or learn from experience, awareness is not an adequate countermeasure to prevent biases to occur. Several countermeasures should be initiated to avoid errors caused by bias (N. Sunde, 2016, referring to Ask & Granhag, 2008).

An important countermeasure to prevent bias is to make a written plan for the investigation containing the competing hypotheses relevant to the investigation (Rachlew, 2009).

The Devil's Advocate has proven to be an important measure to prevent biases to affect decisions (Fahsing, 2016, referring to Herbert & Estes, 1977; Schwenk, 1990). The person given this task should challenge the proposed judgement by building the strongest possible case against it (Heuer & Pherson, 2015, p. 261). This countermeasure is also recommended in literature in several courses by the Norwegian Police University College (e.g. Bjerknes & Johansen, 2009, p. 72; Christianson & Montgomery, 2008, p. 108; Heuer & Pherson, 2015, pp. 260-262). This should also be the mind-set of the person acting as the critical counterpart in the step *consult* in The Investigative Cycle (Fahsing, 2016).

As mentioned in chapter 2.3.4, experts are susceptive to cognitive limitations, due to the expertise itself. To compensate for the tendency to make short-cuts, rely on past experience and select information that may lead to errors, checklists have been found to reduce errors for doctors and pilots (Gawande, 2010). Checklists may be a relevant measure to support the digital forensic experts as well.

To prevent contextual bias, a suggested approach is Linear Sequential Unmasking, which is described (Dror et al., 2015). In this approach, one would initially restrict what information the forensic analyst should receive, and allow him/her to produce initial findings without the risk of contextual bias. After forming initial hypotheses, the analyst would get access to the additional evidence of the case and other contextual details to ensure that important evidence is not overlooked. This approach is discussed in chapter 5.4.

2.4 Organisational challenges in relation to handling digital evidence

2.4.1 Readiness

Readiness is defined as: "The ability to perform digital investigation with minimal cost, while maximizing the usefulness of evidence" (Dilijonaite, 2017, referring to Tan, 2001). This principle applies best in relation to private companies, but is also relevant to law enforcement where cost is a constant concern. However, in a criminal investigation quality will often be of higher priority than speediness (Riksadvokaten, 2016a), which is closely related to cost.

In terms of *digital forensic readiness* there are several dimensions, e.g. legal, policy, processes and procedures, people, tools and infrastructure. Further in this chapter a few of these dimensions that are relevant to my research problem will be touched upon. Some dimensions that are considered relevant to the Norwegian police are the lack of competence requirements, organisation of digital forensic investigation in relation to structure and culture, and challenges with backlogs.

2.4.2 Challenge: Competence requirements

To handle digital evidence within a criminal investigation in Norway, one is not required to hold a certain level of competence, neither with respect to technological or investigative competence.

The aforementioned working group founded by the Norwegian Police Directorate (Politidirektoratet, 2012) surveyed who was handling digital evidence in the police. One finding was that the DFDs in the Norwegian police districts were either an engineer with no police education, or police officers with technological education and/or competence acquired through experience.

In relation to the Digital Forensics Process, the working group found that identification and collection of the physical device containing potential digital evidence was often done by a regular CD, with no particular competence in relation to digital evidence. The assistance of a DFD depended on the planning of the operation and whether the operation was carried out during regular office hours.

The Norwegian Police Directorate has stated that “collecting digital evidence requires appropriate competence and must not be carried out by personnel without adequate training, technical equipment and software” (2010, p. 5, my translation from Norwegian). The Norwegian Police Directorate has not given a further description of what “appropriate competence” or “adequate training” means.

The Norwegian Police Directorate established new functions in the new police districts in 2016 (Politidirektoratet, 2016). The functions in relation to handling digital evidence were described, and included different levels of complexity, from basic to expert tasks. The descriptions are task focused, and competence is not mentioned, hence "adequate training" and "appropriate training" are still not outlined or clarified. The function description for a DFD, named Data detective / Special detective - police or technologist - (Norwegian: Dataetterforsker / Spesialetterforsker, - politi eller teknolog -) is:

- Support the criminal investigation with competence through close cooperation in the cases where this is required.
- Perform advanced collection of digital evidence under search/seizure, crime scene investigation, coordinated tasks (Norwegian: aksjoner), etc.
- Facilitate the analysis conducted by the CD.
- Conduct analysis of collected material – with the use of sufficient tools – independent of complexity/data structures.
- Be a professional advisor for other units within the police district.
- Through carrying out the tasks, document new methodology and knowledge.
- Participate in the development and implementation of training for the DFD liaisons and frontline personnel. (Politidirektoratet, 2016, pp. 100-101, my translation from Norwegian)

However, as one of several measures related to the national strategy to combat digital crime (Justis- og beredskapsdepartementet, 2015) there is an ongoing pilot project in the Oslo Police District (Oslo Politidistrikt, 2017) where one of several tasks is to recommend competence requirements for personnel handling digital evidence. The pilot project is scheduled to be completed ultimo 2017.

2.4.3 Challenge: Culture and structure

As of 2016, the 27 Norwegian police districts were reduced to 12. The reorganisation merged several Computer Crime Departments into larger units.

The detectives handling digital evidence are included in the aforementioned functions of the new police districts (see chapter 2.4.2). A brand new function is the *DFD liaison* (Norwegian: Fagkontakt), which will have the following tasks:

- Be an advisor for own unit within the subject digital evidence.
- Be a professional contact point between own unit and the function conducting digital policing.
- Be a contact point and intermediary of new methodology and new knowledge within digital evidence towards own unit. (Politidirektoratet, 2016, p. 101, my translation from Norwegian)

The police reform has led to major structural changes. In such a situation one must put special emphasis on addressing the *culture.* Within management literature, the expression 'culture beats structure' is well-known (Lloyd, 2000). This means that there is little help in introducing a good structure if the organizational culture is not in line with it. *Organizational culture* can be defined as "the set of shared norms, values and perceptions of reality developed in an organization when the members interact with one another and the environment, and expressed in the members' actions and attitudes at work" (Bang, 2013, p. 327, my translation from Norwegian).

Kowalski (1994) pinpoints culture as one of four core components for a socio-technical system to be in balance. The social part of the system consists of culture and structure, and the technical part consists of methods and machines. Every system is required to be in a balanced state to be able to reach the goals set for the system. When one of the components in a socio-technical system is changed, the other may have to change in order to preserve the balance.

2.4.4 Challenge: Backlogs

The problem of increasing backlogs, where digital evidence is waiting in line to be examined is well documented (Hitchcock et al., 2016, referring to Mislan et al., 2010; Casey et al., 2009; James & Gladyshev, 2015). The possible negative consequences of the increasing

backlogs might be one of the reasons for the following description, which concerns the status of the investigation of digital evidence in 2013:

> The police investigate digital evidence in digital storage devices in most of the serious criminal cases, but apparently not to the same extent in other criminal cases. Digital evidence on the Internet seems to little or no extent to be examined. “Network forensics” is not carried out by the police, and the police have no particular system to analyse big data. (Politidirektoratet, 2013, p. 22, my translation from Norwegian)

A more recent survey found that the problem still remains unsolved. The commission behind the survey stated in their report: “The Commission is aware that large backlogs of pending tasks related to electronic evidence within all types of crime may exist” (NOU 2015:13, p. 265).

3. METHOD

3.1 Introduction

The thesis is a continuation of my theoretical preliminary study (N. Sunde, 2016), and employs a qualitative methodological approach (Olsvik, 2013; Tjora, 2013). According to (Tjora, 2013, p. 207), openness about the choice of methodology and how it was carried out strengthens validity. In this chapter the theoretical framework and choice of methodology will be described and discussed. The quality of the research will be accounted for, and my role and preconceptions as a researcher will be explained.

Further, the process of selection of informants, the data collection through interviews, the transcription and the process of analyzing the qualitative data will be outlined.

3.2 Research methodology

The cooperation between the two professions - the CD and the DFD - is a relatively unexplored area of research. The aim of this study is to achieve insight into the DFDs’ and

CDs' subjective perspectives, reflections, professional judgements and experiences in connection with the process of handling digital evidence.

To explore these aspects in depth, the study builds on a hermeneutic-phenomenological theoretical framework (e.g. Kafle, 2013; Leedy & Ormrod, 2014; Olsvik, 2013). This methodology has limitations in relation to generalizability, but nevertheless, and as will be shown, the survey conducted for the purpose of data collection may contribute to the identification of variables that could be subject to further research.

3.2.1 Hermeneutic-phenomenological perspective

A hermeneutic-phenomenological study is a study that tries to understand the informant's perceptions and perspectives of a certain situation or experience (Kafle, 2013; Leedy & Ormrod, 2014). The school of hermeneutic-phenomenology differs from other schools like transcendental phenomenology i.e. by recognizing that personal opinions and interpretations cannot be excluded completely from the description of a phenomenon (Kafle, 2013). This implicates that the data from this study will be presented partly based on the informant's perspectives and partly based on my own interpretation (Creswell, 2013).

Personally, and in my role as a professional criminal detective, I believe that there is no single reality – but rather multiple realities that are constructed through our experiences and through interactions with others. My philosophical view is therefore closest to social constructivism (Creswell, 2013, p. 24). This is also a necessary belief when choosing my qualitative research approach where I seek to describe the participants' different perspectives on the topics relevant to my research questions (Creswell, 2013, p. 27).

3.2.2 Background and biases

Creswell (2013, p. 11) underlines the significance of reflexivity by positioning oneself both into the research process and in the report. This is an important part of a qualitative study in relation to reliability.

I have worked as a police officer for nearly eighteen years, and have worked with criminal investigation for most of this period. I have specialized within the field cybercrime and digital forensics for seven years, and have worked closely with DFDs through this period. Finally, I have a broad educational background in digital forensics myself. I thus consider myself to have profound knowledge in this field, acquired through formal education and professional experience. My background has influenced my interpretations and decisions during the work with this thesis. This has affected the choice of theory, the coding during the data analysis (see chapter 3.3.6), and the decision of what was considered relevant in the results.

My fundamental professional view as law enforcement officer is deeply anchored in the European Convention on Human Rights (ECHR) with fair trial and presumption of innocence as probably the most profound principles in this context. This has affected the weighing of what I consider to be necessary competence when investigating a criminal case in a manner that sustains the rule of law.

Conducting research interviews is a task that requires training (Leedy & Ormrod, 2014, p. 142). The main difference between the research interview and the police interview is the purpose. However, there are many similarities, e.g. asking open ended questions and focusing on information gathering. I have broad experience with conducting police interviews, and this was an advantage when planning and conducting the interviews in this study.

I conducted a theoretical preliminary study before the work with the thesis begun. The identified non-technical errors and the suggested countermeasures regarding digital evidence might have affected the interview guide by limiting the questions in line with my preliminary study. This could have led the participants' attention too strongly towards these topics, and biasing them to overlook other relevant issues they could have pointed out.

3.2.3 Literature review

The police education, both bachelor and postgraduate, is an interdisciplinary training. Within the subject 'Criminal Investigation', legal psychology, law and criminal investigation methodology are important topics (Myklebust, 2010). My educational background has directed the attention towards possible sources of errors in addition to those of a technical nature, and thus influenced my choice of literature.

When trying to identify non-technical sources of errors in relation to handling digital evidence, the Digital Forensics Process integrated with The Investigative Cycle was chosen as the subject specific theoretical framework. The reason behind this choice is that these are the processes the DFD and the CD would refer to. They also fit well with the way digital evidence is handled within the Norwegian police (see chapter 2.2.2).

Concerning law and psychology, I have focused on literature that is curriculum on various educations on the Norwegian Police University College, and some recent research. I have also included research from the digital forensics community relevant to my research problem.

Most of the literature was reviewed before the interviews. After conducting the interviews, several topics that were not included in my preliminary study stood out as significant, and needed to be followed up. In the preliminary study I focused only on the analysis and presentation phase of the Digital Forensics Process. During the interviews a lot of interesting information came up in relation to the identification phase as well, and I decided to include this phase in this thesis. This involved a literature review after the interviews was done. There were also topics under organizational challenges that surfaced and required further literature review.

3.2.4 Strengths and weaknesses

There are several challenges when performing research on your own colleagues or profession. According to Rachlew (2010) when an insider conducts research, s/he will know about structure, culture and language, which is time saving compared to a researcher new to the field. This was beneficial when planning the interviews because I could understand the

language connected to this type of work, and I knew the investigative procedures, strategies and tools relevant to digital evidence. This knowledge has possibly affected my ability to challenge their statements for details and clarification. On the other hand – my preliminary knowledge could also be an obstacle. It may have reduced the natural urge to follow up with questions, since some of the information they provided was well known to me. As stated by Rachlew about the insider performing research: "The greatest advantage might also represent the greatest challenge; the scope of the preliminary knowledge might be so extensive that it's barring meetings with what's new and unexpected (2010, p. 141, my translation from Norwegian).

A well-known phenomenon from qualitative research is that the researcher «goes native» by identifying him/herself with the participants of the study and losing the analytical distance to the research field and the informants (e.g. Rachlew, 2010, p. 131). Due to my preliminary knowledge and professional experience, as well as my strong commitment to this field of expertise I have payed close attention to this pitfall, to possibly prevent a decreased analytic distance.

During research, there is always a risk for the *Hawthorne effect* (Leedy & Ormrod, 2014, p. 104) which is an example of reactivity, where the participants change their behaviour because of the participation in research. This might lead to e.g. the participants seeking to give a perception of a better work performance than they would perform in reality.

3.3 Research procedure and data material

3.3.1 Sampling procedure

A typical phenomenological study includes 5-25 persons interviewed in 1-2 hours (Leedy & Ormrod, 2014 referring to Creswell, 2007). A too narrow selection poses a risk towards an incomplete picture of the phenomenon in question (Leedy & Ormrod, 2014, p. 154).

I interviewed 6 people in this study. The participants were 4 DFDs and 2 CDs. In the sample there was a mix of police and technical educational background, and also a mix of gender. Due to the scope of the thesis, more informants could have provided a broader and or more detailed information basis for the discussion. This was unfortunately not compatible with the time limit of the thesis.

According to Creswell (2013), in a phenomenological study it is essential that the candidates have experience with the phenomenon being studied. Criterion sampling was therefore selected as sampling method. The study would also benefit from a variety of backgrounds to ensure a variety of perspectives on the sub-problems. I therefore wanted a heterogeneous sample regarding background (technological - and police education).

When selecting candidates for data collection, I considered interviewing candidates from several police districts, but because of the ongoing police reform (Politidirektoratet & Riksadvokaten, 2016), there were many changes in the organisation, both in terms of personnel and organisation. I considered it likely that this situation would affect the answers about collaboration – which was an element in the sub-problems I wanted to address.

I decided upon focusing on the Oslo Police District, and two particular reasons led to this choice. Firstly; at the time of the data collection, there had been no significant organisational changes in the Oslo Police District that would affect the answers about collaboration. Secondly; because of my preliminary knowledge and experience, I knew that there were many problems to point out. I wanted to find a place where they had addressed some known issues and implemented measures to improve the situation. I wanted to focus on “what works” in this study, and the Oslo Police District stood out because of an ongoing pilot project (Oslo Politidistrikt, 2017) where they implemented a strategy with several measures to improve the quality and efficiency of the work with digital evidence.

I wanted the perspective of various professional functions (DFD, CD) handling digital evidence, but also a variation of background (technological- or police education). The criterions for the CDs were that they had worked with digital evidence, and that they had

experienced collaboration with one or more DFDs at the Computer Crime Department in the chosen Police District.

My sampling strategy was a combination of *stratified purposeful strategy* and *snowball strategy*. Stratified purposeful strategy is useful to illustrate subgroups and facilitates comparisons. Snowball strategy is used to identify "cases of interest from people who know people who know what cases are information-rich" (Creswell, 2013, p. 158).

I first contacted the Computer Crime Department in the Oslo Police District, and was given the opportunity to come and present my upcoming study. I gave a presentation of my research questions, and spoke about the above outlined criteria I wanted from my candidates. I asked them to contact me directly on email, and I got positive response from four DFDs.

The CDs were selected with a different approach. I postponed the selection of CDs until after the interviews of the DFDs were done, due to the stratified purposeful strategy. The first interviews uncovered that the Computer Crime Department had the closest cooperation with Department for Homicide Investigations and the Department for Investigation of Sexual Abuse. I decided to select candidates from these departments, since they would have the prerequisite to give a perspective on the collaboration with DFDs, and thus probably have more examples of poor and good collaboration to relate to during the interviews.

I contacted the management of the aforementioned departments, and informed them that I would like two candidates for interviews. My criterions were that they should have experience with investigating digital evidence, and had collaborated with the Computer Crime Department. I asked the management to send out my information letter, and that the candidates could contact me directly. I got one participant from each of the two departments.

3.3.2 Semi-structured interview

According to Marshall og Rossmann (2006), a semi-structured individual interview is a good approach to gain insight into the experiences and interpretations of the interviewee. The

strength of using a semi-structured interview for data collection is the inductive approach where the researcher can gain insight into issues s/he was unaware of before the interviews. Hence the method is suitable for gaining new knowledge in terms of new perspectives or greater degree of detail. The approach is based upon open-ended questions, and gives the opportunity to follow up on information the researcher had not planned for.

When the purpose of the study is to study actions and collaboration within a given context, observation would normally be the selected approach.

Initially I planned to do observations in advance of the semi-structured interviews. With this combination, I would be able to make observations of actions and collaboration, and use this as basis for the following interview. The interviews could then give insight into the interviewees' knowledge, experiences and interpretations, but in addition, I could challenge the interviewee about their perspective on concrete actions or activities.

However, the observation approach required permission from the Attorney General and Ministry of Justice and Public Security (Politihøgskolen, 2015) due to confidentiality of personal data I might come across in my capacity as researcher, during observation. The processing time of such permission was reported to be lengthy (9 months), which effectively ruled out this method as an option for the present project. I therefore decided only to use interview as data collection methodology.

I planned the interviews in line with the 7 phases described by Kvale & Brinkmann (2009, p. 122) which are *development of themes, design, interview, transcript, analysis* and *verification*. On the basis of my research questions, I developed an interview guide, which I tested on a DFD from another police district. I adjusted the questions a bit as a result of the test interview, but the themes stayed the same (see Appendix 3). My interviewees got the opportunity to choose where the interview should take place. I recorded audio from the interviews, which lasted for 2 to 2,5 hours.

To transcribe means to transform from one form to another, and in this context it means to transform from a spoken to a written language. I used Microsoft Excel in order to facilitate the upcoming analysis of the transcripts. Since I use a phenomenological approach, I transcribed

word by word to keep the information as close to reality as possible. I translated the citations to English in line with the rest of the thesis, a measure that contributes to sustain the anonymity for the participants. Each interview was transcribed completely before the analysis started.

3.3.6 Data analysis

I selected the SDI-model described by Tjora (2013, p. 175) as the approach for the analysis. The model is designed to be used upwards as a data driven inductive approach, and downwards as a theory driven deductive approach.

I started with coding in *meaning units* (Norwegian: tekstnære koder) based on the text. A meaning unit is a term that relates to the meaning of the piece of text. I then grouped the meaning units that was related to each other in *categories*. I reviewed the relevance of the data continuously in relation to my research questions, and in each of these steps some information was considered irrelevant, and left out. I ended up with 8 categories, which were

1. *Quality and efficiency*
2. E*xamples of good cooperation*
3. E*xamples of poor cooperation*
4. *Identification phase*
5. *Analysis phase*
6. *Presentation phase*
7. *Investigative competence*
8. *Organisational challenges.*

The data from these categories was gathered in four *main themes* concerning non-technical sources of error: Lack of investigative competence by the detective, absence of the correct competence when necessary during the Digital Forensics Process, bias and missing countermeasures and organisational challenges.

The information from the survey relevant to my research questions is compiled in chapter 4. Data Analysis. It is organized in line with the aforementioned categories. The results of the data analysis were then discussed in relation to theory in chapter 5. Discussion, where the main themes constitutes the main structure of chapter 5.2.

Since the number of participants was small, it was not found valuable to count the number of accounts agreeing on the different statements. If only one has mentioned something, this is reported as “one of “. If more than one – but not all have stated something similar, the term “several of” is used. If all participants have stated approximately the same, the term “all” is used.

The final step upwards in the SDI-model involves development of concepts and theory. Conceptual generalization is the goal of this model, and the researcher wants to develop models, concepts or metaphors which are not directly or solely tied to the empirical data of the study (Tjora, 2013). As a result of my analysis, I suggest a concept with an extension of the dimensions of the Digital Forensics Process in relation to criminal investigation. The extension defines the competence required to conduct each phase with sufficient quality and efficiency. The concept is discussed in relation to theory and empirical data in chapter 5. A general model can be found in 5.2.2.5 (Figure 5-2) and a detailed model of the same concept in chapter 5.2.2.6 (Figure 5-3).

Development of a concept is a natural stopping point in qualitative research of smaller scale, such as this master project. In order for qualitative research to contribute to development of theory, more resources are required, such as a project of larger scale or an assembly of projects, performed by experienced researchers (Tjora, 2013, p. 190).

3.4 Quality assurance

3.4.1 Validity

Validity can be divided into two separate terms: internal validity and external validity. Internal validity is determined by assessing whether the study has sufficient controls to ensure that the conclusions drawn are truly warranted by the data. External validity is determined by

evaluating whether the results can be used to make generalizations about the world beyond the specific research context (Leedy & Ormrod, 2014, p.103). For qualitative studies these terms are not fully applicable, and words as credibility, trustworthiness, confirmability and validation have been suggested used to replace the term validity (Leedy & Ormrod, 2014, p. 106, referring to Lincon & Guba 1985 and Creswell 2007).

Creswell (2013, p. 253) has suggested 8 procedures qualitative researchers may use to increase the validity of the research, and recommends to use at least two of them in any given qualitative study. I have used three of the approaches in this thesis: *Clarify researcher bias, peer review* and *member checking.*

Firstly, In order to give the reader a fair opportunity to assess the validity of this thesis, I have described my background and position which might have influenced the research process from start to end. This is a measure to clarify researcher bias.

Secondly, I have used peer review as a validation strategy, by seeking the advice of a colleague who is using qualitative approach in her ongoing PhD. She has acted as my Devil's Advocate, and has challenged my methods and opinions.

Thirdly, I have used member checking, by sending the quotes to the respective participants to validate the content in translated form. According to Creswell (2013, p. 252) this approach is often used in qualitative studies in order to give the participants the opportunity to judge the accuracy and credibility.

3.4.2 Reliability

In qualitative research, reliability is about the consistency and the trustworthiness of the research results (Kvale & Brinkmann, 2009, p. 271). The reliability is relevant for the interview as well as the transcription and analysis of the collected data.

In the interviews I focused on open-ended questions, formulated as neutral as possible to avoid impacting the interviewees' response. To safeguard the reliability the interviews was recorded, and a complete transcription was done before the data analysis. A weakness with the data analysis is that I conducted the coding on my own. According to Creswell (2013, p. 253) reliability often refers to the stability of response from multiple coders of the data set. To

strengthen the reliability in this process, more personnel could have been included in the coding process, to assess whether they chose similar codes and meaning units. However, this has not been a feasible option in this project.

3.4.3 Generalizability

To consider external validity, three common strategies are used. The first strategy is to check if the research is performed in "the real life world". Unlike a laboratory setting this is more applicable to other real life contexts. The second strategy is to assess if the sample is representative. The third strategy is to assess whether the research is replicable, which means that that another researcher who conducted the same study in a different context would reach the same conclusion (Leedy & Ormrod, 2014, p. 105). However, generalizability holds little meaning for most qualitative studies (Creswell, 2013).

Despite a non-representative sample, and no replicability, the result of this thesis may produce relevant and detailed information about *possible variables* that may be followed up in further qualitative or quantitative research.

3.5 Ethical considerations

The most important ethical aspects when collecting empirical data is protection from harm, informed consent, right to privacy and the right be honestly referred (Leedy & Ormrod, 2014 p. 106-108).

When planning the work with this thesis, I studied the ethical guidelines for the Norwegian Police University College (NPUC, 2015), which provided a good information basis about the duties and restrictions in relation to the research I planned to conduct. According to Personal Data Act, all projects with electronic storage or processing of personal data must report this to the relevant supervisory authority. Before the data collection started, I applied for approval from NSD (Norsk Samfunnsvitenskapelig Datatjeneste), i.e. the privacy ombudsman for the Norwegian Police University College. The approval is annexed to the thesis (Appendix 1).

An informed consent form (Appendix 2) was prepared, with information about the study, that participation was voluntary, and that they could withdraw from the study at any time. I talked

the participants through this form before the interview started, to clarify any issues they had concerning the participation. The form was signed before the interview started.

The transcribed interviews was de-identified, and stored according to applicable rules concerning personally identifiable information.

It's important to sustain the anonymity of the participants during the whole research process (Leedy & Ormrod, 2014 p. 107). The mix of gender and background could lead to participants being exposed and identified, and the gender neutral term "s/he" was used in the thesis.

4. DATA ANALYSIS

4.1 Introduction

The chapter is organized in line with the identified categories during the data analysis (see chapter 3.3.6.). The participants are referred to as either CD or DFD. In relation to gender, due to anonymity precautions all participants are referred to as "s/he" or "the participants".

4.2 Quality and efficiency

All participants were asked what they think distinguishes an investigation with good quality and efficiency. A summary of the mentioned factors are:

- *A targeted investigation*, where the involved detectives have a clear focus, and are conscious of what they are doing, and why.
- *Sufficient resources* for the investigation are allocated, which means that they (both CD and DFD) who are working on the case have set aside necessary time to prevent the case "getting cold". The amount of time reserved to the case must be adequate in relation to the extent and gravity of the case. Early involvement of the DFD is a key factor for success.
- *Good communication* is a prerequisite for good cooperation in the investigation. The DFD and the CD should have an ongoing dialogue throughout the investigation from start to end.

- The activities and decisions regarding the investigation should be *well documented*, and the documentation must be correct according to current standard.
- *Clear investigative- and prosecution management* throughout the investigation. Assessments and decisions are made at the right time and are well documented.
- The *ethical perspective* should be emphasized, so that all those who are implicated in the criminal case are treated with respect.
- The CDs and DFD' strive to *obtain and sustain objectivity*. They are open, and avoid having preconceived opinions. They are observant of subjective opinions from others. Both CD and DFD work with a hypotheses based approach, and focus on uncovering what has happened.
- Both the CD and DFD know the limitation of own *competence*. They know what to do and why, and avoid speculations. They are able to develop and apply new and updated *knowledge and skills*.

4.3 Real-life examples of good cooperation

All participants in the study were challenged to provide one or more real-life example of good cooperation between the CD and DFD in an investigation. They were asked to give the example within the context of the criminal case, and to highlight the reasons for the choice of this particular case.

A DFD told about how *adequate allocation of resources* had contributed to an effective investigation in a complicated case of trafficking in human beings. The Computer Crime Department was involved ahead of the search. The DFD underlined as a particularly positive element in this collaboration that the CDs understood that a great amount of work also had to be done after the search. The analysis of the seized information required time and effort, but also detailed knowledge of the case. It was necessary for recognizing the names, addresses or images relevant to the case. The CDs were well aware that they had to set aside time to participate in the analysis, and worked with the DFD for several weeks. The DFD also facilitated the content analysis, which was conducted by the CDs. The DFD performed the technical analysis in relation to the findings from the content analysis.

A DFD highlighted the importance of *clear leadership* in the investigation of an attempted homicide. Several DFDs were involved in the initial phase, and a coordinating unit was established. A leader from the Computer Crime Department was included in the coordinating unit, and was responsible for managing the tasks regarding digital evidence, which was carried out by the DFDs. This leader gave detailed and continuous information to the DFDs about the development in the case, and this information was essential for the investigation carried out by the DFDs. This led to that the DFD, at an early stage, searched for and recovered deleted evidence, which had great impact on further directions of the investigation. The uncovered evidence was also an important factor for solving the case rapidly.

The DFDs emphasized the importance of being *involved at an early stage of the investigation*. The advantage of this was that they could use their competence to give input when planning search and seizure, so that relevant digital evidence was seized, and that data acquisition was performed in a qualitatively good manner.

A DFD explained how early involvement yielded positive results for solving a sexual crime. The DFD was involved in the search, where the digital devices were seized and data acquisition was performed. S/he conducted preliminary analysis, and was able to provide important evidence in time for the first police interview of the suspect. The suspect was confronted with the evidence, and confessed to having committed the crime. The early discovery of this evidence led to the case being solved rapidly.

To be *included into the investigation team* was highlighted as a key success factor by a DFD. By being included into the team, s/he had experienced how they could use their competence to propose appropriate investigative measures and strategies. S/he underlined how positively they experienced the CD in charge of the investigation expressing the necessity of his/her competence, and acting open-minded to their suggestions.

Another DFD told about his/her positive experience of being included in the investigation team in a case regarding serious child molesting. They had a team-meeting where the CD, the forensic crime scene detective and the DFD were present. The aim of the meeting was to clarify what information they needed to obtain to solve the case. The DFD realized that s/he

could probable be able to solve the information problem by trying out a new and fairly experimental methodology on the seized evidence. This approach was successful, and uncovered crucial and detailed information about the period of time when the suspected child molestation had happened.

A CD used the investigation of a child-homicide as an example of how fruitful it had been to have the DFD included into the investigation team. At a point in time in this case, the investigation had reached a dead end. What eventually led to progress was information uncovered by the DFD. S/he was, in the words of the CD "the most determined mole I've ever met," who found information, which s/he checked, double checked and triple checked. The DFD had after months of analysis on the case extracted fragments of chat from unallocated area of the seized data storage. This could not technically be tied to timestamps or user information, but in the police interview, the suspect admitted to being part of the chat. This was of great importance for proving the suspects intent, and what happened the days, weeks and moth's before the child was killed.

4.4 Real-life examples of poor cooperation

All the participants provided one or more real-life examples of poor cooperation between the DFD and the CD.

Several of the examples from the DFDs were about the experience of not being included in the investigation team, or being included late. Some examples were about receiving solely technical tasks, and experiencing that crucial case information – which is prerequisite for doing a targeted analysis – was not provided, or even kept secret. Some DFDs had experienced CDs not being open to their suggested measures and strategies to collect and analyse digital evidence relevant to the case.

Other challenges that were addressed in the examples of poor collaboration were poor leadership, reluctance to make important decisions, poor communication about the progress of agreed tasks, and frequent change of the main responsible CD of the investigation of the case.

The CDs highlighted other elements in their examples. The lack of knowledge among the DFDs about evidential requirements and how evidence should be reported and presented

properly in a criminal investigation was pointed out by one of the CDs. The CD expressed frustration over not understanding the information s/he received as a result of analysis of digital evidence from the DFDs, and was worried that other parties, e.g. the prosecutor or the judge would not understand it either. S/he underlined that if the material was not presented in an understandable manner, this might be a problem for the rule of law.

4.5 Identification phase

4.5.1 Search

The DFDs all agreed upon the great importance of being involved at an early stage of the investigation – and preferably in time to be part of the planning of an upcoming search. The DFDs would sometimes suggest participating themselves, but experienced that they were increasingly more often invited to attend in the planning.

The DFDs provided several reasons for attending the planning of upcoming searches. Firstly, it was important to clarify what the investigation team wanted to accomplish by the search. This information was necessary to decide if the DFDs needed to be present at the search scene or if they could provide consultative support over telephone. Secondly; if they decided to be present at the search scene; the planning would provide information about which type and level of competence to send to the search scene, since the DFDs have different levels and areas of expertise. Thirdly; the DFD could give input on what to expect and how to act in relation to digital devices – e.g. how to deal with network connected devices, whether they should seize information stored in the cloud etc. Fourthly; if the suspect should be arrested, the DFD could give advice on relevant questions to ask in the initial interview regarding the potential digital evidence, e.g. access codes, ownership and configuration.

Although the DFDs preferred to be involved at an early stage of the investigation, this was not always possible. Sometimes the police received information that they needed act upon immediately. The DFDs tried to be prepared for these situations as well by having an equipment kit ready and packed.

Even though the DFDs had been issued with limited police authority, they had not received any training in e.g. arresting a suspect or handling a violent situation. Some of the DFDs emphasized the importance of the other team members (with police background) being aware of the DFDs limitations regarding police skills. This was because they did not expect the DFD to assist when carrying out an arrest or to be a backup if an unexpected violent situation should occur.

When performing the search, the DFD would normally lead the search of the digital evidence. The DFD would discuss what items to seize with the CD main responsible for the case, who has the final say in relation to this decision.

Early involvement in the case would also give the opportunity to perform preview (see chapter 2.2.2.1) before acquisition of the seized device. This approach had led to good results in several cases, where the DFDs had been able to provide important information already prior to the first police interview of the suspect. The CD conducting the interview could confront the suspect with the information, and this had led to the suspect confessing to having committed the crime. Information from the preview could also be important when the prosecutor should decide whether the suspect should be held in custody or released.

4.5.2 Decision about seizure

The large amount of seized devices and data seemed to have become a major challenge for the participants. Both data acquisition and data analysis required considerable resources. Several of the DFDs stated that they did not have the capacity to examine all digital devices present at the search scenes, even though they could contain relevant evidence for the criminal case.

The amount of data to be seized depended on the gravity of the case as well as the amount of data storage devices present at the crime scene relevant to the case. In homicide investigations, all digital devices would routinely be seized, and the DFD would perform data acquisition of all the seized devices. The DFDs told that they in cases of less severity, tried to limit the amount of seized data to the items they considered the most promising in terms of finding relevant evidence to the case.

The DFDs provided several examples of such predictions. One told that they would try to make a prediction based on where the digital device was found, and whether it had signs of recent usage e.g. from the amount of dust on the device. Another told about predictions based on external characteristics such as colour or name tags.

One DFD told about a case where they had discovered an enormous amount of digital storage devices. The suspicion was not very strong, and the case was not one of the most severe. They decided that they could not seize all the digital devices, but there was not any obvious way of determining which of the devices that was the most promising as potential evidence. They did some kind of statistical calculation, and decided to seize only a few of the devices.

A CD explained about a case where the suspicion concerned sharing of images of child sexual abuse. The CD participated in the search, and they found a large amount of digital devices. They decided only to seize devices that could communicate, since these were the most likely to prove or disprove the element of sharing.

4.5.3 Preview

Several of the participants told that they occasionally did preform previews (see chapter 2.2.2.1), but not on a regular basis. A participant explained that they conducted previews more often now than before in order to take a more informed decision about which devices to seize. The reason for the increased use of preview was that they recently had acquired a hardware write blocker, which enabled them to preserve the integrity of the evidence during preview.

> Yes, this is the situation of today… there is so much seizure, and it is positive that we are moving towards making better assessments on a better foundation than at random. For example, that pink flash drive probably belongs to the daughter...

The purpose of preview before the time consuming data acquisition could be to look for specific evidence, such as images or messages. This could be important information to bring up in the first police interview.

Preview could also be done after acquisition, but before analysis of the seizure, in order to obtain a better basis to decide what should be examined first. A DFD told that e.g. in

homicide cases such an approach would be useful to find the device that was used closest up to the time when the crime was committed, and s/he would start the start the analysis here.

4.5.4 Prioritizing

The management at Department for Homicide Investigations and the Department for Investigation of Sexual Abuse would prioritize which cases the DFDs should work with. If the Computer Crime Department was instructed to give priority to a case, there was an expectation that the case also is prioritized by the CD/team in charge of the investigation.

Within each case – the DFD wanted the CD to decide which of the digital devices that should be subject to data acquisition and analysis first. The reason was that the CD would have more in-depth knowledge of the criminal case, and thus a greater prerequisite for making such a decision.

One DFD expressed that it could be very demotivating if the communication failed regarding what seized devices to perform data acquisition and analysis of. The DFD had experienced to put great effort in acquisition of the seizure in a case which s/he was told was urgent. When the DFD contacted the CD to obtain input for the analysis phase, s/he learned that that the case was dismissed.

4.6 The analysis phase

4.6.1 Mandates

Previously, the Computer Crime Department required the CD to use a form where the task should be described in writing. As a result they often received an open or untargeted mandate which lead to inefficient and time consuming analysis for the DFD. According to several of the DFDs, it was a problem that many CDs did not know or understand how time consuming the analysis phase was, both for the CD and the DFD involved.

They had recently changed this routine, and discarded the written form in favour of an oral agreement on the task. According to the DFDs, the CDs often struggled hard to define a purpose of the tasks. The DFDs were under the impression that they occasionally were requested to acquire digital devices by routine – and not as a result of targeted planning. If the CD was unable to provide a clear mandate, the DFD would give input on what s/he could look for during the analysis. The DFD would usually read the relevant documents in the criminal case, e.g. the police interviews, to get a better foundation for deciding upon the target of the analysis.

One of the DFDs told that s/he routinely arranged a meeting with the CD after performing acquisition of the seized devices. The aim of this meeting was to clarify what the analysis should seek to uncover, and to what extent the CD would contribute in the content analysis.

Several of the DFDs stressed the importance of having detailed knowledge of the case in order to do a sufficient good job with the analysis of the seized data. One of the DFDs said the following:

> We need to have knowledge about the details of the case in order to do a good job. If we don't – how can we examine data and understand what we see, and see the bigger picture? It is very important.

However, sometimes an open approach to the analysis could provide good results. A DFD told that at the early stages of a homicide investigation where the perpetrator was unknown, an open approach could be used to look evidence or clues that could lead to identification of the perpetrator.

Some departments in the Oslo Police District use System A (anonymized) to set up a plan for the investigative tasks, but the DFD would normally not receive the task here. If the task was described in this system, it would usually be described quite generally. The details of the task would be communicated orally over telephone or in a face to face meeting between the CD and the DFD. The CDs participating in this study would always use System A to set up a plan the investigations they were in charge of.

When the DFDs and the CD had discussed the mandate of the task, the DFD would write what they agreed upon in another system, System B (anonymized), which only the DFDs had access to. The DFD would also document the progress of the data acquisition and analysis, as well as the result of the analysis here. A participant told s/he would write a duplicate of the information recorded in System B in System A to make sure the information was available to the rest of the investigation team. However, s/he emphasized that this was quite time consuming. None of the DFDs would routinely share the notes on the agreed upon mandate with the CD, and one of the DFDs explained the reason to be that s/he was afraid of giving the impression of not trusting the CD.

One of the CDs expressed that s/he wanted the DFD to document details about the progress of the investigation of the digital evidence in System A, instead of a system the CD had no access to. This way, the CD could continuously have access to updated information on the progress of the tasks handled by the DFDs and relevant results of the analysis.

Several of the participants emphasized the benefit of the recent measure of employing DFD liaisons in different departments of the organisation. This had led to a significant improvement – especially in relation to acquisition and analysis of the seized digital evidence. Without the DFD liaisons, the seizure would have been put in the line of the growing backlog. According to the DFDs, the DFD liaisons would know the languages of both the CD and the DFD, and would often contribute to a better understanding among the CDs about e.g. how much time and resources the different analysis approaches would request.

The DFDs who worked with the Department for Investigation of Sexual Abuse had experienced a big improvement in this situation:

> We see that things have improved much since we got a liaison at the Department for Investigation of Sexual Abuse, because he is some kind of bridge between us and them. He speaks both languages, can take our party and explain to them – no, this is not how things work…this is the time such a task will require. To be our man there, and that has helped a lot.

Several of the participants were worried about the knowledge and skills among the ordinary CDs within the police. The poor technological competence often resulted in wide and

inconclusive mandates, and unrealistic expectations of the speediness of an analysis of digital evidence.

4.6.2 Three types of cooperation

According to the DFDs' descriptions, there were essentially three variants of cooperation between the CD and the DFD in the analysis phase of the Digital Forensics Process:

1. The DFD received a mandate from the CD, and conducted the analysis on his/her own.

2. The DFD and the CD collaborated on performing the analysis. The CD focused on the content analysis, e.g. deciding whether images or chat were relevant as evidence to the case, while the DFD carried out examinations that required technological competence, e.g. to examine when during the chat an image was sent, to recover deleted information og information hidden in virtual containers. The technical analysis would be carried out by the DFD, and was often about exploring the context, verifying and documenting the result of the content analysis.

3. The DFD conducted acquisition of the seized device, and the CD performed the analysis on his/her own.

According to one of the DFDs, cooperation type 3 was the most prevalent form of cooperation in less serious cases, which also were the most common cases to them. Because of the large number of cases, they did not have the capacity gain in depth case knowledge, and it was therefore more appropriate that the CD did the content analysis. The DFD would give advice and provide training if necessary.

In relation to cooperation type 3, one of the CDs wanted a more standardized form of cooperation in severe – yet uncomplicated cases. The CD considered it of great advantage that the DFD routinely extracted information e.g. images and communication logs, and provided them to the case analysis team at the department heading the investigation. The case analysis team would collect and analyse all the pieces of information in the case, and the CD considered it ineffective if the analysis of digital evidence was done separately.

4.6.3 Updates of the case progress

If the investigation of a case was lengthy, the DFD tried to stay updated by monitoring the log in System A and the case file in BL ('Basis Løsninger'). BL is a general information system for case documents in criminal investigations.

When there was no team established, and the CD was heading the investigation on his/her own, the CD and DFD would communicate over phone, email or in face-to-face meetings.

If a team was established, and the DFD was included, the progress meetings were an important setting to get information about developments in the case and to obtain input for further analysis on the seizure.

If the DFD made interesting discoveries during the analysis, s/he would normally first communicate these verbally to the investigative team, since they might have immediate implications for the decisions and direction of the investigation. The information would eventually be documented in a report, which was included in criminal case file.

4.7 Presentation phase

4.7.1 Reports

According to all the DFDs, the general rule was to write reports about their own activities in a criminal case.

The DFD would usually write report about the data acquisition of the seizure. When the CD performed the content analysis, the DFD would write a report about the processing, since it involved a filtering of the data the CD had access to. As a result of the content analysis, the CD would write a report where the information of interest was described.

If the DFD conducted a technical analysis in relation to the findings from the content analysis, the DFD would write a report about it. In case of e.g. child sexual abuse, the CD would describe the content analysis with focus on which images s/he has selected, and why. The

DFD would examine and document technical contextual data in relation to the selected images, and evaluate and describe how and when they got there.

The DFD could also write reports about preliminary results of the analysis to provide an information basis for e.g. pre-trial custody hearings. The report would constitute the basis for maintaining the charge, and underpinning the legal conditions in relation to risk of evidence destruction or of repeating the crime.

The DFD was sometimes tasked with only the data acquisition of the seized devices, and the CD wanted to perform the analysis him/herself. In such situations the DFD would want to review the report from the CD to prevent incorrect conclusions due to lack of technological competence.

Several of the DFDs emphasized writing reports as neutrally as possible, focusing heavily on the facts. However, if a report on the analysis of data should make sense, the evidence should be put into a context. A DFD told s/he normally separated the report into two parts: An objective part, and more subjective part. The subjective part was more explanatory, where the findings were put into a context, e.g. an image was sent as a result of a threat posed on a chat conversation.

In order to provide an accurate overview of the scope of the analysis, several of the participants highlighted the benefit of a clear and concretised mandate. On such a basis, they found it easier to describe the actions performed in relation to the analysis easier, e.g. what they had searched for and which information this had resulted in. This way the DFDs could avoid doubts about what they had searched for during the analysis, in particular doubts about negative findings, e.g. whether one could conclude that particular information was not present on the seized device.

One DFD told that writing reports could be challenging, and stated the following:

> What I consider one of the most difficult tasks - to explain things in a way that is descriptive and can show that the findings are relevant, but yet at the right level.

This corresponded well with what a CD described about the same issue:

> Traditionally the Computer Crime Department has not been good at the reporting phase. Maybe a bit cruel to say, but the practices have been highly variable. And they do not have the same culture as we have. They lack the understanding a CD has for what good documentation should look like.

Several DFDs told that in order to bring the best possible quality into writing reports they would routinely read and assess each other's reports. They had no template or list of criteria to refer to, so the feedback would depend on the reader's ability, motivation and knowledge. A DFD said that when s/he was doing such a review, s/he would try to ask him/herself whether s/he understood what was described, whether there was correlation between the presented findings and the conclusion, and whether the conclusion held water.

4.8 Investigative competence

4.8.1 Investigative methodology

When asked about the competence in relation to investigative methodology and The Investigative Cycle, several of the participants without police background expressed a great desire to learn more about these topics. Some of the DFDs had applied for educations relevant to these topics. However, because of the large number of applicants, the DFDs were often not prioritized by the management for enrolment to these educations. One DFD said s/he had asked to be involved in major cases, so s/he could learn more about investigative methodology, as well as the mind-set of the detectives.

The situation among the participants with police background was quite different. When asked about the competence in relation to investigative methodology and The Investigative Cycle, they considered own competence sufficient, and all had completed post graduate courses or educations in relation to the topic.

4.8.2 Investigation of guilt and innocence

All participants in this study were asked questions about how they conducted their investigation in relation to the issue of guilt or innocence.

One of the DFDs told that the mandates for the analysis often were quite open and general at an early phase of the investigation, and specific questions were more frequent at a later phase.

Other DFDs s explained that they often got very specific questions to answer during the analysis phase. When detailed questions formed the basis of the analysis, one DFD emphasised the importance of documenting the details of the mandate. The reason was to prevent false negatives, such as the assumption that a certain image was *not present* among the seized data, since it was not among the identified illegal images. The same DFD also stressed the importance of documenting the negative information – which was information that they had decided to - or been requested to - look for, but did not find.

The analysis of the seizure could serve many different purposes, and could be aimed at e.g. trying to find something that underpinned the reported crime. The target of the analysis could also be trying to verify the suspect's account from the police interview. According to one DFD a normal approach in homicide investigations was to identify all relevant activity as close to the time of the incident as possible. Another DFD stated that the actual crime rarely happened on the computer, hence the analysis often revolved around finding relevant information to clarify the suspect's intentions.

One DFD told that s/he tried to avoid preconceived theories, and strived to be as open minded as possible when s/he started examining the seizure. The initial strategy was to look for something that immediately caught the attention.

Several of the DFDs said they tried to challenge the potential evidence they uncovered. They emphasized that pieces of digital evidence could not stand alone, and should be supported by other information and evidence. Evidence should always be evaluated to determine the relevance or reliability. Sometimes the presence of the evidence could be explained otherwise, e.g. the evidence was downloaded by someone else than the suspect or the evidence was a result of an automated process caused by a pop-up window or malware.

One DFD explained the search for exculpatory evidence as follows:

> If a lot of illegal content is found, and I discover that the username on this computer is different from the name of the suspect. And he says the computer belongs to a friend, it is

> important that I document who is the registered user, when the machine was installed and those things, and not exclude information that could be beneficial to the suspect.

Another DFD gave an example of a search for mitigating circumstances and exculpatory evidence. The DFD analysed a call record from a mobile phone that covered the period around when the crime was committed. During this period there was no log data, but there were log data both before and after. This could be explained with the suspect turning off the mobile phone when committing the crime. The DFD had to refute alternative explanations of this potential evidence e.g. this being a recurring pattern with the natural explanation that the suspect was taking a nap at every day at the same time. S/he therefore looked at the call records for a longer period back and forward in time to see whether this had happened before, or just this once when the crime was committed.

One of the DFDs underlined that the goal of the analysis was not to get a suspect convicted, but to be able to conclude on something with the greatest possible certainty.

4.8.3 Hypotheses

The DFDs were presented in various degrees to the hypotheses of the cases they were tasked with. In more serious types of crime concerning homicide and sexual abuse the investigation was planned in System A, and the hypotheses were available to all who were participating in the investigation.

In criminal cases of less gravity the investigation was usually not planned in System A. In such situations the DFDs were often not presented to the hypotheses of the case.

The DFDs did not seem to focus heavily on the hypotheses of the case. The hypotheses would normally not form the basis for the analysis of the seized data, since the DFDs usually got more specified mandates or tasks.

When asked about how they would test the hypotheses, some DFDs told that they had the greatest focus on refuting the hypotheses. A DFD exemplified this with a case with suspicion of downloading images of child sexual abuse. In such a case, the DFD told that s/he would

look for illegal images, and investigate the internet activity log for traces of searching and downloading such files. If there was no trace of search or downloading activity, or illegal images, s/he would consider the hypothesis disproved. But, not all cases were as clear as this example. In other cases s/he could find a few illegal images among large amounts of legal pornography. In such situations the aim of the investigation would be to uncover whether the images had ended up on the computer as a deliberate act or if they had been downloaded by accident when the suspect thought s/he downloaded a collection of files with legal pornography.

The focus on hypotheses was quite different among the CDs participating in this study. One of the CDs said they worked structured on the basis of hypotheses in all cases on his/her department. The CD expressed that it was an important principle that the hypotheses also were available for the DFDs that worked on the case. S/he considered the hypotheses to be an essential supplement for the DFDs in an early phase of the investigation, if the case was very open and unresolved, and the need for information was urgent.

At a later phase of the investigation the CD would not expect the DFDs to focus heavily on the hypotheses of the case, and would provide more specific tasks or questions for the DFD to answer through the analysis. The CD considered the hypotheses based approach as a safety net for objectivity:

> The first security precaution is hypothesis formation. To establish a set of hypotheses to avoid the pitfall of confirmation bias. So the basis we commit to; and which we agree to deal with; is a set of hypotheses to vaccinate us against not being objective, that is to ensure an objective investigation.

Another CD did also use a hypotheses based approach in the cases s/he was in charge of. The CD considered the hypotheses to be important in order to stay open minded and sustain objectivity.

4.8.4 Penal Code and Criminal Procedure Code

The DFDs, with one exception, told that they did not use the Penal Code or the Criminal Procedure Code actively and systematically in their work. Some DFDs expressed they did not see the necessity of it, and if they were unsure what the investigations would seek to identify,

they would rely on the CD assigned to the case. A CD stated that s/he did not expect the DFDs to have good knowledge of the sections in the Penal Code. The CD considered the task to define the information requirement in the case to be the responsibility of the CD - and to derive appropriate investigations tasks on this basis. However, one of the CDs admitted that the subjective conditions in the various sections of the Penal Code could be quite difficult to understand even for an experienced detective with a police background.

The DFDs without a police background had been issued with limited police authority. This implicates police authority during working hours, and within the police district. As mentioned in chapter 2.1.3, a detective with limited police authority may conduct coercive measures such as search and seizure. Some police operations and methodologies require additional certifications, e.g. use of pepper spray and emergency driving, but none of the DFDs without a police background had these formal qualifications. When the limited police authority was issued, they only received a one-day course in relevant topics like e.g. coercive measures. Several DFDs expressed that this training was inadequate, and that they would have liked more training in relevant subjects.

4.8.5 Crime phenomena

When asked about their level of knowledge about crime phenomena, all the DFDs told that they only had experience based knowledge from the cases they had worked on. Some of the DFDs worked with a wide range of criminality types, while others worked almost exclusively with violent- or sexual crimes.

The DFDs who worked with specific crime types stated that they had gained knowledge by working over some time with the same crime type. The DFDs covering the various crime types told they had to rely more on the CD assigned to the case concerning knowledge of the crime phenomenon. The reason for this was that it would be difficult, or perhaps impossible to gain in-depth knowledge about all the various crime phenomena they came across.

A DFD told that s/he initially used the same approach and strategy in all types of crime s/he investigated. The methodology had evolved on the basis of experience, and the DFD now used different approaches and strategies when processing and analysing various crime phenomena. The DFD said that s/he was unsure whether the developed approaches and

strategies were as good as they should be, because s/he had no best practice or knowledge base to refer to.

According to some of the DFDs, there was no established practise in sharing different analysis strategies among the DFDs, and one said s/he believed that more extensive sharing of good practice would be beneficial to the knowledge development within the Computer Crime Department. Several of the DFDs expressed that they would like to gain more knowledge about the crime phenomena they were investigating.

4.8.6 Biases and heuristics

The DFDs in this study told that they had never received training in the subject bias and heuristics, and the knowledge they had on these subjects was solely experience based. Several of the DFDs were unsure whether their knowledge level was sufficient.

The participants with police background said they considered their own knowledge in relation to these subjects sufficient.

4.8.7 Measures regarding objectivity

All the participants expressed that it was important to safeguard the objectivity requirement during an investigation. When they were challenged about measures to sustain their own or others objectivity, most of the participants pointed at awareness as an important measure.

One DFD said s/he tried to have a professional attitude. This implied that s/he constantly reminded him/herself that the cases were not about objects but real persons, and that the persons actually could be innocent. The DFD was conscious of how s/he talked about the cases to other colleagues, especially those who were new at the Computer Crime Department. This way s/he wanted to prevent the development of a poor culture in relation to how they talked about the suspect or the other parties of the criminal case.

A CD told that s/he tried to distance him/herself as much as possible when analysing images and video of child sexual abuse. The CD would listen to music in order to maintain this distance, and would strive at spending the least amount of time possible on each image or video to avoid emotions to influence the decisions during the analysis.

A DFD said s/he used his/her senior investigation officer actively to read through his/her reports, with particular focus on the conclusions. The senior investigation officer would look at the report with fresh eyes, give input and challenge the conclusion. The DFD considered this to be a beneficial measure for increasing the quality of the report.

Other DFDs talked about similar experiences among colleagues at the Computer Crime Department, and they experienced positivity towards asking critical questions about each other's conclusions about findings.

A DFD said the following: (P = participant, I: interviewer)

> P: Among other things, I remember a report where I wrote the name of the suspect. And then my colleague asked a question: Can you with 100 percent certainty state that the suspect wrote the SMS? Yes it is his phone, and he has the code, but I can't. So then it was like...
>
> I: So you changed your report?
>
> P: Yes, I had to.

One of the CDs mentioned several measures to sustain the objectivity:

The CD emphasized the hypotheses based approach and the investigation plan as key factors to ensure a broad and objective investigation.

The CD also stated that it was important for the objectivity that everyone who participated in the investigation had a common understanding of where it was heading; if the investigation was heading towards a specific goal or if it was still widely defined. S/he said:

> At one time or another during the investigation we will drop the all the alternative hypotheses and focus towards one target. That's what's done.

The DFD stressed that that hypotheses were never deleted, and they could be picked up again if necessary at a later stage of the investigation.

The DFD also mentioned evaluation as an important measure to safeguard objectivity. The information s/he received from the Computer Crime Department was evaluated on several

levels of the organization - both by him/her as main responsible detective of the investigation (Norwegian: hovedetterforsker) and by the case analysis team at his/her department.

4.8.8 Sources of influence

When asked what could influence their decisions during the investigation, several DFDs told that they were probably influenced by both the case documents they read, and the information they received about the case from other detectives. However, the case information was considered necessary to perform a sufficient analysis, and they did not consider avoiding this type of information as a relevant countermeasure.

None of the DFDs had experienced poor or unethical behaviour in relation to the suspect or other parties in the case. A DFD said s/he had never experienced a suspect being backbitten - not even a killer.

The DFDs told that they occasionally needed debrief, since they on a regular basis could be exposed to emotionally stressful images and videos of child sexual abuse. Debrief was not systematized - but happened between colleagues when necessary. One DFD told that during a spontaneous debrief they could develop quite strong negativity directed towards the perpetrator. Several stressed that if they experienced emotional problems with what they saw or heard during investigations, they would have access to a psychologist.

4.9 Organisational challenges

The topic *organisational challenges* was only scratched upon in this study. However, the participants pointed out several topics of importance in relation to quality and efficiency in the investigation of digital evidence.

4.9.1 DFD liaisons

According to the participants, the technological competence of the regular detective was poor. The Computer Crime Department did not have the resources to assist in all matters. Severe crime would naturally be prioritized; hence there would be fewer resources to investigate digital evidence in criminal cases of less gravity. The crime which was not prioritized would not just be trifling matters, but quite serious crime cases like fraud, domestic violence and robbery.

Several of the DFDs referred to the ongoing pilot project (Oslo Politidistrikt, 2017) as a promising measure, where establishing DFD liaisons (see chapter 2.4.3) in various departments in the police district was done as an attempt to improve the situation of insufficient competence and increasing backlogs. The DFD liaisons would be tasked to carry out data acquisition and data analysis of digital evidence that did not pass the priority threshold at the Computer Crime Department. The DFD liaisons would be closely followed up and receive regular training by assigned DFDs from the Computer Crime Department.

4.9.2 Organisational and physical positioning

Several DFDs highlighted an appropriate position in the organization as important. The Computer Crime Department was according to the DFDs currently located outside the investigation departments, and the participants emphasized that this was necessary in order to have the opportunity to develop technological competence and methodologies.

The participants also highlighted close physical location to the detectives they collaborate with as a success factor for high quality when investigating digital evidence. Close physical location increased the possibility of developing good relationships through informal contact, which led to good cooperation in the criminal cases they investigated together.

4.9.3 Routines, management and responsibility

A CD referred to a quite new procedure of organizing the work of severe criminal cases. The aim of the procedure was to enable a rapid establishment of a well-functioning project based organisation with the sufficient competence in place when certain crimes or certain levels of severity of a crime occurred.

The DFDs were not aware of any formal procedures or guidelines regulating cooperation between the CD and DFD when investigating digital evidence. However, several participants emphasized the great efficiency benefit from the well-functioning procedures of prioritizing cases by the management. According to the DFDs this had led to a more correct utilization of resources, hence better efficiency of the investigation.

Another measure that, according to the DFDs had great impact on quality and efficiency of the investigation was the dialogue to establish mandates. When they replaced the written

forms with oral dialogue, the DFDs experienced that the investigations got more targeted, and that they could use their competence to propose approaches for the analysis more often.

5. DISCUSSION

In this chapter, I will provide answers to the research problem by addressing and discussing the defined sub-problems.

Firstly, I will look into how the characteristics of an investigation with high quality provided by the participants fit with the goal defined by the Attorney General. The identified non-technical sources of errors in a criminal investigation will then be discussed (see chapter 5.2). These are divided in four main themes (see also chapter 3.3.6): Lack of investigative competence by the detective (see chapter 5.2.1), absence of the adequate competence at the right time the Digital Forensics Process (see chapter 5.2.2), bias and missing countermeasures (see chapter 5.2.2.1) and organisational challenges (see chapter 5.2.3). In chapter 5.3 the consequences if these errors occur are outlined. The countermeasures to prevent the errors from occurring are discussed in relation to individual, cooperation and organisational levels in chapter 5.4. Eventually, some real-life examples which could illustrate good cooperation between CDs and DFDs during investigation of digital evidence are described and discussed in chapter 5.5.

5.1 What are the characteristics of an investigation that is safeguarding the rule of law?

Good quality, efficiency and active prevention of errors of justice are prerequisites to safeguard the rule of law. As mentioned in chapter 2.1.1, the objectives for a criminal investigation defined by the Attorney General are high clearance rate, rapid case processing and adequate penalty. This has been challenged by Myhrer (2014, p. 197) who argues that objectivity and procedural correctness should be prioritized higher than rapidness. These are all criterions for achieving the overall goal of any criminal investigation, which is a result where the rule of law is safeguarded for all the involved parties.

The participants provided their perspective of what constitutes an investigation characterized by high quality and efficiency (see chapter 4.2).

Their answers can be summarized to:

A targeted investigation with sufficient resources and competence, characterized by clear investigation and prosecution management, and good communication. The personnel involved in the investigation strive to maintain objectivity and high ethical standards.

The characteristics given by the participants seems to be suitable to achieve the objectives defined by the Norwegian Attorney General, however – they are closer to Myhrer's description of objectives for an investigation.

5.2 Which non-technical sources of errors relevant to a criminal investigation may be identified?

5.2.1 Lack of investigative competence

Do the personnel conducting the criminal investigation of digital evidence have the adequate investigative competence?

As described in chapter 2.1 and in the preliminary study (N. Sunde, 2016, chapters 4.1 and 5.1), criminal investigation is conducted within all the phases of Digital Forensics Process, and the phases *identification*, *analysis* and *presentation* requires competence beyond the technological competence. This is also supported by the participants' descriptions of activities during these phases by the Digital Forensics Process (see chapters 4.5-4.7). To handle digital evidence in line with the objectives to achieve high quality (see chapter 2.1.1), the detectives need a minimum of investigative competence. *Investigative competence* can be summarized to consist of the following competence components:

- *Knowledge about ICCPR and ECHR (see chapter 2.2.1)*
- *Knowledge about the Penal Code - and evidential requirements (see chapter 2.2.1)*

- *Knowledge about Criminal Procedure Code – principles, obligations and coercive measures (see chapter 2.2.1)*
- *Knowledge about relevant crime phenomena (N. Sunde, 2016, chapters 4.1 and 5.1)*
- *Skills in use of The Investigative Cycle (see chapter 2.2.3)*
- *Skills in hypothesis generation and testing (see chapter 2.2.3)*
- *Knowledge about relevant biases, and sufficient countermeasures (see chapter 2.3)*
- *Knowledge and skills in relation to the procedures of a criminal investigation, and the relevant investigative methods (N. Sunde, 2016, chapters 4.1 and 5.1)*
- *Documentation and presentation skills (see chapter 2.2.2.5)*

There are no defined competence criteria for investigating digital evidence, except the vague requirement of "adequate training" and "appropriate competence" stated by the Norwegian Police Directorate (see chapter 2.4.2).

The participants with police background gained a formal basic level of these components during their bachelor education at the Norwegian Police University College. However, the DFDs without police background lacked this competence. They had only received a one-day course in topics related to investigation when they were issued with limited police authority.

The participants were asked about their level of competence in relation to several of the investigative competence components during the interviews. Since the DFDs with police background gained formal investigative competence during the police education, I will only discuss the investigative competence components from the list above in relation to the *DFDs without police background*.

Knowledge about criminal law/criminal procedure law: This subject was covered in the aforementioned one-day course for the DFDs. Only one of the DFDs used the Norwegian Penal Code or Criminal Procedure Code as a reference on a regular basis when performing analyses of digital evidence or carrying out coercive measures. The topics were part of the one-day course when being issued with limited police authority.

However, there seemed to be awareness about the objectivity requirement in Criminal Procedure Code, and several participants gave examples of this (see chapter 4.8.2).

Knowledge about crime phenomena: None of the participants had received any particular training in specific crime phenomena, and the knowledge was experience based - gained through working with different phenomena in the cases they were assigned to.

Knowledge and skills in relation to the procedures of a criminal investigation, and the relevant investigative methods / use of The Investigative Cycle: None of the participants had received any training in criminal investigation related subjects except the aforementioned one-day course. Several of them expressed that they wanted to gain more knowledge about this topic, since they performed investigative tasks during the Digital Forensics Process. However, several had experienced to not being prioritized by the management when applying for criminal investigation educations.

Skills in hypotheses generation and testing: None of the DFDs had received training in the subject hypotheses generation and testing. The DFDs did not normally use the hypotheses as the basis of their analysis. In more severe cases, hypotheses were defined by the CD/team managing the investigation, and the DFDs got access to these. In such occasions some DFDs told that they had the greatest focus on refuting the hypotheses, and some gave examples that described how this was conducted (see chapter 4.8.3).

Knowledge about relevant biases and countermeasures: None of the participants had received any training in the subject, and were only able to name awareness as a countermeasure (see chapter 4.8.6). Several of the DFDs were unsure whether they needed training in this subject.

Documentation and presentation skills: The participants had not received any training in documenting digital evidence in reports, and some expressed that they found this task quite challenging (see chapter 4.7.1). A CD who would be a receiver of such a report told that the reports written by the DFDs often had insufficient quality – due to improper documentation of the digital evidence.

To summarize, investigation of digital evidence is carried out by DFDs without necessary investigative competence. There is reason to worry about whether the objectives posed by the Attorney General are achievable when considering the lack of investigative competence among the DFDs.

5.2.2 The presence of the right competence at the right time

The CDs and the DFDs have different competence, and together they would often hold the necessary investigative and technological competence to conduct an investigation with high quality. So, is the investigation of digital evidence structured in a manner ensuring that the right competence is in place at the right time?

Since the scope of the thesis is limited to the non-technical sources of errors, only the Digital Forensics Process phases requiring almost exclusively technological competence; collection and examination; are excluded. The identification, analysis and presentation phases require investigative competence, and are subjects to the further discussion. I will discuss whether the absence of the right competence in these phases when investigating digital evidence could be a source of error. However, first I will discuss bias, heuristics and missing countermeasures as a potential source of error, since this is relevant for all the Digital Forensics Process phases.

5.2.2.1 Bias, heuristics and countermeasures

Is the knowledge about bias and heuristics at an adequate level, and are the participants able to carry out effective countermeasures against these pitfalls?

The risk of bias and heuristics when carrying out a criminal investigation is well documented through research (see chapter 2.3). The research has also provided promising results regarding several countermeasures that could prevent bias affecting detectives' decisions (see chapter 2.3.5).

The police education has provided training in this subject for several years (see chapter 2.1.3). The DFDs without police background had no training in relation to bias and countermeasures. The participants with police background considered their level of knowledge in this subject to be sufficient (see chapter 4.8.6).

What's the risk?

The interviews do not provide a sufficient amount of information to perform a risk assessment concerning bias and heuristics in the criminal investigations conducted by the participants. However, there are indications in this material that might be worth highlighting.

The lack of knowledge about bias and heuristics could affect the ability to recognize situations where bias or heuristics might occur or already has had an impact on the investigation. Knowledge would be necessary to understand why and how countermeasures should be implemented in the organisation.

There were several factors that could increase the risk of confirmation bias and tunnel vision. The DFDs were *not routinely informed about the hypotheses of the case*. This, in combination with *time pressure* could lead to an increased risk of bias. Add emotions like *sorrow and anger* – which could be a reaction to emotionally stressful content within the seized data – and the risk could increase even further.

As a result of exposure to emotionally stressful content, the participants conducted informal debriefings with colleagues. If this colleague was involved in the investigation of the particular case, there would be a risk that the emotions could decrease the colleagues' objectivity.

The participating DFDs were specializing towards technical expertise within digital forensics, and the participating CDs were specializing towards investigative expertise within a particular crime phenomenon. The physiological changes of the brain when developing expertise increase the risk of errors. This is due to several reasons, e.g. the tendency to take short-cuts. Experts are also more susceptible to confirmation bias and overconfidence (see chapter 2.3.4). Several of the participants are experts within their fields, and are therefore more at risk for the types of bias mentioned.

The DFDs were exposed to contextual information which was not related to their analysis. This happened e.g. when they were included in the investigation team or were accessing the case file. This increased the risk of *contextual bias* (see chapter 2.3.1). This bias is particularly problematic because the information that might affect the interpretation of the digital evidence

is often not documented – and could therefore stay undetected during the investigation and trial.

The external contextual information could perhaps be held away from the DFD, while it is probably impossible to prevent exposure to the internal contextual information within the seized data. Internal contextual information could for instance reveal preferences, behaviours and fantasies that make the suspect appear as immoral or cruel, with bad intentions. Conceivably, such information might affect the decisions by the DFD.

Countermeasures

The lack of formal competence in the subject bias/heuristics does not exclude the fact that the DFDs without police background might have gained experience based competence, or possess unconscious competence (see chapter 2.3.1). There were several statements that indicate that some relevant measures were carried out. The DFDs strived to be objective when carrying out investigation (see chapter 4.8.7). One told about how s/he tried to have a professional mind set – where s/he would remind him/herself that the suspect might be innocent. Another DFD mentioned how s/he would try to create distance to the emotionally disturbing content by listening to music during the analysis. Another DFD talked about precautions in relation to how s/he talked about the parties of a criminal case to prevent influencing other colleagues. The routine of assessing each other's reports (see chapter 4.7.1) is relevant to the measure 'Devil's Advocate' (see chapters 2.2.3 and 2.3.5). The DFDs were aware that the information in the case file could affect their objectivity, but considered this information crucial to perform a targeted analysis.

The CDs mentioned several measures and activities that correspond quite well with the countermeasures against bias outlined in chapter 2.3.5, e.g. documenting the hypotheses of the case in an investigation plan. This is expected due to their police education from the Norwegian Police University College. However, there might be an indication of overconfidence (see chapter 2.3.1), due to the description of the hypotheses based approach as a safety net for objectivity by one of the CDs. The CD uses the expression "to vaccinate us against being objective", which might be an indication of exaggerated faith in the ability to

exclude bias from affecting the investigation. Bias can be prevented, but no measure is proven to fully exclude bias from occurring.

To summarize, the response from the participants without police background indicates a lack of knowledge about bias, heuristics and effective countermeasures. Effective countermeasures do not seem to be implemented properly, and hence there is an increased risk of errors.

5.2.2.2 Digital Forensics Process: Identification phase

Does the survey indicate that the right competence is present in the identification phase? This question will be discussed in relation to planning of search and decisions about seizure.

Planning the search

A possible source of error is the absence of the sufficient competence when planning and conducting searches. Technological competence is needed to predict and assess which devices the search team might encounter, and which tools and equipment is needed to collect them in a forensically sound manner (see chapter 2.2.2). Technological competence is also necessary to decide about the best way to deal with data stored outside the search scene, e.g. cloud services and webmail (see chapter 2.2.2.1).

In relation to investigative competence, the investigative steps should always be based on the information needed to test the hypotheses (see chapter 2.2.3) and the relevant sections of the Penal Code (see chapter 2.2.1). In order to have this knowledge available, the DFD should be part of the planning of the search together with the investigation team which has the updated case knowledge. The team should consist of the necessary technological and investigative competence to be able to make the best possible guess about these potential evidential sources, and the related obstacles they might encounter.

The participants described how not being included in the planning, or being included at a late stage was problematic in relation to being well prepared for searches (see chapter 4.5.1). According to the participants, the planning was also relevant to decide which level and type of technological competence they should send to the search scene.

Decision about seizure

The participants were asked about how decisions about seizure were made.

When the search scene and the suspect were under control, the search team would get an overview of the potential evidence on the scene. Then, a decision was made about which devices to seize and which to leave behind. Due to the statements from the participants the enormous amount of potential digital evidence forced them to make decisions aimed at limiting the scope of seizure to a minimum (see chapter 4.5.2). They described situations where relevant devices were left on the search scene or irrelevant seizure was collected. The participants also told about many different approaches for deciding which items to collect, e.g. decisions based on exterior factors such as colour, contextual information about the digital device such as the room in which it was found, or statistical calculations (see chapter 4.5.2).

The problem with digital evidence in a switched off state is that one cannot determine whether it is carrying important evidence to the case or not. One might be able to make a successful guess based on the case knowledge and the contextual factors of the device, but this approach is very risky. This situation might be compared to entering a search scene, and trying to guess whether there is important evidence in a room which door is closed.

The decisions based on exterior factors, contextual information or statistics are inadequate because they lead to randomly collected evidence. The tendency still to use these approaches may be linked to the feature-positive effect (see chapter 2.3.2), since the presence of features in relation to exterior or context have more influence on our decisions than the absence.

To assess whether the information revealed is relevant to the case, the content must be considered in relation to the hypotheses of the case (see chapter 2.3.3). It is also important that the methodology applied at the search scene safeguards the principles of forensically soundness (see chapter 2.2.2). A preview of the data may be the best approach to this challenge, where the detective may have a look at the information on the device prior to the decision about seizure or not. The Digital Field Triage Member (see chapter 2.2.2.1.a) is a research based approach, and tries to meet the challenges with availability of technological

competence and the need for information when making decisions about seizure. Preview is an important component of this model, which also facilitates preliminary analysis of the data.

If the right competence is not available on the search scene, there is also a risk of evidence being altered or destroyed due to inadequate handling of the digital device containing potential evidence. The Oslo Police District is currently implementing a model with several similarities to the Digital Field Triage Member (see chapter 2.4.2), and one of the goals of this measure is to increase the competence of handling digital evidence in other parts of the organisation.

Summary

To summarize the aspects of the identification phase, the survey indicates that the right competence is not always present in the identification phase. There seems to be no procedure or routine ensuring that the DFD is present when searches are planned. Preview is not routinely used to make a more informed decision about seizure, and the decisions are sometimes made on the basis of undependable contextual factors of the digital device.

5.2.2.3 Digital Forensics Process: Analysis phase

Does the survey indicate that the right competence is present during the analysis phase? This question will be discussed in relation to mandates, hypotheses generation and testing, and the analysis sub-phases.

Mandates

Mandates are used to define the scope of the analysis of digital evidence. The mandates may be defined in various ways and levels. If they are too wide or narrow, too partial or activity based, they could be a source of errors. Surveys have revealed that DFDs often perform the analysis without a clear and targeted mandate (see chapter 2.2.2.4.b).

Some DFDs told about wide and generally defined mandates. Sometimes the mandates seemed to be of a routine nature, or even ill-conceived thought out. The DFDs were often asked by a CD to perform acquisition of all the seized material, but the CD was unable to define a plan or purpose for the analysis of the data (see chapter 4.6.1). According to the DFDs, they had already implemented an important measure to prevent poor mandates. They

had rejected the old written form in favour of a dialogue with the CD to establish a mutual understanding of the purpose of the upcoming task.

A weakness in the oral dialogue approach seems to be the lack of notoriety in the wake of the dialogue. The DFDs had their own system (System B) for writing down their understanding of the task. The CDs did not have access to this system, but used a different system (System A) to define tasks for the investigation.

Another important potential source of errors was the missing link between the hypotheses in the investigation and the mandate or task given to the DFD (see chapter 2.2.3). The DFDs seemed to have low focus on the hypotheses, and the CDs seemed to request more specific tasks often based on one or more of the hypotheses (see chapter 4.8.3). The missing link between the hypotheses and the mandate entails several risks of errors. It could lead to a biased or partial search for evidence. This could result in important evidence being overlooked or a one sided elucidation of the case. This could also result in false negatives causing erroneous conclusions about the absence of information.

Hypotheses generation and testing

Up to the analysis phase, the digital device has been a carrier of potential evidence. During the analysis phase, the information is open, and can be understood, assessed and analysed by a human – and by this serve as evidence of who, what, when, why, where and how a crime was committed. The Investigative Cycle is particularly relevant to the analysis phase, because the phase involves the forming and testing of the hypotheses relevant to the case (see chapter 2.2.3) In order to conduct the hypotheses testing properly, the DFD should look for evidence that supports or refutes the hypotheses, as well as information that might lead to new hypotheses in the case. The analysis might also uncover clues that could lead to other sources of potential evidence.

The survey indicated that the DFDs seemed to have a passive approach towards the hypotheses of the case (see chapter 4.8.3). They trusted the CD to define the information requirement in the mandate or task they were given. This fits well with the statements from

the CDs, who told that they worked actively with hypotheses in their own cases, but defined more specified tasks to the DFDs.

Errors may occur when there is lack of insight into - or confusion about - which hypotheses that are subject to testing in the investigation. This can lead to an investigation guided by gut-feeling and experienced based knowledge. In such situations, whether the detectives succeed in safeguarding the presumption of innocence would then be more or less due to chance. The likelihood of biased decisions increases if they are not made on the basis of a set of alternative hypotheses where both guilt and innocence is defined (Fahsing, 2016). Errors may also occur if the detectives don't understand how hypotheses testing should be conducted (see chapter 2.2.3). Working solely towards verification will result in a poor scientific test of the hypotheses - since it only takes one piece of information to disprove it (Tilstone et al., 2013, p. 7, referring to Popper).

Analysis sub-phases

The analysis of digital evidence is suggested to be divided in three sub-phases based on the nature of the task (see chapter 2.2.2.4.a). This distinction can also be useful in order to pinpoint which competence is necessary to carry out the different analysis sub-phases.

The different types of competence required in the sub-phases are illustrated in Figure 5-1, and the activities of the phases are discussed in relation to investigative and technological competence components below.

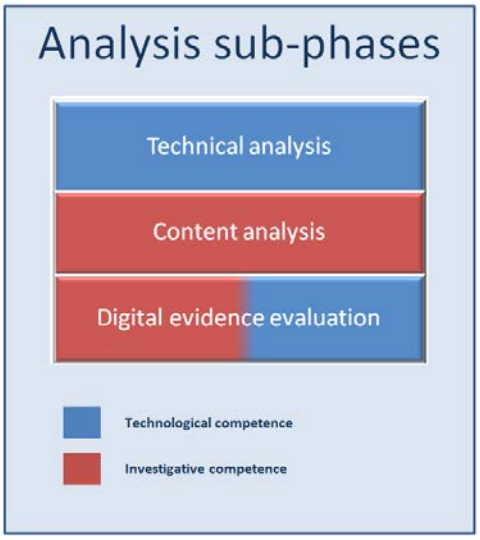


Figure 5-1: Three sub-phases of the analysis phase

Technical analysis is done by conducting analysis activities with verifiable outcomes (see chapter 2.2.2.4.a). The activities require pure technological competence, and could be performed by a DFD with no investigative competence.

Content analysis is done by identifying and documenting relevant content information from electronically stored data (see chapter 2.2.2.4.a). To be able to perform the content analysis, the CD will need to operate some kind of interface from the processing tool, but this is not considered part of the term technological competence. The investigative competence is necessary to evaluate the evidence against the relevance to the hypotheses of the case and the relevant sections of the Penal Code, as well as other evidential information in the case.

Digital evidence evaluation is done when trying to determine accuracy, causation, linkages, spoliation and meaning (see chapter 2.2.2.4.a). This analysis activity requires both investigative and technological competence. The technological competence is necessary to examine and assess the evidence in relation to accuracy, causation, linkages and spoliation. Unlike the technical analysis, the outcome cannot be verified by e.g. an algorithm, and the conclusion would therefore be based on the technological competence by the detective.

During the digital evidence evaluation, the detectives might find evidence of activities, such as downloading, organising, renaming or deleting of files. To determine the meaning of these activities, investigative competence is necessary, because it must be assessed in relation to the hypotheses of the case as well as relevant sections of the Penal Code. The activities should also be described in reports in order to show whether they meet the conditions for criminal liability (see chapter 2.2.1). An example of documenting meaning could be to describe activities on a suspects' computer, where illegal images of sexual child abuse had been moved from a storage medium and placed in shared folders on the computer. This activity could indicate the intentions of sharing the illegal images with others on the internet.

The participants referred to two types of analysis; technical analysis and content analysis. This is in line with the distinction made by the Oslo Police District in the aforementioned pilot project (see chapter 2.4.2). The participants did not make a clear distinction between the technical analysis and the digital evidence evaluation, but one DFD described how s/he would divide the report in an objective part, and a subjective – more explanatory - part (see chapter 4.7.1). The "subjective part" could probably apply to a description of a result of the digital evidence evaluation.

The DFDs described *three approaches* of collaboration between the CD and DFD during the analysis phase (see chapter 4.6.2) In the *first approach*, the DFD performed the analysis on his/her own, on basis of a mandate. In the *second approach*, the DFD and CD collaborated on the analysis, where the CD was responsible for the content analysis and the DFD would carry out the analysis of technical nature. In the *third approach*, the DFD only would perform the data acquisition, and the CD would conduct the analysis on his/her own.

On the basis of the descriptions of activities in these phases, the DFD would perform all the three analysis sub-phases in the first approach. This would include activities that require investigative competence (see chapter 5.2.1). If the DFD lacked this competence, the risk of errors could increase.

The second approach involved the CD, who would carry out the content analysis. A CD would normally have police background and thus the formal investigative competence in place. On the basis of descriptions of activities in this approach (see chapter 4.6.2) the DFD would conduct both the technical analysis and the digital evidence evaluation. The DFD would normally have sufficient competence to perform the technical analysis, since it requires solely technological competence (see chapter 2.2.2.4.a).

As described earlier in this chapter, the digital evidence evaluation requires a combination of investigative and technological competence. A DFD without police background would have the necessary technological competence, but would lack the adequate investigative competence to perform the task. Cooperation with a detective with police background would therefore be necessary; otherwise there would be an increased risk of errors.

The third approach described by the participants, was the CD performing the analysis, hence the three sub-phases, on his/her own. The CD would most likely have sufficient competence to do the content analysis, because s/he would normally have police background. The technical analysis requires technological competence, but since the outcome is verifiable – errors would be quite easy to discover. The challenge here would be to have technical skills to perform the calculations. However, the main problem with this approach is the digital evidence evaluation phase, which requires both technological and investigative competence. In this sub-phase there is an increased risk of errors in terms of misinterpretations of accuracy, causation, linkages etc. since the CD often would lack the necessary technological competence.

Summary

To summarize the aspects of the analysis phase, the study indicates that to conduct the investigation of the three sub-phases of the analysis phase, a combination of investigative and technological competence must be available. The survey indicates that this phase sometimes is carried out by personnel lacking adequate competence.

It seems like there is not enough attention drawn towards which competence is required for the different analysis sub-phases, and thus there is an increased risk of errors. The risk is probably greatest when a CD or a DFD performs analysis alone, since s/he then lacks the necessary competence as well as the safety net of error detection constituted through collaboration.

The implemented measure of dialogue seems to be is fruitful in terms of concretizing a too wide mandates. However, to achieve the goal of high quality, the mandate must be targeted and anchored to the hypotheses and the corresponding sections from the Penal Code. There seems to be a missing link between the mandates and the hypotheses of the case.

5.2.2.4 Digital Forensics Process: Presentation phase

The presentation phase includes documenting the digital evidence in reports and presenting the evidence in court. Due to the scope of the thesis, the latter is excluded from further discussion. An important question to answer in this respect is whether the necessary investigative competence is present in the presentation phase when digital evidence is investigated.

According to The Investigative Cycle (see chapter 2.2.3), evidence should be assessed against the criteria accuracy, reliability and relevance. The result of this assessment should be presented in a report.

The presentation phase is a continuation of the work from the former phases of the Digital Forensic Process. The complexity of the reports written in this phase depends on which phase the documentation is related to. Writing a report from the analysis sub-phase *technical analysis* might be a quite straightforward task due to the verifiable outcome. However, writing a report from the analysis sub-phase *digital evidence evaluation* would be more a complex task. This phase would involve technical terms in order to explain e.g. linkages or causation. The challenge would be to explain these elements in a way that clarifies the accuracy, reliability and relevance of the evidence. In the same time, the report must be written in a language which is understood by a recipient with low technological competence (see chapter 2.2.2.5.a).

As described, several DFDs are recruited to the Norwegian police to conduct investigation of digital evidence (see chapter 2.1.3). They lack training in subjects generally relevant to investigation, and specifically in this respect – documenting digital evidence in reports.

There are no defined competence criteria or mandatory further education for a DFD (see chapter 2.4.2). The DFD without police background would therefore often lack investigative competence, which would form the basis for a precise documentation of relevant digital evidence in reports.

One participant without police background told that writing reports was challenging in terms of describing the evidence on an appropriate level of complexity. A CD who often was a receiver of the reports stated that the reporting skills were highly variable among the DFDs at the Computer Crime Department. A positive measure in this respect is that the DFDs routinely read and assessed each other's reports. The CD receiving the report also would also be an assessor in this respect, and might ask for changes in the report when necessary.

Summary

To summarize the aspects of the presentation phase: Documenting digital evidence in a criminal investigation is a complex task that often requires both technological and investigative competence. The survey indicates that the DFDs without police background have inadequate investigative competence for documenting digital evidence in reports. There are routines in place for peer-assessment of reports, however – there seems to be somewhat arbitrary whether the assessor has investigative competence. Due to lack of investigative competence, there is an increased risk of errors.

5.2.2.5 Conceptualization of competence requirement in relation to Digital Forensics Process

As outlined in the former chapters, during the identification, analysis and presentation phases of the Digital Forensics Process within a criminal investigation, both technical and investigative competence is necessary. An inadequate level of competence may be a source of errors.

The model below is developed to give a general overview of the necessary types of competence during the phases of the Digital Forensics Process. The squares does not indicate

any size or level of this competence, and a more detailed description of the tasks can be found in Figure 5-3 (see chapter 5.2.2.6).

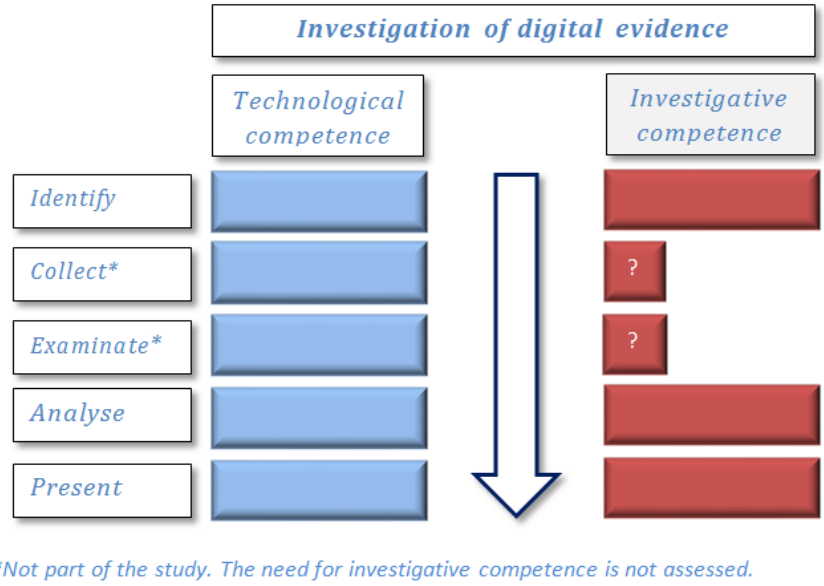


Figure 5-2: General model of necessary types of competence in the Digital Forensics Process within a criminal investigation.

5.2.2.6 Detailed model of competence requirement in relation to Digital Forensics Process

Figure 5-3 is based on the chapters State of the art (chapter 2), Data analysis (chapter 4) and the chapters 5.2.1 - 5.2.2.4. The figure is a detailed version of Figure 5-2, and attempts to clarify and visualize the distinction between tasks within the Digital Forensics Process that require technological and/or investigative competence. The purpose of Figure 5-3 is to simplify planning for which competence to have present at a given time or phase of the investigation. I would like to emphasize that the blue or red column of the figure is related to *types of competence* that should be present when a specific task is performed, and not to a *person.*

Phases – Digital Forensics Process	Technical tasks	Required competence: - Technological	Investigative tasks	Required competence: - Investigative - Case knowledge
Identification				
		- Planning of search and seizure o Preparation for collection (readiness) o Preservation (integrity, chain of custody) o Preview and triage in relation to OOV		- Planning of search and seizure o Identification of potential evidence suitable for testing the hypotheses and relevant sections of the Penal Code o Evaluate result of the preview o Decide seizure by considering ethical and legal issues, and relevance towards hypotheses
Collection		NOT PART OF THESIS		NOT PART OF THESIS
Examination		NOT PART OF THESIS		NOT PART OF THESIS
Analysis				
		- Define mandate o Give input on which analysis sub-phases to conduct		- Define mandate o Information requirement in relation to hypotheses and sections of the Penal Code o Decide which analysis sub-phases that should be conducted o Scope, cooperation model and responsibilities
		- Technical analysis o Analysis with verifiable results, e.g. compare image to checksum of known illegal images		- Content analysis o Images, internet activity, communication etc.
		- Digital Evidence Evaluation o Analysis in relation to accuracy, causation, linkages and spoliation		- Digital Evidence Evaluation o Hypotheses testing and generation of new hypotheses o Evaluation of evidential requirements in relevant sections of the Penal Code o Analysis of meaning
Presentation				
		- Document the result of the relevant activities from the Digital Forensics Process phases - Result of identification phase o Documentation(description and photo) of where found, configuration and state - Result of analysis phase o Mandate/scope of the analysis o Technical analysis o Digital Evidence evaluation		- Document the result of relevant activities from the Digital Forensics Process phases - Result of identification phase o Purpose for seizure o Relevant contextual factors - Result of analysis phase o Scope of the analysis o Content analysis o Digital Evidence Evaluation

Figure 5-3: Detailed model of necessary types of competence in the Digital Forensics Process within a criminal investigation.

5.2.3 Organisational challenges

Are organisational challenges sources of errors in the relation to handling digital evidence in a criminal investigation?

5.2.3.1 Competency requirement

As described in chapter 2.4.2, there are currently no specified competence requirements for handling digital evidence in a criminal investigation. The Norwegian Police Directorate has stated that digital evidence should only be collected by personnel with “appropriate competence” and “adequate training”, but has not explained which knowledge components these terms represent.

In the ongoing pilot project in the Oslo Police District (see chapter 2.4.2.), one of the tasks is to provide input to a potential competency requirement. This will hopefully lead to defined levels of required competence for the different tasks related to handling of digital evidence.

The participants did not highlight lack of competency requirements as a problem for themselves, but several were concerned about the level of technological knowledge among most of the CDs (see chapter 4.6.1).

The participants without police background described their tasks during investigation of digital evidence. These tasks were carried out without any formal investigative competence, and several expressed the desire to gain basic skills in this respect. However, when relevant educations at the Norwegian Police University College were scheduled, they were often not prioritized among the applicants from the police district.

The findings in the survey show that the investigation of digital evidence was performed by DFDs without formal investigative competence. This underpins the need for defining competency requirements, which should include both technological and investigative competence components.

5.2.3.2 Culture and structure

Due to the ongoing police reform there are major changes in the structure of the police organisation under implementation (see chapter 2.4.3). The DFD liaison is a new function, and the Oslo Police District has implemented this function as part of the aforementioned pilot project (see chapter 2.4.3). Several of the participants were positive to the new function, and told that the DFD liaisons could contribute to a better understanding between the CD and DFD because they had both investigative and technological competence (see chapter 4.9.1). Some of the DFDs told that they already had experienced improvement in relation to the amount of digital evidence being seized and analysed.

In relation to these major structural changes, there is a risk that the system might be moved out of balance. In order to sustain or re-establish the balance the culture must be payed necessary attention (see chapter 2.4.3). If not, the expected positive effects of the structural changes may not be achieved.

The participants emphasised the importance of having routines for prioritizing which cases to work with (see chapter 4.5.4). They also highlighted the well-functioning procedure for

defining the mandate of the task (see chapter 4.6.1). They underlined the advantage of being involved in the investigation at an early stage, as well as being included in the investigation team (see chapter 4.3). There was no procedure or routine description in place to support these activities, except when extraordinary situations occurred, e.g. a terror attack. In this respect, the quality and efficiency of a criminal investigation could benefit from defining the procedure of cooperation between the CD and DFD including the aforementioned elements when handling digital evidence in a criminal investigation.

5.2.3.3 Backlogs

Large backlogs are problematic in relation to the speediness of the investigation of digital evidence (see chapter 2.4.4). The survey indicates that the problem seems to be caused by a combination of lack of technological competence and necessary resources.

The participants told that the increasing backlogs to some extent were caused by uninformed decisions about seizure (see chapter 4.5.2). They were optimistic because of the implementation of DFD liaisons, and expected the backlogs to reduce over time as a result of this measure (see chapter 4.9.1).

As the study has revealed, the problem might be more complex, due to several x-factors. The increasing backlog may be explained with several of the other identified challenges, e.g. wide mandates (see chapter 4.6.1), absence of the right competence (see chapter 4.4), delays because of pending decisions and prioritizations (see chapter 4.4 and 4.5.4) communication challenges due to the use of different systems for task management (see chapter 4.6.1) or frequent change of CD responsible for the case (see chapter 4.4). Within these challenges several variables that could affect the increasing backlog could be derived. These variables could be relevant to further research.

Summary

To summarize, the study indicates that several organisational challenges may constitute non-technical sources of errors when digital evidence is investigated. The terms “appropriate competence” and “adequate training” are not described in detail in relation to the competence components required to perform the tasks of the Digital Forensic Process.

The study indicates that there is no defined procedure for cooperation between the CD and the DFD during a criminal investigation. Such a procedure could contribute to ensure that important measures beneficial to the quality or efficiency of the investigation are carried out routinely.

The problem of large backlogs has been and seems still to be a challenge, and should be investigated further.

5.3 What are the consequences if these errors occur?

The study has identified several sources of errors, and if they are not prevented or eliminated, the errors might occur. I have limited my discussion to consequences that pose a risk for the rule of law for the involved parties.

Inadequate technological and investigative competence may cause errors that have consequences for the quality and efficiency of the investigation. If competency criteria are not defined, there is an increased risk of errors due to detectives conducting tasks they are not skilled to do. These errors can be e.g. misinterpretations of evidential value, false negatives due to erroneous conclusions about absence of information (see chapter 2.2.2.4.b) or evidence being overlooked. There is also a risk that such errors might stay undetected during the investigation, since the general technological competence within law enforcement seems to be low.

If the *right competence is not present at the right time*, this may lead to several errors.

The result of a phase can only be as good as the result of the former phases. The errors from the identification, analysis and presentation phase could propagate from one phase to another. In other words, the possibility of proving guilt or innocence may be lost or disrupted due to inadequate skills by those planning and conducting the identification phase.

E.g. if the potential source of evidence is not be identified or collected due to inadequate competence, this error propagates into the analysis phase. The result of the analysis phase depends on the quality of the former phase, e.g. whether the seized data holds relevant,

complete and reliable information. The presentation of this evidence in a report may only be as good as the result of the analysis, resulting in lower quality of the presentation phase.

In the analysis phase there are several challenges with mandates. If they are defined too wide or too narrow, this might lead to untargeted, partial or biased analyses of seized data (see chapter 2.2.2.4.b). However more importantly, a mandate which is not anchored in the hypotheses of the case is a bigger problem because in such a situation a targeted, unbiased and objective analysis is more due to chance - and this may have consequences for both quality and efficiency of the investigation.

The anchoring to the hypotheses of the case is necessary to ensure a structured approach to the seized data, which is suitable to test the competing hypotheses of the case in an unbiased and efficient manner (see chapters 2.2.3 and 2.3.5).

If the detective has technological competence, but no investigative competence there are several risks:

- The presumption of innocence might not be adequately addressed (see chapter 2.2.1).
- The conditions for criminal liability may not be adequately considered (see chapter 2.2.1).
- The competing hypotheses may not be identified or tested (see chapter 2.2.3).
- Relevant information is not revealed due to lack of knowledge of crime phenomena (N. Sunde, 2016, chapters 4.1 and 5.1).

In the presentation phase, poor documentation of the evidence might lead to misinterpretations of the evidential value of the individual evidence, or cause an erroneous or inaccurate perception the total evidence situation of the case.

Bias might occur in all the above mentioned phases, and may lead to evidence being overlooked or misinterpreted in terms of relevance and value (see chapter 2.3).

The errors occurring when handling digital evidence may cross contaminate other lines of evidence (see chapter 2.3.5). Since the reliability of evidence is established by e.g. cross checking it against other evidence, an improper interpretation of digital evidence accuracy,

linkages, causation, spoliation and meaning may cause an erroneous determination of other evidences reliability.

A poor identification, analysis and/or presentation phase might lead to inadequate penalties, or to people being wrongfully convicted or acquitted.

Errors caused by *organisational challenges* might have several consequences.

Cooperation characterized by randomness and lack of regulations might increase the risk of the right competence being absent when needed. This will affect the following identification, analysis and presentation of evidence - and may as mentioned have consequences for quality, efficiency and rule of law.

Large backlogs could seem to be solely an efficiency problem. If the causes of the problem are not precisely identified, there is a risk of wasting resources on ineffective measures which will not solve the problem. However, backlogs may also be a quality problem, since a lengthy investigation caused by large backlogs may lead to reduction of the penalty if the suspect is found guilty.

5.4 How can the errors be prevented or countered?

The examples provided by the participants shows that the DFD being included into the investigation team, preferably at an early stage of the investigation, clear leadership and adequate allocation of resources are important factors for good cooperation between CD and DFD when investigating digital evidence.

The sources of errors may be prevented or countered:

At an individual level:

There is a need to define competence criteria for handling digital evidence during a criminal investigation. It is also necessary to specify the terms “adequate training” and “appropriate competence” (see chapter 2.4.2) in relation to both technical and investigative competence.

At a cooperation level:

To avoid wrongful decisions about seizure, in respect of relevant evidence not being collected, preview should be used to support this decision. Investigative competence as well as case knowledge must be available to assess whether the information revealed in the preview indicates that the device/data is relevant to test the hypotheses of the case.

The investigation of digital evidence would most likely benefit from a common platform for the CD and the DFD; such as System A; for task management.

To counter errors in relation to hypotheses generation and testing, the investigation should be carried out in line with The Investigative Cycle (Fahsing, 2016, p. 20). The hypotheses should be written down (see chapter 2.3.5) kept in an updated state, and available to all who are conducting investigative tasks in the case (Riksadvokaten, 2016b).

In order to prevent errors caused by bias and heuristics effective countermeasures should be applied, such as:

- Knowledge and awareness measures about bias and heuristics, since the DFDs without police background could lack this knowledge (see chapter 4.8.6).
- Hypotheses based approach – where the general rule is that the hypotheses form the basis for any task, to facilitate an unbiased investigation safeguarding objectivity, presumption of innocence and the rule of law. The hypotheses should be available in a common system to all detectives with tasks in relation to the investigation.
- To prevent bias and heuristics, such as confirmation bias and group think, a structure where the decisions and conclusions are routinely challenged would be beneficial. The measure ‘Devil’s Advocate’ (see chapter 2.3.5) could be implemented as a routine.
- A routine-based assessment of reports could also be a measure to detect if the analysis is carried out by a detective with inadequate competence – and possibly stop erroneous evidence from cross-contaminating other lines of evidence.
- In cases of serious crime with little 5WH information, the Linear Sequential Unmasking (see chapter 2.3.5) could be a relevant approach to facilitate an open and unbiased first assessment of the seized data. This approach increases the ability to discover information that would otherwise be overlooked due to bias.

- To avoid bias caused by informal debriefing, a routine could be implemented to safeguard this activity being carried out by colleagues with no role in the case, or a professional psychologist.

The impact of the suggested countermeasures against bias relies on whether a culture where the detectives are open to and believe in the advantages of such a countermeasure being established (see chapter 2.4.3). The structural changes could therefore be accompanied by measures to develop a culture where challenging each other's decisions and asking for a second opinion is done on a regular basis.

At an organisational level:

In a readiness perspective, a competence plan could contribute to ensure the sufficient competence available in the organisation. The plan should cover both technological and investigative competence.

A routine description should be produced to facilitate structured cooperation. The routine description should outline when the different competence's must be available, to ensure involvement of the right competence at the right time during the phases of the Digital Forensics Process (see Figure 5-3). A routine description could also include regulate how mandates should be formed and the prioritizing of cases.

The problem of the increasing backlog should be subject to further research, to ensure an informed decision basis for the measures to counter this challenge.

5.5 The real life examples

All the participants provided real-life examples which could illustrate cooperation they believed had positive impact on to the quality or efficiency of the investigation.

The DFDs highlighted to be *included in the investigation team* as an important factor.

Several of the examples have a significant element in common. By being involved, the DFD seems to get a deeper understanding of the information requirement of the case. Instead of

being told what to do, the DFD gets the opportunity to make use of own competence to suggest approaches that may contribute to providing the necessary information.

A very good illustration of this is the meeting in a child molesting case referred by a DFD (see chapter 4.3). During the meeting the information requirement is discussed, and the DFD suggests testing a new methodology to provide the necessary information. What makes this illustration so good is that this approach would most likely never be thought of by a CD without the technical competence possessed by the DFD. The creative approach is a result of the DFD using his/her competence to think about how he/she may solve the information requirement.

It seems like the involvement in the investigation team makes the DFD take ownership of the case, which again leads to the DFD putting more effort and creativity into solving the tasks compared to when the DFD is requested to perform a task with no further involvement. The description from the CD of the DFD in the child homicide case gives clear indications of this (see chapter 4.3). The CD describes the DFD as the most determined “mole” s/he had ever met. The DFDs involvement in this case was lengthy, and required a vast amount of mental endurance.

To be *involved in the investigation at an early stage* was also highlighted by the DFDs. In such situations it was possible to plan for what type and level of competence, equipment and level of assistance the Computer Crime Department should provide at e.g. a search scene. The early involvement had also led to important evidence being uncovered at an early stage so that it could be brought into the first police interview of the suspect. As a result the suspect confessed to having committed the crime, and the case was solved rapidly.

There were examples where clear leadership and good communication was underlined. Adequate allocation of resources did also seem to have a significant impact on the efficiency of the cooperation and the quality of the results (see chapter 4.3).

6. CONCLUSIONS

By including theories from different disciplines such as law, forensic psychology, investigative methodology and digital forensics - and by obtaining information from informants, a number of sources of errors when investigating digital evidence during the Digital Forensic Process were identified in this study:

6.1 Insufficient investigative competence

To investigate digital evidence in a criminal case, investigative competence is required. The components of investigative competence can be summarized to:

- *Knowledge about ICCPR and ECHR*
- *Knowledge about the Penal Code - and evidential requirements*
- *Knowledge about Criminal Procedure Code – principles, obligations and coercive measures*
- *Knowledge about relevant crime phenomena*
- *Skills in use of The Investigative Cycle*
- *Skills in hypothesis generation and testing*
- *Knowledge about relevant biases, and sufficient countermeasures*
- *Knowledge and skills in relation to the procedures of a criminal investigation, and the relevant investigative methods*
- *Documentation and presentation skills*

6.2 The right competence is not present at the right time

The handling of digital evidence in a criminal investigation requires both technological and investigative competence. The DFD and the CD have complementary competence, but this study indicates that they rarely possess the combination of necessary competence alone.

An alternative to every DFD developing investigative competence is to ensure that the sufficient types of competence are present at the right time. This is particularly important when decisions and tasks within the Digital Forensics Process phases that require

investigative competence are carried out. This requires a form of cooperation that facilitates optimal utilization of the different competences, as well as prevention and countering of errors.

The limitation of both the Digital Forensics Process and The Investigative Cycle in this context is that they do not provide any guidance about how this cooperation should be the carried out to ensure quality and efficiency in the investigation of digital evidence. The present study gives basis for an outline of the necessary competence components related to the Digital Forensics Process in the context of a criminal investigation. By implication, the outline can be understood as a proposal of the technical and investigative competence requirements for the identification, analysis and presentation phase.

Importantly, a combination of investigative and technological competence is needed in all these phases. In the thesis, this has been discussed in relation to:

- The identification phase, when planning of searches or decisions about seizure is made.
- The analysis phase, when the mandate is decided upon, and where the hypotheses generation and testing is conducted within three analysis sub-phases.
- The presentation phase, when the result of the handling of the evidence in the former phases is documented in reports together with a presentation of the evidence itself.

A component within the investigative competence is knowledge about bias, heuristics and countermeasures. This study has uncovered lack of knowledge and efficient countermeasures against these cognitive limitations, which constitute major risks of errors in the investigation of digital evidence.

6.3 Organisational Challenges

There are no defined competency criteria for handling digital evidence within a criminal investigation. The Norwegian Police Directorate has stated that this only should be carried out by personnel with “adequate training“ and “appropriate competence”, but has not outlined the meaning of these terms.

There are no routines defining how the cooperation between a CD and a DFD should be done during criminal investigation. This has implications for communicating the tasks, prioritizing of cases and when the right competence is involved in the investigation team.

Large backlogs have been and are still a problem for the quality and efficiency of investigation of digital evidence.

6.4 Consequences

The identified errors may lead to:

- Insufficient or poor quality, due to the investigation being inadequately purpose oriented in relation to the information requirement of the case.
- Inefficient investigations and lengthy case processing, caused by an unnecessarily large scope of the analysis.
- Inadequate protection of the rule of law, caused by errors in the investigation. The errors might origin from partial investigation of digital evidence, insufficient hypotheses generation or testing, or poor investigation in relation to the evidential requirements.

6.5 Countermeasures

The sources of errors may be prevented or countered:

On *the individual level*, by the individual detective having sufficient technological and investigative competence, as well as knowledge about the limitations of own competence.

On *cooperation level*, by the parties knowing which technological and investigative competence components that are required in the steps of Digital Forensics Process, and ensuring that the sufficient competence is available when necessary. A routine description could be developed to facilitate a structured cooperation.

The cooperation between the CD and DFD would benefit from a common platform for task management where the hypotheses of the case are available, as well as a description of the information requirement for testing the hypotheses.

To prevent bias and heuristics, such as confirmation bias and group think, a structure where the decisions and conclusions are routinely challenged would be beneficial. The impact of such a measure depends on whether a culture where the detectives are open to and believe in the advantages of such a countermeasure is established.

On an *organisational level*, by creating a plan for competence development in relation to both technological and investigative competence. A thoughtful organizational and physical location of the DFDs also seems to matter.

6.6 Real life examples

The examples provided by the participants show that the DFD being included into the investigation team, preferably at an early stage of the investigation, clear leadership and adequate allocation of resources are important factors for good cooperation between CD and DFD when investigating digital evidence.

7. FUTURE WORK

There are several variables that could affect the quality and efficiency when handling digital evidence within a criminal investigation. On the basis of the information given by the participants, there are several aspects that could be subject to further research:

First and foremost, the scope of the thesis has been limited the research to the Oslo Police District. To survey the cooperation between CDs and DFDs in other police districts would give a broader insight into how the investigation of digital evidence is carried out in the Norwegian police.

In relation to the Digital Forensics Process, the decisions concerning seizure are critical to the investigation, since the decision has an impact on the scope of the seized material. A decision which is too narrow may lead to important evidence being left out, whereas a decision which is too broad may result in a vast amount of data which is too time- and resource consuming to be efficiently dealt with. If the wrong decision is made, this will be an unrecoverable error

that will limit the quality of all the further phases. Research could give more insight into on what basis these decisions are made. Further research on the use of preview of potential digital evidence could provide answers to whether more extensive use of this approach could lead to higher quality and efficiency in criminal investigations.

The hypotheses of the case, as well as the relevant sections of the Penal Code should constitute the basis for all the investigation tasks in a criminal investigation. Research could give more insight into whether this actually is the situation when tasks in relation digital evidence are defined.

Based on the discussion in this thesis, to develop and maintain adequate technological and investigative competence for all the individual detectives seems to be an unachievable goal. Further research could give more insight into whether there is awareness in relation to the necessary types of competence, whether they are in place when the different tasks are carried out, and how this is organised. Research concerning how the competence could be utilized in the best possible manner during the criminal investigation could be beneficial to the development of routines and structures in relation to organizing criminal investigation.

In relation to organisational challenges, the increasing backlogs should also be given more attention from a research point of view. There are several measures carried out in the police that seem to be based on the assumption that the increasing backlog is caused by a lack of personnel with technological competence. To counter the problem, more personnel with technological background have been recruited to the police. Several measures to raise the technological competence among CDs have also been done, e.g. more focus on technological competence in the police education and the implementation of DFD liaisons in the Oslo Police District. There might be several other variables that affects the increasing backlog, and thus should be looked into. Research could provide a better information basis for the decision about measures to reduce the backlog, hence improving the quality and efficiency in relation to investigation of digital evidence.

8. BIBLIOGRAPHY

Ask, K. (2013). Bias: Fejl og faldgruber i efterforskning. In C. Hald & K. Vrist Rønn (Eds.), *Om at opdage: Metodiske refleksioner over politiets undersøgelsespraksis*. Fredriksberg: Samfundslitteratur.

Bang, H. (2013). Organisasjonskultur: En begrepsavklaring. *Tidsskrift for norsk psykologforening*. *50*(4), 326-336.

Bjerknes, O. T., & Johansen, A. K. H. (2009). *Etterforskingsmetoder - en innføring*. Bergen: Fagbokforlaget.

Bjerknes, O. T., & Williksen, E. (2015). *Politirapport, 4. utgave*. Høvik: Vett & viten.

Burch, N. (1970). *The four stages for learning any new skill*. Solana beach: Gordon Training International.

Carrier, B. (2005). *File system forensic analysis*. Upper Saddle River: Addison-Wesley Professional.

Carrier, B., & Spafford, E. H. (2004). *An event-based digital forensic investigation framework.* Paper presented at the Digital forensic research workshop.

Casey, E. (2002). Error, uncertainty, and loss in digital evidence. *International Journal of Digital Evidence, 1*(2), 1-45.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic science, computers and the Internet*. Amsterdam: Elsevier.

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

Christianson, S. Å., & Montgomery, H. (2008). Kognition i ett rättspsykologiskt perspektiv. In P. Granhag & S. Å. Christiansson (Eds.), *Handbok I rättspsykologi*. Malmø: Liber AB.

Creswell, J. W. (2013). *Choosing Among Five Approaches*. Thousand Oaks: Sage.

Dean, G. (2000). *The experience of investigation for detectives.* (Doctoral Dissertation, Queensland University of Technology), Dean, G., Brisbane.

Dilijonaite, A. (2017). Digital Forensic Readiness. In A. Årnes (Ed.), *Digital Forensics. An Academic Introduction*: Preprint.

Dror, I. E. (2011). The paradox of human expertise: why experts get it wrong In N. Kapur (Ed.), *The paradoxical brain* (pp. 177-188). Cambridge: Cambridge University Press.

Dror, I. E. (2013). The ambition to be scientific: human expert performance and objectivity. *Science and Justice, 53*(2), 81-82.

Dror, I. E., Thompson, W. C., Meissner, C. A., Kornfield, I., Krane, D., Saks, M., & Risinger, M. (2015). Letter to the Editor-Context Management Toolbox: A Linear Sequential Unmasking (LSU) Approach for Minimizing Cognitive Bias in Forensic Decision Making. *Journal of forensic sciences, 60*(4).

ECHR. *European Convention on Human Rights (ECHR)*.

Edmond, G., Tangen, J. M., Searston, R. A., & Dror, I. E. (2015). Contextual bias and cross-contamination in the forensic sciences: the corrosive implications for investigations, plea bargains, trials and appeals. *Law, Probability and Risk, 14*(1), 1-25.

Ekfeldt, J. (2016). *Om informationstekniskt bevis.* (Doctoral Dissertation, Juridiska Institutionen, Stockholms Universitet), Ekfeldt, J. , Stockholm.
Fahsing, I. A. (2013). Tænkestile: effektivitet, dyder, krydspres i efterforskninger. In C. Hald & K. Vrist Rønn (Eds.), *Om at opdage: Metodiske refleksioner over politiets undersøgelsespraksis*. Fredriksberg: Samfundslitteratur.
Fahsing, I. A. (2016). *The Making of an Expert Detective. Thinking and Deciding in Criminal Investigations.* (Doctoral Dissertation, University of Gothenburg), Fahsing, I. A., Gothenburg.
Fahsing, I. A., & Rachlew, A. (2015). Politiavhøret. In R. Aarli, M. Hedlund, & S. E. Jebens (Eds.), *Bevis i straffesaker*. Oslo: Gyldendal.
Flaglien, A. O. (2017). The Digital Forensics Process. In A. Årnes (Ed.), *Digital Forensics. An Academic Introduction*: Preprint.
Forst, B. (2004). *Errors of justice: Nature, sources and remedies*. Cambridge: Cambridge University Press.
Gawande, A. (2010). *The checklist manifesto: How to get things right*. New York: Metropolitan Books.
Grunnloven. (1814). *Kongeriket Norges Grunnlov*.
Hamremoen, E. (2016). *Kriminalteknikk: Første enhet på åstedet. 2. utgave*. Oslo: Gyldendal.
Heuer, R. J., & Pherson, Y. (2015). *Structured analytic techniques for intelligence analysis (2nd edition)*. Thousand Oaks: SAGE CQ press.
Hitchcock, B., Le-Khac, N., & Scanlon, M. (2016). Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists. *Digital Investigation, 16*, S75-S85.
ICCPR. (1966). *International Covenant on Civil and Political Rights*.
Justis- og beredskapsdepartementet. (2015). *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*. Oslo: Justis- og beredskapsdepartementet.
Kafle, N. P. (2013). Hermeneutic phenomenological research method simplified. *Bodhi: An Interdisciplinary Journal, 5*(1), 181-200.
Kjelby, G. J. (2015). Bevisrettens grunnprinsipper og hovedregler i straffesaker. In R. Aarli, M. Hedlund, & S. E. Jebens (Eds.). Oslo: Gyldendal.
Kolflaath, E. (2015). En metode for bevisbedømmelsen i straffesaker. In R. Aarli, M. Hedlund, & S. E. Jebens (Eds.), *Bevis i straffesaker*. Oslo: Gyldendal.
Kruse, W. G., & Heiser, J. G. (2002). *Computer Forensics. Incident Response Essentials*. Indianapolis: Pearson Education.
Kvale, S., & Brinkmann, S. (2009). *Interview*. København: Hans Reitzel.
Leedy, P. D., & Ormrod, J. E. (2014). *Practical Research Planning and Design.* Harlow: Pearson Education Limited.
Lloyd, T. W. (2000). *Management*. Orlando: Dryden Press.
Marshall, C., & Rossmann, G. B. (2006). *Designing qualitative research interviewing*. Thousand Oaks: Sage.
Mills, C. M., & Keil, F. C. (2004). Knowing the limits of one's understanding: The development of an awareness of an illusion of explanatory depth. *Journal of Experimental Child Psychology, 87*(1), 1-32.

Myhrer, T. (2001). *Etterforskningsbegrepet: Avgrensning, vilkår, roller og ansvar*. *Tidsskrift for strafferett, 1*(1), 6-30.
Myhrer, T. (2014). *Kvalitet i etterforskningen. Særlig om påtaleansvarliges rolle og betydning. Delrapport i «Etterforskningsprosjektet»* Retrieved from https://brage.bibsys.no/xmlui/bitstream/handle/11250/282259/kvalitet_i_etterforskningen.pdf?sequence=1&isAllowed=y
Myklebust, T. (2010). Politiavhør som metode *Arbeidsmetoder og metodearbeid i politiet*. Oslo: Politihøgskolen.
NOU 2015:13. (2015). *Digital sårbarhet - sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Oslo: Departementenes sikkerhets- og serviceorganisasjon, Informasjonsforvaltning.
Olsvik, E. H. (2013). *Vitenskapsteori for politiet: tenkemåter for kunnskapsstyrt politiarbeid*. Oslo: Gyldendal Akademisk.
Oslo Politidistrikt. (2017). *Foreløpig rapport fra pilotprosjekt om IKT og internett i politiarbeidet. Tiltak 8 i Justis- og beredskapsdepartementets strategi for bekjempelse av IKT-kriminalitet*. Oslo: Oslo Politidistrikt.
Politidirektoratet. (2010). *Behandling av beslag i straffesaker. (Rundskriv RPOD-2010-7)*. Oslo: Politidirektoratet.
Politidirektoratet. (2012). *Politiet i det digitale samfunnet. En arbeidsgrupperapport om: elektroniske spor, IKT-kriminalitet og politiarbeid på Internett*. Oslo: Politidirektoratet.
Politidirektoratet. (2013). *Etterforskningen i politiet*. Oslo: Politidirektoratet.
Politidirektoratet. (2016). *Rammer og retningslinjer for etablering av nye politidistrikter Versjon 1.1 av 26. august 2016*. Oslo: Politidirektoratet.
Politidirektoratet, & Riksadvokaten. (2016). *Handlingsplan for løft av etterforskningsfeltet*. Retrieved from http://riksadvokaten.no/filestore/Dokumenter/2016/Etterforskningslftet_POD_final.pdf.
Politihøgskolen. (2012). *Videreutdanning for Nordic Computer Forensic Investigators Introduction Module 1*. Retrieved from http://www.phs.no/Documents/2_Studietilbud/3_EVU/Godkjent%20studieplan%20NCFI%20%20Introduction%20modul%201%20-%20hogskolestyret%206%20juni%202012.pdf.
Politihøgskolen. (2013). *Videreutdanning for Nordic Computer Forensic Investigators Module 2*. Retrieved from http://www.phs.no/Documents/2_Studietilbud/3_EVU/Studieplan%20NCFI_Module_2_revidert%202706%202013%20med%20pensumendr%201509%202014-1.pdf?epslanguage=no.
Politihøgskolen. (2015). *Forskningsetisk veileder for Politihøgskolen, 2. utgave*. Oslo: Politihøgskolen.
Politihøgskolen. (2016). *Fagplan Bachelor - Politiutdanning 2016 - 2019*. Retrieved from http://www.phs.no/Documents/5_Studenter/Fagplaner/Fagplan%202016%20til%202019.pdf.

Politiinstruksen. (1990). *Alminnelig tjenesteinstruks for politiet*.
Rachlew, A. (2009). *Justisfeil ved politiets etterforskning: noen eksempler og forskningsbaserte mottiltak* (Doctoral Dissertation, Det Juridiske Fakultet, Universitetet i Oslo), Rachlew, A., Oslo.
Rachlew, A. (2010). Å forske på sine egne *Arbeidsmetoder og metodearbeid i politiet*. Oslo: Politihøgskolen.
Riksadvokaten. (2015). *Norsk politi og påtalemyndighets behandling av straffesakene mot Sture Bergwall – Hva kan vi lære? Rapport fra arbeidsgruppe. (Riksadvokatens publikasjoner nr. 3/2015)*. Retrieved from http://riksadvokaten.no/filestore/Dokumenter/2015/Riksadvokatenspublikasjoner3_2015.pdf
Riksadvokaten. (2016a). *Mål og prioriteringer for straffesaksbehandlingen i 2016 - politiet og statsadvokatene. (Rundskriv 1:2016)*. Retrieved from http://riksadvokaten.no/filestore/Dokumenter/2016/Ml-ogprioriteringsskriv2016.pdf.
Riksadvokaten. (2016b). *Politiavhør. (Rundskriv 2:2016)*. Retrieved from http://riksadvokaten.no/filestore/Dokumenter/2016/Avhrsrundskriv.pdf.
Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). *Computer forensics field triage process model.* Paper presented at the Proceedings of the conference on Digital Forensics, Security and Law.
Straffeloven. (2005). *Lov om straff*.
Straffeprosessloven. (1981). *Lov om rettergangen i straffesaker*.
Sunde, I. M. (2015). Databevis. In R. Aarli, M. Hedlund, & S. E. Jebens (Eds.), *Bevis i straffesaker*. Oslo: Gyldendal.
Sunde, I. M. (2017). Cybercrime Law. In A. Årnes (Ed.), *Digital Forensics. An Academic Introduction*: Preprint.
Sunde, N. (2016). *Non-technical errors and uncertainties of electronic evidence.* (Project report from preliminary study, NTNU), Gjøvik, Sunde, N.
Tilstone, W., Hastrup, M. L., & Hald, C. (2013). *Fischer's Techniques of Crime Scene Investigation*. Boca Raton: CRC Press.
Tjora, A. (2013). *Kvalitative forskningsmetoder i praksis, 2. utgave*. Oslo: Gyldendal Akademisk.
UNODC. (2013). *Comprehensive Study on Cybercrime*. New York: United Nations.

9. APPENDIXES

Appendix 1: NSD approval

Appendix 2: Consent form

Appendix 3: Interview guide

Appendix 4: Sunde, N. (2016). *Non-technical errors and uncertainties of electronic evidence.* (Project report from preliminary study, NTNU). N. Sunde, Gjøvik.

Appendix 1

Inger Marie Sunde
Politihøgskolen
Postboks 5027 Majorstua
0301 OSLO

Vår dato: 25.10.2016 Vår ref: 50252 / 3 / AGH Deres dato: Deres ref:

TILBAKEMELDING PÅ MELDING OM BEHANDLING AV PERSONOPPLYSNINGER

Vi viser til melding om behandling av personopplysninger, mottatt 27.09.2016. Meldingen gjelder prosjektet:

50252	*Non technical errors and uncertainties with Electronic evidence*
Behandlingsansvarlig	*Politihøgskolen, ved institusjonens øverste leder*
Daglig ansvarlig	*Inger Marie Sunde*
Student	*Nina Sunde*

Personvernombudet har vurdert prosjektet og finner at behandlingen av personopplysninger er meldepliktig i henhold til personopplysningsloven § 31. Behandlingen tilfredsstiller kravene i personopplysningsloven.

Personvernombudets vurdering forutsetter at prosjektet gjennomføres i tråd med opplysningene gitt i meldeskjemaet, korrespondanse med ombudet, ombudets kommentarer samt personopplysningsloven og helseregisterloven med forskrifter. Behandlingen av personopplysninger kan settes i gang.

Det gjøres oppmerksom på at det skal gis ny melding dersom behandlingen endres i forhold til de opplysninger som ligger til grunn for personvernombudets vurdering. Endringsmeldinger gis via et eget skjema, http://www.nsd.uib.no/personvern/meldeplikt/skjema.html. Det skal også gis melding etter tre år dersom prosjektet fortsatt pågår. Meldinger skal skje skriftlig til ombudet.

Personvernombudet har lagt ut opplysninger om prosjektet i en offentlig database, http://pvo.nsd.no/prosjekt.

Personvernombudet vil ved prosjektets avslutning, 31.10.2017, rette en henvendelse angående status for behandlingen av personopplysninger.

Vennlig hilsen

Kjersti Haugstvedt

Agnete Hessevik

Kontaktperson: Agnete Hessevik tlf: 55 58 27 97
Vedlegg: Prosjektvurdering

Dokumentet er elektronisk produsert og godkjent ved NSDs rutiner for elektronisk godkjenning.

NSD – Norsk senter for forskningsdata AS Harald Hårfagres gate 29 Tel: +47-55 58 21 17 nsd@nsd.no Org.nr. 985 321 884
NSD – Norwegian Centre for Research Data NO-5007 Bergen, NORWAY Faks: +47-55 58 96 50 www.nsd.no

Appendix 2

Forespørsel om deltakelse i forskningsprosjektet

Masteroppgave: «Ikke-tekniske feil og usikkerhetsmomenter ved etterforskningen av elektroniske bevis» v/ Nina Sunde

Bakgrunn og formål

Dataetterforsker og etterforsker vil i utgangspunktet kunne inneha nødvendig komplementær kompetanse for å etterforske elektroniske bevis på en måte som innebærer god kvalitet og effektivitet, og som forebygger justisfeil.

Situasjonen i dag er likevel preget av lang saksbehandlingstid, ulik organisering av arbeidet og usikkerhet omkring hvem som skal gjøre hva med elektroniske bevis i straffesakskjeden.

I mitt masterstudie ved PHS/NTNU Gjøvik vil jeg forsøke å identifisere hvorvidt det er et «gap» i kompetansen mellom dataetterforsker og etterforsker ved håndteringen av elektroniske bevis i straffesakskjeden. Dersom jeg finner dette «gapet» vil jeg forsøke å identifisere mulige årsaker til dette, med fokus på kunnskap/ferdigheter, organisatoriske utfordringer og bias. Jeg vil forsøke å identifisere eksempler på god praksis, med andre ord – hva som fungerer, og hvorfor.

Informantene er dataetterforskere (med eller uten politibakgrunn) eller etterforskere fra Oslo Politidistrikt som har samarbeidet om elektroniske bevis i straffesakskjeden.

Hva innebærer deltakelse i studien?

Studien blir gjennomført ved å intervjue informanter og analysere resultatet fra intervjuene opp imot relevant teori.

Intervjuene vil gjennomføres en til en, og vil vare 1- 1 ½ timer. Spørsmålene vil dreie seg prosessen for behandling av elektroniske bevis, med hovedfokus på planlegging, analyse og presentasjon. Samarbeid med andre aktører i straffesakskjeden vil også være relevant. Tema som kompetanse og organisatoriske utfordringer vil også bli berørt. Intervjuene blir tatt opp på lyd.

Hva skjer med informasjonen om deg?

Alle personopplysninger vil bli behandlet konfidensielt. Det er kun jeg som har tilgang til personopplysningene, og disse vil lagres adskilt fra intervjudataene. Intervjuene vil danne grunnlag

for analysen som presenteres i rapporten (masteroppgaven). Deltakernes navn vil ikke bli brukt i rapporten, og det vil heller ikke bli gitt inngående beskrivelser av person eller arbeid som vil kunne identifisere deltakerne. Dersom opplysninger om bakgrunn blir benyttet i tilknytning til sitater, vil du få anledning til å lese gjennom disse.

Prosjektet skal etter planen avsluttes 01.06.17, og personopplysninger og opptak blir slettet når endelig sensur på masteroppgaven er klar (september/oktober 2017).

Frivillig deltakelse
Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn. Dersom du trekker deg, vil alle opplysninger om deg bli anonymisert.

Dersom du ønsker å delta eller har spørsmål til studien, ta kontakt med meg, Nina Sunde, tlf. 91660069. Veileder er Inger Marie Sunde, Politihøgskolen, tlf. 91660052. Studien er meldt til Personvernombudet for forskning, NSD - Norsk senter for forskningsdata AS.

Samtykke til deltakelse i studien

Jeg har mottatt informasjon om studien, og er villig til å delta

---

(Signert av prosjektdeltaker, dato)

Appendix 3

Intervjuguide – Master's Thesis:

NB: Husk å underskrive på samtykkeskjema!

Formalia

Alder, utdanning, år i politiet, derav med etterforskning, erfaring med etterforskning,

Politi (etterforskningsrelevant) utdanning eller kurs

Begrenset politimyndighet og evt. kurs i tilknytning til dette

Spesielle saksfelt du jobber med?

Egen rolle

- Beskrive sin rolle prosessen med elektroniske bevis i en typisk etterforskning (av saksfeltet han/hun jobber med)

Beskrive etterforskningens gang (etterforskningsprosessen) i saksfeltet han/hun jobber med

- Hvordan er gangen i en typisk etterforskning som du deltar i fra begynnelse til slutt.
- Hvordan følger du utviklingen i saken?
- Hvordan vet du hva du skal gjøre til enhver tid i saken? (Etterforskningsplan? Mandat?)

Kvalitet og effektivitet vil være begrep som går igjen i dette intervjuet.

- Hva tenker du kjennetegner en etterforskning med høy kvalitet?
- Hva tenker du kjennetegner en etterforskning gjennomført med høy effektivitet?

Det gode eksemplet

- Fortell om en sak hvor samarbeidet gikk godt. Vær konkret og detaljert, og
    - Hvorfor fungerte det fint?
    - Selv om dette er et eksempel på godt samarbeid, hva kunne evt. vært enda bedre?

Eksemplet på dårlig utfall

- Fortell om en sak hvor samarbeidet ikke gikk godt
    - Hva konkret var det som gjorde at samarbeidet ikke fungerte godt?
    - Evt. hva fungerte som det skulle?

Samarbeid med etterforsker/dataetterforsker (ta utgangspunkt i utvalgte faser i Digital Forensics Process – (identification – collection – examination – analysis - presentation)

- I planleggingsfasen
  - Hvordan foregår planleggingsfasen når potensielle elektroniske bevis skal sikres
  - Hvordan tas beslutningen om hva som skal beslaglegges
  - Hvordan tas beslutningen om hva som skal sikres og undersøkes
  - Hvordan tas beslutningen om evt. live-sikring (hva legger du i begrepet)
  - Dersom tvangsmidler benyttes, hvordan håndteres dette
  - Hvordan prioriteres hva som skal samles inn for sikring?
  - Forundersøkelse:
    - Skjer det en prioritering av hva som skal speiles først?
    - Skjer det en prioritering av hvilke beslag som skal undersøkes først?
  - Hvilke utfordringer synes du ligger i denne fasen som kan påvirke kvalitet og effektivitet i etterforskningen (feil og usikkerhetsmomenter)
  - Hvordan tenker du man kan bringe størst mulig grad av kvalitet og effektivitet inn i denne fasen (dvs: Når og hvordan bør kompetansen til espor etterforsker trekkes inn i etterforskningen etter ditt syn)

- I analysefasen (Denne fasen starter etter at alt er pakket ut og klargjort for analyse, enten av etterforsker eller dataetterforsker. Fasen varer helt til rapportering)
  - Beskrive hvordan analysefasen gjennomføres (alene, i samarbeid, hvem gjennomfører hva – dataetterforsker vs. etterforsker)
  - Hva danner grunnlaget for analysen (hypoteser – alternative forklaringer, bestilling, mandat mv.)
    - I hvilken grad benyttes hypoteser / alternative forklaringer i dette arbeidet? Fortell
    - Hvilken rolle spiller straffebud (subjektive og objektive vilkår)

  - Hvordan bestemmes søkeord (hvem – når)
  - Hvilke andre undersøkelsesstrategier kan du velge? Hvordan bestemmes disse?
  - Hvis en person er mistenkt for noe – (eks å ha delt overgrepsbilder på nett) og du skal undersøke databeslaget. Hva leter du etter?
    - Jobber for å bekrefte eller avkrefte hypotesene eller begge deler?
    - Leter du aktivt etter spor på at mistenkte er uskyldig? Gi eksempler
    - Hvordan ivaretas kravet til objektivitet?
    - Tiltak for å ivareta objektivitet?
  - Kunnskap om kriminalitetsfenomenet – hva er relevant, hvordan ivaretas dette?

        - Hvordan foregår kommunikasjon med etterforsker i denne fasen
        - Bevisvurdering- hvordan foretas den, og av hvem
        - Bias – påvirkningsfaktorer:
            - Hva kjenner du til omkring dette?
            - Hva tenker du øker farene for bias i det arbeidet du utfører?
            - Gjør du noe for å hindre at det skjer – og evt. hva?
        - Hvilke utfordringer synes du ligger i denne fasen som kan påvirke kvalitet og effektivitet i etterforskningen (feil og usikkerhetsmomenter)
        - I analysefasen – Hvordan tenker du man kan bringe størst mulig grad av kvalitet og effektivitet inn i denne fasen

    - I presentasjonsfasen (presentasjonsfasen omfatter rapportering og presentasjon av resultatet) Det være seg både tekniske og taktiske rapporter etter undersøkelser av beslag, det kan være presentasjon tiltenkt etterforskningsledelse, jurist eller i hovedforhandling)

        - Hvem skriver rapporter / Hvem skriver hvilke rapporter?
        - Hvordan bestemmes form og innhold på det som skal presenteres i retten?
        - Hvilke utfordringer synes du ligger i denne fasen som kan påvirke kvalitet og effektivitet i etterforskningen (feil og usikkerhetsmomenter)
        - Hvordan tenker du man kan bringe størst mulig grad av kvalitet og effektivitet inn i denne fasen

    - Om samarbeid generelt:
        - Finnes det noen prosedyre, retningslinjer eller lignende som styrer når og hvordan samarbeidet mellom espor etterforsker og generell etterforsker skal foregå?

Andre samarbeidsaktører i straffesakskjeden

- Samarbeid med dataetterforsker med politibakgrunn
- Samarbeid med jurist? – beskriv hvordan dette samarbeidet foregår (hvordan styrker det arbeidet ditt? – utfordringer med dette?)
- Samarbeid med etterforskningsleder? – beskriv hvordan dette samarbeidet foregår
- Samarbeid med kriminaltekniker? – beskriv hvordan dette samarbeidet foregår
- Andre?

Egen kunnskap

- Egen vurdering av kunnskap om etterforskningsprosessen (samle - collect, kontrollere - check, koble - connect, bygge - construkt, vurdere – consider, konsultere - consult)
- Egen vurdering av kunnskap om strafferett (subjektive og objektive vilkår)

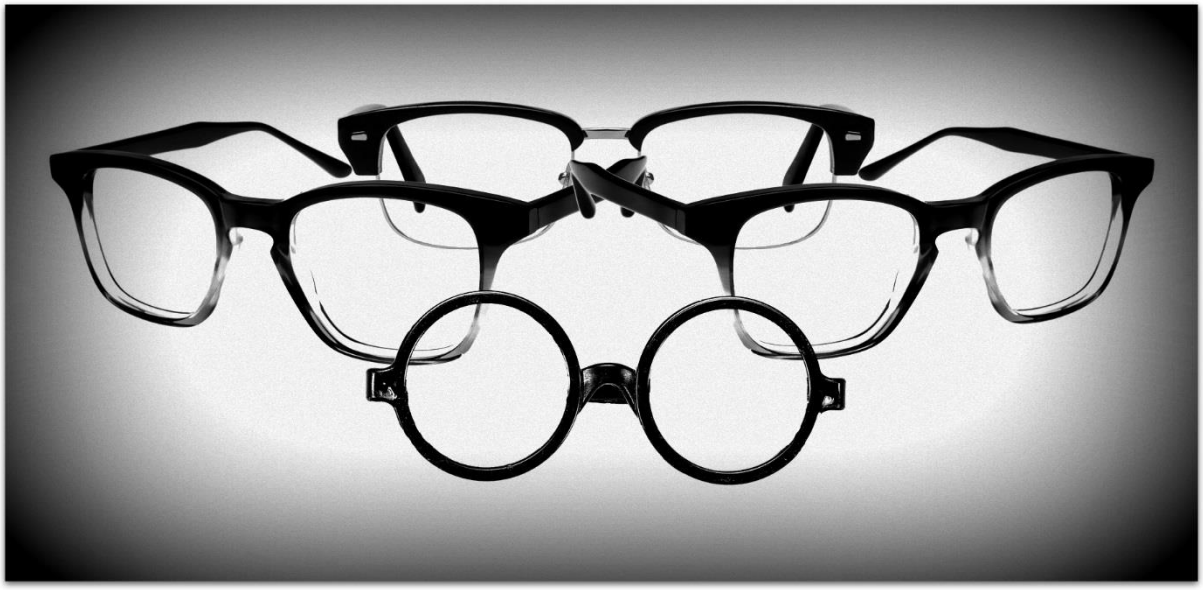
- Egen vurdering av kunnskap om straffeprosess (krav om objektivitet, forpliktelser, tvangsmidler)
- Egen vurdering av kunnskap om ulike kriminalitetsfenomener
- Egen vurdering av kunnskap og bevissthet om påvirkningsfaktorer/bias
    - Hva gjør du for å forhindre dette?

Organisatoriske utfordringer som kan påvirke samarbeidet

- Organisatorisk plassering
- Fysisk plassering – avstand
- Kommunikasjonskanaler
- Ressurser
- Rutiner, instrukser, prosedyrer for samarbeid i sak
- Annet?

Appendix 4

Non-technical errors and uncertainties of electronic evidence



By Nina Sunde

IMT 4883 Experience-based Specialization Project (5 ECTS)

Spring semester, 2016

Innhold

1. INTRODUCTION

The ultimate goal of any criminal investigation is to uncover and present the truth. Here, the concept of "truth" means a reconstruction of past events by the evidence uncovered in the criminal investigation. Since we cannot fully reconstruct the actual truth, it is of critical importance that the evidence is sufficient and reliable.

Electronic evidence is often considered reliable and unbiased, and serves the purpose of establishing the indisputable facts of a criminal case. The reason for this is mainly that they are generated by machines, and not processed through the perception of a witness. However, there are several uncertainties and errors associated with the data as evidence. This has been thoroughly covered from a technical point view (eg. Casey, 2002; Ekfeldt, 2016). The non-technical errors and uncertainties seem to seem to attract far less attention than the technical pitfalls. My focus will therefore be on non-technical uncertainties and errors concerning the electronic evidence during the digital forensics process (DFP).

1.1 Research question

The question I would like to investigate in this report is:

> Do the non-technical errors and uncertainties of electronic evidence handling pose a threat towards not uncovering the whole truth in a criminal case?

To be able to conclude on this question I will try to identify non-technical errors and uncertainties that might occur in a criminal investigation when handling electronic evidence. I will discuss the possible implications from these errors and uncertainties, and suggest some countermeasures.

1.2 Methodology

This report is the result of an analysis based on a combination of the DFP and the 6c's of investigation. The DFP and the 6c's of investigation in conjunction will form the analytical framework, which is used to break down the research question into manageable sub questions.

The DFP is an established process when handling electronic evidence, both within and outside a police investigation (Casey, 2009; ACPO, 2012). There have been several versions of the DFP (Casey,

2011). The DFP version described by Flaglien (2015) is chosen as the basis for the discussion in this report.

The reason for the choice of DFP as part of the framework is that it supports a sound and structured investigation of electronic evidence, by handling them in compliance with several important principles, like evidence integrity, repeatability and chain of custody. This corresponds well with the process of handling electronic evidence in a criminal case in the Norwegian police.

In criminal investigation in general, the 6c's of investigation is a well-established model of describing the investigation process (Fahsing, 2013). The model is an important part of the fundament of the study "Videreutdanning i etterforskning", offered by Norwegian Police University College (NPUC). This is a study in investigation process and methodology, and it is aimed at criminal detectives (CD) in the Norwegian police (NPUC, 2015b).

The 6c's of investigation is chosen because it is research based, and contains a detailed description of the necessary steps to maintain sufficient quality and to prevent errors of justice. As already mentioned, it is also a fundamental part of the theory in the training of post-graduate CD's in Norway (NPUC, 2015b).

The analysis is based on hermeneutical methodology (Olsvik, 2013), and is an attempt to identify and concretize non-technical errors and uncertainties of a criminal investigation involving electronic evidence, and to suggest countermeasures to prevent them.

The goal is to concretize a hypothesis for my upcoming master thesis, where I wish to obtain qualitative data to investigate it further.

The DFP is described in more detail in chapter 2.1, and the 6c's of investigation in chapter 2.2. The phases prior to the analysis phase in DFP are excluded to limit the scope of the report. The focus will be on the analysis and presentation phase of the DFP. The non-technical errors and uncertainties when handling electronic evidence in a criminal case during these phases are discussed in the chapters 4.1.1 and 4.1.2. Bias as a possible cause of error is discussed in chapter 4.2. In chapter 4.3, some organizational challenges are identified, described and briefly discussed. In chapter 5, some countermeasures against errors and uncertainties when handling electronic evidence in the DFP are suggested, as well as countermeasures to prevent bias. Some possible actions to meet the organisational challenges are also described.

A researcher will always bring in his or her preliminary knowledge when addressing a research question. This might affect the research-related distance to the topic. My preliminary knowledge

regarding the topics discussed in this report is based both on long term experience and theoretical knowledge. I have sixteen years of experience from criminal investigations, hence six within the cybercrime branch. I have been teaching criminal investigation methodology as well as investigation of electronic evidence for four years at the NPUC (2012-present). I have also attended several studies involving criminal investigation methodology, management of investigation, and investigation of electronic evidence prior to my current master program at NTNU Gjøvik/NPUC. Undoubtedly, the experience and knowledge I have acquired strengthens my ability to perform the analysis. Moreover, the analytical framework I have established provides for a systematic approach, where each issue will be analysed according to its pros and cons. Uncertainties regarding the conclusion that can be drawn, will be highlighted. Thus, there should be little risk that any preconceptions I might have developed should obscure the analysis.

1.3 Terminology and background

United Nations Office on Drugs and Crime (UNDOC) did define *evidence* as well as *electronic evidence* in the report Comprehensive study on Cybercrime:

> Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence is all such material that exists in electronic, or digital form (2013, p. 157).

In this definition, evidence is related to the trial. However, in this report the term "evidence" will be used about collected items or information during the investigation, with the potential to be presented as evidence in court.

In this report, the discussion will be limited to digital forensics performed by internally employed digital forensic detectives (DFD) in the Norwegian police, and not investigation done by private companies.

Only open investigation of criminal cases is included in this report, and covert police methodology, like covert audio surveillance and interception of communication will not be included.

An important term in this report is *digital forensics*. According to UNDOC (2013, p. 159), digital forensics can be described as "the branch of forensic science concerned with the recovery and investigation of material found in digital and computer systems". When the term "digital forensics" is used in this report, it is only in relation to investigation of criminal cases by the police, within a police investigation. The DFP is described in further detail in chapter 2.1.

UNODC (2013) divides digital forensics in three categories, depending on the source of the potential evidence. *Computer forensics* focuses on collecting and analysing desktop computers and laptops fond in homes or in businesses. *Mobile device forensics* is collecting and analysing low-powered mobile devices. Two distinguishing features about mobile devices are the mobility – they are with their owner at all times, and their connectivity – they are connected at all times. *Network forensics* is described as collecting and analysing evidence from online services and cloud storage, and gathering information about network traffic.

For the purpose of the present analysis, it is not necessary to distinguish between the categories, and the term "digital forensics" will be used further in the report.

According to a report by the Norwegian National Police Directorate (POD), the investigation of electronic evidence in Norway is handled by police officers with technical training and skills, or by civil engineers employed within the police (POD, 2012). Regardless of background, they will handle many of the same tasks concerning the investigation of the evidence. Several of the civil engineers also get "limited police authority" (Norwegian: "begrenset politimyndighet"), and might then carry out cohesive measures during the investigation. A police detective, regardless of civil or police educational background, who has handling electronic evidence as his/her main working task will be named "digital forensics detective" (DFD) further in this report.

In extraordinary situations, there is a need for extraordinary tools, software or competence. Norwegian criminal investigation service has a specialized unit of engineers who can provide assistance in such cases (POD, 2012).

The formal responsibility for a criminal case lies with the prosecutor, whilst the responsibility for the progress and implementation of the investigative tasks lays with the criminal detective (CD) and his police superintendent. The CD normally has a bachelor degree from NPUC. The prosecutor, the CD and the DFD each have independent responsibility to act in compliance with legal requirements and limitations. They are also responsible for contributing to a satisfactory progress of the investigation, and an efficient use of resources when investigating a criminal case.

Investigation is described by Myhrer (2014, p. 14, my translation from Norwegian):

> Criminal investigation is a purpose-oriented process with the aim of collecting information in order to clarify whether there is basis for a criminal reaction against somebody for an act, which has been, committed. [1]

The collection and analyses of the electronic evidence is a part of the investigation steps, and must be carried out in accordance with the Norwegian Criminal Procedure Code (NCPC). This means that the DFD, regardless of educational background, is subject to the same requirements under the NCPC as the CD when handling tasks in the criminal case, with an individual responsibility to safeguard the procedural objectivity requirement stated in NCPC § 226 (Kjelby, 2015).

In the textbook "Kriminalteknikk" (Hamremoen, 2012), covering crime scene forensic investigation, electronic evidence is represented as one of several tasks within criminal forensics. The book aimed at bachelor students at NPUC, has a chapter dedicated to collection of electronic evidence.

I will limit my discussion to criminal investigations. Legally, the physical storage medium and the computer data are different objects. The collection of the data is considered to be a *search*, and *seizure* is done when relevant information is uncovered and documented (Sunde, 2015b). According to the DFP, seizure is done in the analysis phase. The entire DFP when conducted during a criminal investigation is in fact to effect coercive measures, and must be carried out in compliance with the NCPC.

Non- technical errors and uncertainties might alone, or in junction with other circumstances cause "errors of justice" (Norwegian: "justisfeil"). Errors of justice is described by Rachlew (2009, p. 4) to be "any deviation from the optimal outcomes of the criminal investigation" (my translation from Norwegian).[2]

2. THE JOURNEY FROM INFORMATION TO EVIDENCE

The DFP is a series of steps to handle electronic information in compliance with important principles with the purpose to present the information as evidence in court. Every step of DFP requires technical expertise. Several of the steps requires additional knowledge and skills in order to safeguard the potential value of the evidence, as well as making it understandable to the prosecutor,

[1] «Etterforskning er en formålsbestemt innsamling av informasjon for å avklare om det er grunnlag for å reagere strafferettslig mot noen for en utvist atferd» (Myhrer, 2014, p. 14).

[2] «ethvert avvik fra straffesakens optimale utfall» (Rachlew, 2009, p. 4)

other detectives with responsibilities in the criminal case, and other parties with legal interest in the case, like the defence lawyer.

In this chapter, I will describe the procedural steps of the DFP. I will also describe the 6 c's of investigation. The DFP and the 6c's of investigation will later represent a framework for my analysis of the potential non-technical errors and uncertainties when handling electronic evidence in a criminal case.

2.1. DFP

The phases of the DFP version I have chosen are identification, collection, examination, analysis and presentation (Flaglien, 2015).

The DFP supports a sound and structured investigation of electronic evidence, by handling the source of the electronic evidence as well as the electronic evidence itself (the data) in compliance with several important principles (Flaglien, 2015). By following these principles, it is possible to prevent evidence dynamics and introduction of error (Casey 2011). The principles are: Evidence integrity, chain of custody and repeatability.

Evidence dynamics is "any influence that changes, relocates obscures or obliterates evidence regardless of intent between the time evidence is transferred and the time the case is resolved" (Casey 2011, p. 27).

The principle of *Evidence integrity* has the aim of preserving the evidence in a state identical to the origin from identification to presentation (Casey 2011; Flaglien, 2015; Hamremoen 2012).

The principle of *Chain of custody* supports the former, and means that every contact with the evidence should be accounted for (Casey 2011; Flaglien 2015; Kruse & Heiser 2002).

The principle of *Repeatability* means that the analysis of the evidence should be documented in a manner that makes it possible to be repeated by another and with the same result (Casey 2011; Flaglien 2015; Hamremoen 2012).

The DFP phases will be described in more detail below.

The identification phase:

Digital devices and systems, which might contain electronic evidence, are identified (Flaglien, 2015). Identification is done based upon information in the criminal case, but also on the experience and knowledge of the DFD.

When the evidence has been identified, it must be preserved. This is done by isolating, securing and documenting the physical and electronic evidence.

The collection phase:

The electronic evidence is copied, if possible – bit –by –bit, using appropriate methods and techniques (Flaglien, 2015). This is done to ensure the integrity of the evidence. This also preserves deleted information, which might be crucial to a criminal investigation.

The examination phase:

Examination is described as "Preparation and extraction of the relevant information to retrieve potential digital evidence from the collected data while protecting its integrity" (Flaglien 2015 p. 53, referring to NFSTC 2009 and Carrier 2004). During this phase, the important task is to prepare the evidence for the analysis phase. The examination often requires restructuring and pre-processing of the raw material to make it "readable" for a DFD in the upcoming analysis (Flaglien, 2015).

The analysis phase:

Analysis is the "processing of information that addresses the objective of the investigation with the purpose of discovering the person(s) responsible of the incident or crime." (Flaglien, 2015 p. 59, referring to Yusoff 2011). In this phase, the information is open and available, ready to be analysed.

The presentation phase:

In the presentation phase, the findings from the analysis phase are presented for a party with legal interest in the case. This might be the CD, the prosecutor, the defence lawyer, the court etc. To maintain potential of the evidence to prove guilt or innocence, it is crucial that the findings are presented in an understandable manner.

2.2 The investigative cycle (6c's of investigation)

"The investigative cycle" refers to the investigation of criminal cases, and is divided into 5 steps. These steps are referred to as the 5c's of investigation (Dean, Gottschalk & Solli-Saether, 2008), and are: Collecting, checking, considering, connecting and constructing. The purpose of the investigation cycle is to transform information into evidence with an established reliability, and the procedural steps can be used handling any type of evidence in a criminal investigation.

Fahsing has argued for extending the investigative cycle with another procedural step – consulting. The rationale is that, to be challenged by-, or to get a second opinion from a colleague might prevent errors of justice caused by confirmation bias and tunnel vision (Riksadvokaten 2015, p. 497). This college might play the role as the "devil's advocate", which is a recommended countermeasure to prevent confirmation bias (Christianson & Montgomery, 2008). I will therefore include the step in my analysis, and refer to the process as the 6c's of investigation further in this report.

I consider the 6c's of investigation to be relevant for analysing the non-technical errors and uncertainties the steps of the DFP, and particularly relevant to the analysis phase, where most of the "detective work" is done.

The fundament of all the 6c's of investigation procedural steps are 5WH: what, when, where, who, why and how, also described as the investigative star (Tilstone, Hastrup & Hald, 2013).

The 6 c's are based upon abductive logic, which was first described by C.S. Pierce as an addition to inductive and deductive logic in science. Abduction is carried out by forming and testing hypotheses to find the best possible guess about what the end result of the experiment or research may be (Tilstone et al., 2013). Fahsing and Rachlew (2015) state that the methodology in a criminal investigation and the quality of information obtained through this, will normally not enable a stringent falsification of theories in (deductive) scientific sense. However, the hypotheses thinking will test the available evidence better than with pure inductive inference.

Abductive testing of the hypotheses is also referred to as "pragmatic proof testing" (Norwegian: "pragmatisk bevisprøving"), where the goal is to determine which of the hypotheses represent the best explanation of the event (Fahsing & Rachlew, 2015 p. 227, referring to Diesen, 1994).

I will now go through the 6c's of investigation and briefly describe the essence of each procedural steps.

Collect: Collect all available and relevant data.

Check: Consider if the data is accurate, reliable and relevant. Consider whether you have the competence to make this assessment, or if you need specialist support.

Connect: Refine and structure information. Break up in smaller information pieces, organize and visualize. Consider how the information can be understood, and how different pieces of information correlate, correspond or contradict with each other.

Construct: Identify all possible explanations/hypotheses of the available information according to the 5WH. The hypotheses must involve the worst case scenarios, but also the possibility of innocence.

Consider: Test all hypotheses by looking for information that prove or disprove the crime. Identify information gaps. Make a plan to fill the information gaps, and log all the decisions (Fahsing, 2013).

Consult: Always get a second opinion. The assessor should consider blind spots and whether bias has affected the investigation (Fahsing, 2015).

3. EVIDENTIAL REQUIREMENTS

As the analysis concerns criminal investigation in Norway, a brief description of the main evidential requirements in Norwegian law is necessary.

A person charged for a crime must be entitled to a *fair trial*. This means eg. that the charged person should be allowed contradiction, or in other words - to ask questions to witnesses during the trail (Kjelby, 2015).

The principle of *presumption of innocence* means that a suspect of a crime shall be considered not guilty until legally guilt is proved. This is stated in the Norwegian Constitution § 96, 2'nd paragraph.

The state, represented by the prosecutor, carries the *burden of proof* in the trail, and the person charged for a crime has the right to remain silent through the trail (Kjelby, 2015).

The parties are entitled to present the evidence they wish, as long as it is relevant to the merits of the case. Nevertheless, this is subject to a fundamental exception. The scale and scope of the presentation of evidence shall be reasonably proportionate to the importance of the case (Kjelby, 2015).

In order to be convicted of a crime, these general conditions for *criminal liability* must be fulfilled:

1. The objective conditions: The act must be rendered criminal according to law.

2. The subjective condition: The individual must have acted with intent. Negligence is sufficient only if the law explicitly says so.

3. The individual must be personally criminally capable, i.e., by being above the minimum age, and not be mentally incapacitated.

4. There must not be circumstances, which render an otherwise criminal act lawful, such as emergency or exigent circumstances (Sunde, 2015a).

Myhrer (2001, p.4) has described the purpose of criminal investigation to be "to obtain necessary information required to handle the criminal case during the prosecution stage, the adjudication stage and the stage of the execution of sentence" (my translation from Norwegian). [3]

The investigation must be carried out in an *objective* manner. If the criminal investigation can conclude that there has been a punishable offence, and the investigation has uncovered a suspect of the crime, the investigation must identify mitigating or aggravating circumstances. The mitigating circumstances are listed in the Norwegian Penal Code (NPC) § 77, and the aggravating circumstances in NPC §78.

Evidence is described by Kolflaath (2015) as any type of information that directly or indirectly illuminates one of the themes of proof, or illuminates the reliability of the information or the credibility of the source of information.

Importantly, evidence can have different evidential value, depending on various circumstances – for instance, the reliability of the information and the credibility of the source (Kolflaath, 2015).

A crime is legally proved, when it is proved *beyond any reasonable doubt*. In order to sentence an individual of a crime, the judge must be convinced about the question of guilt, and any reasonable doubt must be in advantage of the defendant (Aall, 2015). This presupposes that the criminal case is illuminated sufficiently, concerning both evidence against him or evidence to his favour.

[3] Etterforskningen har således til formål å innhente informasjon av betydning for behandlingen av straffesaken både på påtalestadiet, pådømmelsesstadiet og fullbyrdelsesstadiet.

4. NON-TECHNICAL ERRORS AND UNCERTAINTIES WHEN HANDLING ELECTRONIC EVIDENCE IN A CRIMINAL INVESTIGATION

The need for technical skills when handling electronic evidence is thoroughly discussed in several articles and books (eg. Casey, 2009; Franke, Hjelmås & Wolthusen, 2009). In chapter 4.1, I will describe some non-technical errors and uncertainties that might occur during investigation of electronic evidence, and suggest the skills and knowledge needed to prevent or avoid them from happening. As described in chapter 2.1, the DFP and the 6c's of investigation forms my analytical framework, and the focus will only be on the analysis and presentation phases.

For simplicity, the detective handling the electronic evidence will be referred to as "the DFD" in this chapter, and the detective in charge of conducting the general investigation of a criminal case will be referred to as the CD. In real life criminal investigations in Norway, there are large variations of the involvement from the CD in the procedural steps of the DFP.

Bias as a possible source of error will be described in chapter 4.2, and some organisational challenges in relation handling electronic evidence will be outlined in chapter 4.3.

4.1 NON-TECHNICAL KNOWLEDGE AND SKILLS WHEN HANDLING ELECTRONIC EVIDENCE IN THE DFP

4.1.1 Analysis

Up to the analysis phase, the digital device has been a carrier of potential evidence. During the analysis phase, the information is open, and can be understood, assessed and analysed by a human – and by this serve as evidence of who, what, when, why, where and how a crime was committed. The 6c's of investigation is particularly relevant to the analysis phase, because the phase involves the forming and testing of the hypotheses of the investigation. The DFD will look for evidence that supports or refutes the hypotheses, but also for information that might lead to new hypotheses in the case. The analysis might also uncover clues that lead to other sources of potential evidence.

The Norwegian supreme court has twice held that identification and extraction of evidence is considered “continued search” (Norwegian: “fortsatt ransaking”) (Sunde 2015b referring to Rt. 2011 p. 296 and p. 1188), which is a coercive measure. The rationale is that seizure requires an assessment of the relevance of the object in relation to the crime (NPUC § 203).The assessment can first be performed in the analysis phase. The electronic information is an object in itself, which can be seized separately from the storage medium. Pursuant to the assessment, information from the digital image is selected and exported/copied from the digital image. The selected information serves as evidence, and can be presented in court.

Forensic tools provide a variety of predefined keyword lists tailored to different crime types. These may be useful, but cannot replace a structured identification of indicators based upon the hypotheses in the specific case (Heuer & Pherson, 2014). Every case is unique, and will contain exclusive information that can be extracted and documented as evidence.

According to Eklund (2016) there is a risk of false negatives when conducting a search. A narrow range of search terms might cause a wrongful conclusion that certain material is not present in the source.

This highlights the need for knowledge about the specific case as well as the current crime phenomenon relevant to the investigation.

In order to search for relevant information that can serve as evidence, the DFD must have knowledge about the relevant paragraphs from the NPC covered by the hypotheses of the investigation. The DFD must be able to identify the subjective and objective conditions of the paragraph to perform relevant searches of information, as well as to understand the relevance of the uncovered information.

Since analysis of electronic evidence is a part of the investigation, this must be done in compliance with the NCPC. The DFD must document all relevant information, and if the investigation has identified a suspect – the DFD must seek to clarify both the evidence against him and the evidence in his favour. Even if the evidence indicates that a suspect has committed a crime, there might be circumstances that render an otherwise criminal act lawful. This can be emergency or exigent circumstances (Sunde, 2015a). In other words, whoever conducts the analysis; he is obliged to look

actively for evidence proving that the suspect is innocent or information indicating mitigating circumstances.

An example of search for mitigating circumstances is the following: In Easter 2014 a German citizen was accused of the murder of his wife Agnes. He admitted to have killed her, but claimed that she wanted to die, and that she had consented to him killing her. If this hypothesis could not be falsified - but only strengthened, this could lead to mitigating circumstances when sentencing. The DFD actively searched for information to support the "consent hypothesis", but was not able to find any information indicating this was the truth. This involved analysis of internet communication like Facebook activity, analysis of a sound file recorded on the same day she was killed, and also witness testimonies. The police found no evidence that supported this hypothesis. The district court concluded that the accused had planned and carried out the murder without Agnes' consent (TJARE-2014-129689).

The procedural steps collect, check, connect, construct, consider and consult from the 6c's of investigation will now be used when discussing the analysis phase of the DFP.

6c's - Check:

An important part of the analysis will often revolve around checking and testing information obtained from other digital sources, as well as non-digital sources, such as interviews and forensic crime scene investigations. These actions require updated knowledge about the ongoing investigation of the specific criminal case, and a close dialogue with the investigation team.

The DFD must assess whether the information is accurate, which means whether the information has a sufficient level of detail. The DFD must also check whether it is relevant to prove or refute the hypotheses of the case.

And finally, the DFD must consider the reliability of the information. To make this assessment the DFD must consider the source and context of the information, and whether it can be confirmed by external sources of information. A hypothetical example: During the investigation of a grooming case, the DFD finds a chat log on the suspects' machine, but the DFD is not able state whether the log has been altered. To ascertain the reliability of this potential evidence, the DFD can search for other digital devices carrying relevant information. There might be a log from the same chat on the victims' machine, or a copy of the log on the server providing the chat service.

6c's - Connect:

An important part of the analysis will be to contribute to establish the narrative of the case. The evidence gains meaning when it is presented within the context of a narrative (Kolflaath, 2015). Timestamps and location data are common examples of evidence forming the fundament of the narrative. These evidence types are often considered reliable, even though there are several errors and uncertainties in relation to them (Casey, 2002). The DFD must be aware of the risk that the reliability of these evidence types might be overrated by the decision makers during the during the investigation as well as in court, and provide sufficient research to be able to assess the reliability by testing, or by looking for traces of the same evidence in external sources.

However, there are other issues concerning time and connection of events that is important for the DFD to be aware of. Several paragraphs in the NPC are linked to repetitive actions (The NPC §§ 190, 261, 282 and 301), or actions that have occurred over a period of time (The NPC §§ 255 and 283). In cases of domestic violence, a common problem is to schedule the repeated violent incidents. The DFD will have an important task in order to confirm or refute the hypotheses about repetitive actions when analysing the electronic evidence, and possibly provide a more exact time for the claimed incidents. Knowledge about the relevant paragraphs and the conditions of these is crucial to be able to conduct a proper analysis in such cases.

6c's - Construct:

The DFD must contribute to the forming of new hypotheses during the investigation based upon the information he or she uncovers in the analysis phase. This should be done whenever new information is uncovered that changes the status of the hypotheses of the case. Some of the hypotheses might cover criminal activity, and the DFD must be able to identify relevant paragraphs from the NPC. To be able to do so – the DFD must understand the objective and subjective conditions of the paragraph.

6c's - Consider:

During this phase, the hypotheses are tested. The DFD conducting the analysis must have updated knowledge about which hypotheses that are relevant to the investigation, and which that are already refuted. If the communication between the DFD and the CD in charge of the case is too rare, there is a risk that the DFD is searching for information to test already refuted hypotheses. This is ineffective, and a waste of often limited resources in a criminal investigation.

Casey (2011) mentions verification methodology as a common error in digital investigations. The DFD must have sufficient skills in conducting hypotheses testing, and understand abductive, deductive and inductive logic, and the purpose of falsification (Tilstone et al., 2013).

6c's - Consult:

The DFD must be aware of the need to obtain a second opinion or seek to be challenged by others when it comes to choice of methodology and interpretation of findings.

Analysis of electronic evidence is a subjective interpretation of information. There are several pitfalls related to bias when working alone with an investigation task, which will be covered in more detail in 4.2.

In addition to the struggle to conduct the analysis in an unbiased manner, it is important to recognize the limitations of one's own competence. To be able to uncover and understand potential evidence, the DFD must be aware of his own strengths and weaknesses in the various areas of required knowledge, and to ask for assistance when needed.

Summary of the necessary non-technical knowledge and skills in the analysis phase:

To handle potential electronic evidence during the analysis phase in a manner that prevents errors of justice is a complex and diverse task. The DFD needs knowledge about the NCPC, with special attention to § 226 and the coercive measures in chapter 13-17. He also needs to have sufficient knowledge about the relevant crime phenomenon(s) of the particular case. To contribute to the forming of hypotheses, the DFD needs continuous updated information about hypotheses relevant to the specific case. To test the hypotheses the DFD needs knowledge about the 6c's of investigation, and hypotheses testing by falsification in particular. This also requires knowledge about the general conditions for criminal liability, as well as the relevant paragraphs of the NPC – and their specific objective and subjective conditions.

4.1.2 Presentation

The result of the DFP must be documented in reports. Those involved in the investigation will read the reports, and these are the prosecutor, other detectives with responsibilities in the case and other parties with legal interest in the case, e.g. the defence lawyer. It is important that they understand the findings and the evidential value they possess. This requires that the findings are described and documented in an understandable manner to a non-technician.

In court, evidence can be presented in different ways, depending on the type of evidence. Document evidence (eg. exported emails, pictures, text documents) is handed out to the parties and read/presented by the prosecutor. If necessary, the physical device that was the source of the evidence (eg. mobile phone, laptop) might be presented for visual inspection by the court.

Witnesses – including the DFDs, give their testimony orally. Physical evidence is presented in pictures or brought to the courtroom. The DFD is often asked to present the findings documented in the analysis report orally, and might be allowed to use a presentation to visualize the findings. To have value as evidence it is crucial that the court understands the testimony from the detective as well as the evidential value of the document evidence. If the DFD uses technical terminology, there is a risk that the content of the testimony is misunderstood or not understood at all.

The DFD needs presentation skills to ensure that the evidential value is properly accounted for during the investigation, as well as in court.

4.2 BIAS WHEN HANDLING ELECTRONIC EVIDENCE

Bias is “the impact of the subjective factors on our perceptions that lead to systematic errors in our judgments of the reality” (Christianson & Montgomery, 2008, p. 110, my translation from Swedish).

Bias represents a threat to the objectivity of the detective. It might lead to improper testing of hypotheses, and introduce errors of justice into the investigation (Ask, 2013).

In relation to the DFP, confirmation bias is very relevant to a criminal investigation. This is one of the most common biases, and appears in two different ways. When testing a hypothesis, a detective will have a tendency to look for information that corresponds with the hypothesis. And, when information is ambiguous and open to more than one interpretations – the detective tends to choose the interpretation that corresponds with the opinion with the hypotheses he or she believes in the most (Ask, 2013).

Bias might also cause tunnel vision, which means that the detective solely focuses on one hypothesis or one suspect, ignoring other possible hypotheses or perpetrators (Ask, 2013 referring to Findley & Scott, 2006).

The risk of confirmation bias is influenced by different situational factors, that often can be present during a criminal investigation: Time pressure, emotions like confidence, frustration, sorrow and anger, personal responsibility, concern about future consequences (Ask, 2013) and motivation, (Fahsing, 2015).

Bias is also covered in relation to DFP by Casey (2011), who stresses the importance of being unbiased and open minded, and the importance of falsification methodology to reduce the risks of error. He also warns about preconceived theories based on former experience. This might cause the DFD to overlook or misinterpret the information, and lead to unfounded conclusions.

If the DFD is working in close cooperation with the rest of the investigation team, there is a risk of group thinking. This is "the reluctance to think critically and challenge the theory that dominates within the group" (Fahsing 2015, p. 15). To avoid group thinking from occurring, it is important to be aware of the risk of this condition occurring, but also to initiate countermeasures to prevent it.

4.3 ORGANIZATIONAL CHALLENGES IN RELATION TO HANDLING ELECTRONIC EVIDENCE

There is no established or mandatory way of organizing the work with electronic evidence in the Norwegian police. In 2013 this was looked into by a working group established by the Attorney General and POD, and the result was presented in the report "Politiet i det digitale samfunnet". The working group found that this work was organized in a variety of ways in the different police districts (POD, 2013).

There is no defined level of knowledge and skills required to conduct the investigation of electronic evidence in a criminal investigation in Norway. POD (2010, chapter 3.3) has stated that collecting electronic evidence requires "distinguished competence" and must not be carried out by personnel without "adequate training, technical equipment and software" (my translations from Norwegian). [4]

The aforementioned working group surveyed who was handling electronic evidence in the police. They found that the DFD in the Norwegian police districts was either an engineer with no police education, or a police officer with education or/and competence acquired through experience. NCIS has a specialized unit with engineers who provide assistance to the local DFD's when extraordinary competence, software or special tools are needed.

In relation to the DFP, the identification and collection of the physical device containing potential electronic evidence was often done by a regular CD. The assistance of a DFD depended on the planning of the operation and whether the operation was carried out during regular office hours.

[4] «Sikring av e-spor krever spesiell kompetanse og må ikke gjennomføres av personell uten adekvat opplæring, teknisk utstyr og programvare.»

Often the DFD performed all the steps in the DFP from collection to presentation, without a clear mandate about the aim of the analysis. This was not considered efficient compared to when the CD defined a specific task or purpose with the analysis (POD, 2013).

On the other hand – a too precise or limited mandate might increase the risk of bias, and will pose a threat to the objectivity of the DFD analysing the electronic evidence. If the DFD received a mandate that, for instance, described the aim to be to find all evidence that could confirm that a suspect was sharing stolen credit card information, there is a risk that the DFD would not search for the opposite, or maybe overlook signs of the opposite if they occurred.

The working group also found that the analysis sometimes was carried out in cooperation by the CD and the DFD, with involvement by the prosecutor. This way of handling the analysis was reported to be less time consuming, and provided "good evidence" (my translation from Norwegian) to the case. It was also pointed out that this way of organizing the work increased the competence of all of those involved (POD, 2013).

Myhrer (2014) promotes close cooperation between the detectives and the prosecutor, and states that this is necessary for a successful investigation of a criminal case.

In a criminal investigation, it is often necessary to consider "destructive" collection of evidence, which means to sacrifice a potential evidence to obtain another evidence. In a forensic crime scene investigation, this might be that the detective chooses one of the blood drops at the scene to test whether it is blood, but cannot use the same drop for DNA analysis afterwards, because of the pollution of chemicals used for the testing. This way of thinking must also be a part of the decision making when collecting electronic evidence.

To make a decision about destructive collection the DFD needs a broad spectrum of knowledge – both on the technical side and about the particular crime phenomenon, as well as the particular case. There might be a great risk that a single person in the investigation does not have all the knowledge needed to make a good decision in a situation like this. Close cooperation between the DFD, CD and the prosecutor will probably be a step in the right direction.

Standard procedures are often a safety net to prevent errors and mistakes in an investigation. This is also the situation in investigation of electronic evidence. Integrity and repeatability are important principles that should only be departed from under certain given circumstances. In the early days of digital forensics it was easier to act in compliance with these principles and still be in possession of important and reliable evidence as the result. Today, the situation is quite different. The extended use of encryption, the decentralized and fragmented storing of data and the complex technology

often results in none or unavailable evidence if the digital device is collected according to best practise.

To obtain evidence through live forensics might be the only option – but this methodology is contrary to the principles mentioned above. In some jurisdictions the evidence obtained through live forensics might even be denied to be presented before court. In the Norwegian court, the situation is different. The main rule is that the parties are allowed to present the evidence of their choice, as long as the court considers it relevant. Evidence collected through live forensics might therefore be presented. The value of the evidence might be considered lesser, but there is a low risk of denial of presentation in court.

5. DISCUSSION – The non-technical errors and uncertainties of the DFP, and suggested countermeasures

5.1 The DFP and the need for non-technical knowledge and skills

Based on chapter 4, the necessary non-technical competence or skills to handle electronic evidence in a criminal case to ensure quality and efficiency can be summarized to:

- Criminal law and evidential requirements
- Criminal procedure law – principles, obligations and coercive measures
- Knowledge about relevant crime phenomenon's
- The 6c's of investigation
- Abductive, deductive and inductive logic, and hypotheses testing
- Bias (Forensic psychology)
- Presentation skills

The big question is – do you find a DFD with a sufficient level of this spectrum of knowledge and skills in the Norwegian police today? The answer is probably only by exception, and most likely no.

A DFD with police background will probably have sufficient skills in understanding the NPC and the NCPC. The study "Videreutdanning i etterforskning" (NPUC 2015b) would provide an update on law and general investigation methodology, and provide skills in planning and conducting an

investigation according to the 6c's of investigation. This is an optional post graduate education as of today. However, a DFD with a police background would need broad competence in digital forensics.

Engineers with no police education have a greater need for criminal investigation related competence to handle evidence properly during an investigation. They often lack the basic knowledge about the NPC and the NCPC. They would also need in depth knowledge and skills in planning and conducting an investigation according to the 6c's of investigation.

Basic knowledge and skills regarding the crime phenomenon is also crucial for both police and engineers. This can be obtained by consulting more experienced DFD's or CD's. There are several courses covering different crime phenomenon at NPUC (investigation of sexual assault of children, investigation of homicide, investigation of organized crime, etc.) but they all aim at CD's. Close cooperation with the experienced and skilled detective on the phenomenon might compensate for the knowledge gap, and might also be fruitful in building your own competence.

To make a judge understand and assess complex electronic evidence, presentation skills are essential. There are no specific courses at the NPUC covering this topic today, but it is one of several topics within the course Nordic Computer Forensic Investigator 2 (NPUC, 2013). However, learning from good practice is a way of building these skills. To be present in court when an experienced DFD presents the result of his or her analysis might be of great value to the unexperienced DFD.

To handle potential electronic evidence in an optimal manner to maintain and visualize the true value of the evidence is a complex task. Each non-technical area of knowledge and skills defined in the list above require in depth or maybe expert knowledge. The police is already equipped with personnel who possesses one or more of these skills, but the combination of all the mentioned skills and knowledge is rare. To aim at educating and training every DFD to possess these levels of knowledge and skills might be considered unachievable, without even mentioning maintaining the necessary level of expertise. It is important to remember that these are all non-technical skills, and come in addition to the technical knowledge and skills – that of course needs to be developed and maintained.

One could argue that checklists could compensate for the knowledge gap. This could be the solution if every case had similar characteristics and artefacts. The reality is that every case is unique concerning its circumstances and artefacts, and requires individual exhibits. A checklist would only cover for the similarities, and not the entire knowledge gap.

Close cooperation between the CD, the DFD and the prosecutor is probably one part of the solution to cover the knowledge gaps. In complex cases, extraordinary expertise might also be required from within or outside the police.

A suggested countermeasure to avoid errors and loss caused by non-technical errors and uncertainties when investigating a criminal case would therefore be a basic level of knowledge on all the mentioned areas, for DFD's, the CD's and the prosecutors. This would facilitate a smoother and more efficient cooperation that would compensate for some of the knowledge gaps. On the other hand – the CD and the prosecutor needs to have a basic knowledge about technology and the possibilities regarding electronic evidence to contribute in a sufficient manner in this cooperation. The DFD and the CD must be capable of identifying his or her limitations – and be able to ask for advice or assistance when necessary.

5.2 Countermeasures regarding bias:

To prevent bias, it is important that the DFD have sufficient knowledge about how and when bias might occur, and how it might affect his or her decisions. However, awareness is not an adequate countermeasure to prevent bias to occur. Several countermeasures should be initiated to avoid errors of justice caused by bias (Ask & Granhag, 2008).

A countermeasure could be to ask a colleague to be the critical counterpart in the investigation team during the investigation, and challenge the opinions and decisions made by all those involved in the investigation (Christianson & Montgomery, 2008). As aforementioned, this is also included as a procedural step (consult) in the 6c's of investigation.

Another countermeasure is to maintain focus on the hypotheses testing through the entire investigation, by cooperation through a plan where the hypotheses, paragraphs and investigation steps are documented (Ask & Granhag, 2008). This measure – a plan for the investigation - is also described in the circular about police interviews (The Norwegian Attorney General, 2016b, p.3). It is crucial for the quality of the investigation that the entire investigation team have access to this plan. This way they can continuously update themselves on the hypotheses that are relevant to the investigation, and the status on the testing of these.

5.3 Countermeasures regarding organisational challenges

5.3.1 Mandates

An investigation team will often plan and conduct the investigation in relation to a written plan for the investigation. If the DFD is not considered a part of this team, he or she might receive a mandate where the purpose or task concerning the investigation of the electronic evidence is described.

If mandates are used, there is a risk that these are defined to rigorously or narrow (Casey, 2011), and this could cause tunnel vision and errors of justice. If the mandate is not reproduced in the report, the reader might get the impression that the investigations have been conducted in an objective manner in accordance with the requirements of the NCPC, and possible errors of justice might be hard to uncover. There is also a risk that the mandate is to broad (POD, 2012). This might lead to the task being unnecessary time consuming, and whether the analysis is covering the relevant hypotheses would be based on coincidences, more than structured work. The details of a mandate should therefore always be documented in the report from the analysis.

The detectives should exercise caution when communicating through mandates. This might increase the risk of confirmation bias and tunnel vision. A preferred alternative could be a continuously updated plan of the investigation available for all the involved detectives as described in chapter 5.2. If the plan would provide information on the status of the hypotheses, it could also save time and effort for the detectives by avoiding unnecessary investigation of already falsified hypotheses.

The investigation would probably benefit from including the DFD in the investigation team of the particular case. To conduct analysis alone or together with CD, the DFD must have access to the continuously updated plan documenting the relevant hypotheses to test. The DFD might need to consult the prosecutor to gain knowledge about the relevant paragraphs in the NPC in the specific case, and he might also need information about the crime phenomenon. A close cooperation between the CD, DFD and the prosecutor is therefore recommended as a countermeasure against non-technical loss and uncertainties regarding the electronic evidence.

5.3.2 Principles and standard procedures

As outlined in chapter 4.3 deficient update and development of standard procedures might stand in the way of efficient collection of evidence. Maintaining evidence integrity is an important principle in all parts of a criminal investigation – as well as in investigation involving electronic evidence. However, the principle of integrity might stand in the way for the necessary availability of the information.

To solve a case, it might be necessary to collect evidence in a manner that conflicts with the principle of integrity in order to obtain any evidence at all. The evidence might still be presented in court, but the evidential value might have been reduced because of lower reliability.

The Norwegian Attorney General (Riksadvokaten, 2016a) has stated that high quality is a main goal in criminal investigation. When considering the issues (eg. size, complexity, availability) of the electronic evidence of today, a standard procedure with a strong focus on integrity can pose a risk against reaching the goal of quality in the investigation of a crime. It might be necessary to move back from standard procedures when collecting electronic evidence at a crime scene – and rather emphasize close cooperation between the parties with the sufficient competence to make the best possible decision about the approach of collection of the electronic evidence.

5.3.3 Organizing the work

Based on chapter 5.1, there are reasons to believe that it might be impossible for a single CD or a DFD to gain and maintain all the necessary knowledge and skills to handle electronic evidence in an optimal manner during a criminal investigation.

Today, the CD and the DFD belong to different organisational groups, and the level of cooperation varies a lot. From the discussion above, I have concluded several times that close cooperation between the CD, DFD and the prosecutor would be a relevant measure. There is a need to look into this issue, and try to identify the best possible way to organize the investigation teams to ensure the presence of the sufficient knowledge level within the team from the start until the end of the investigation.

6. CONCLUSION

My aim was to answer the question: Do the non-technical errors and uncertainties of electronic evidence handling pose a risk for not uncovering the whole truth in a criminal case?

In this report, I have pointed out several non-technical risks in relation to the DFP when handling evidence in a criminal investigation. I have discussed the kind of knowledge and skills which are needed to obtain the true potential of electronic evidence, and described some pitfalls regarding bias. I have considered some organisational challenges in relation to the DFP in criminal investigations.

I have pointed out pitfalls, possible errors and challenges. What possible consequences might be the result of these?

Lack of sufficient knowledge, adverse decisions caused by bias, and unsolved organizational challenges might lead an unnecessary time consuming investigation. However, more importantly it might lead to a non-acceptable level of quality of the evidence. Evidence could be destroyed, and evidential value might be reduced. Evidence could be misinterpreted, and evidence might never be found. In other words – the result might be minor or major errors of justice.

I have identified several possible non-technical errors and uncertainties that pose a risk to the quality and efficiency of a criminal investigation involving electronic evidence. Nevertheless, the risk goes beyond this. Errors and uncertainties in relation to evidence of a criminal case pose a risk that the defendant does not receive a fail trail.

Errors of justice during a criminal investigation might in a worst case scenario cause an innocent person to be convicted for a crime he never committed. If so, the guilty person goes free – and will not be convicted for the crime he committed.

7. LITTERATURE

Aall, Jørgen. (2015). Uskyldspresumsjonen og beviskravet i straffesaker. Aarli, R., Hedlund, M. & Jebens, S. E. (Red.) *Bevis i straffesaker*. Oslo: Gyldendal.

ACPO (2012). *Good Practice Guide for Digital Evidence*. Downloaded 15.04.16 from: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Ask, K. (2013). Bias: Fejl og faldgruber i efterforskning. I C. Hald & K. Vrist Rønn, (Red.), *Om at oppdage: Metodiske refleksjoner over politiets undersøkelsespraksis*. Fredriksberg: Samfundslitteratur.

Ask, K. & Granhag, P. A. (2008). Psykologiska perspektiv på bevisvärdering. I: P. A. Granhag & S. Å. Christianson (Red.), *Handbok i rättspsykologi*. Stockholm: Liber.

Casey, E. (2011). *Digital Evidence and Computer Crime: forensic science, computers and the Internet*. USA: Elsevier.

Casey, E. (2002). Error, uncertainty, and loss in digital evidence. *International Journal of Digital Evidence*, *1*(2), 1-45.

Christianson, S. Å. & Montgomery, H. (2008). Kognition I ett rättspsykologiskt perspektiv. Granhag, P. & Christiansson, S.Å. (Red.), *Handbok I rättspsykologi.* Malmø: Liber AB.

Dean, G., Fahsing, I. A., Gottschalk, P., & Solli-Saether, H. (2008) Investigative thinking and creativity: empirical study of police detectives in Norway. *International Journal of Innovation and Learning*, 5(2), pp. 170-185.

Ekfeldt, J. (2016). *Om informationstekniskt bevis*. Juridiska institutionen, Stockholms universitet, Stockholm.

Fahsing, I.A. (2015). *The Making of an Expert Detective. Thinking and Deciding in Criminal Investigations*. Gothenburg: Department of Psychology.

Fahsing, I. A. (2013). Tænkestile: effektivitet, dyder, krydspres i efterforskninger. I C. Hald & K. Vrist Rønn, (Red.), *Om at oppdage: Metodiske refleksjoner over politiets undersøkelsespraksis*. Fredriksberg: Samfundslitteratur.

Fahsing, I. A. & Rachlew, A. (2015). Politiavhøret. I: Aarli, R., Hedlund, M. & Jebens, S.E. (Red.) *Bevis i straffesaker*. Oslo: Gyldendal.

Farmer, D. & Venema, W. (2005). *Forensic discovery.* Upper Saddle River: Addison-Wesley.

Flaglien, A. O. (2015). The digital forensics process. In: *Digital Forensics*. Årnes, A. (ed.) Gjøvik: Gjøvik University College (Preprint)

Franke, K., Hjelmås, E., & Wolthusen, S. D. (2009). Advancing Digital Forensics. In *Information Assurance and Security Education and Training* (pp. 288-295). Springer Berlin Heidelberg.

Hamremoen, E. (2012). *Kriminalteknikk.* Oslo: Gyldendal Norsk forlag AS.

Heuer, R. J. & Pherson, Y. (2014). *Structured analytic techniques for intelligence analysis* (2nd ed.). Thousand Oaks: SAGE CQ press.

Kjelby, G.J. (2015). Bevisrettens grunnprinsipper og hovedregler I straffesaker. In: Aarli, R., Hedlund, M. & Jebens, S. E. (Red.) *Bevis i straffesaker*. Oslo: Gyldendal

Kolflaath, E. (2015). En metode for bevisbedømmelsen I straffesaker. In: Aarli, R., Hedlund, M. & Jebens, S. E. (Red.) *Bevis i straffesaker*. Oslo: Gyldendal.

Kruse, W.G & Heiser, J.G. (2002). *Computer Forensics. Incident Response Essentials*. Indianapolis: Pearson Education.

Myhrer, T. (2014). *Kvalitet i etterforskningen. Særlig om påtaleansvarliges rolle og betydning. Delrapport i «Etterforskningsprosjektet»*. Phs Forsking 2015:1. Downloaded 23.04.16 from https://brage.bibsys.no/xmlui/bitstream/handle/11250/282259/kvalitet_i_etterforsknin gen.pdf?sequence=1&isAllowed=y

Myhrer, T. (2001). *Etterforskningsbegrepet: Avgrensning, vilkår, roller og ansvar.* Tidsskrift for strafferett, 1(1), 6-[30].

Norwegian Criminal Procedure Code (1981). Lov av 22. Mai 1981 om rettergangsmåten i straffesaker (Straffeprosessloven).

Norwegian National Police Directorate (2010). RPOD- 2010-7. *Behandling av* beslag *i straffesaker*. Downloaded 23.04.16 from: http://fido.nrk.no/0f9e97f92048ab8ee84d28411b7d5399bf32998537b841582648e891b1818 aac/Rundskriv%202010-007.pdf

Norwegain National Police Directorate (2012). *Politiet i det digitale samfunnet. En arbeidsgrupperapport om: elektroniske spor, IKT-kriminalitet og politiarbeid på Internett.* Oslo: Politidirektoratet.

Norwegian Penal Code (2005). Lov av 20. Mai 2005 om straff (Straffeloven).

Norwegian Police University College (2015a). *Fagplan Bachelor Politiutdanning 2015-2018.* Downloaded 23.04.16 from: http://www.phs.no/Documents/5_Studenter/Fagplaner/Fagplan%20bachelor%202015-2018.pdf

Norwegian Police University College (2015b). *Videreutdanning i etterforskning*. Downloaded 24.04.16 from: http://www.phs.no/Documents/2_Studietilbud/3_EVU/Godkjent%20studieplan%20VEF%20i%20hogskolestyret%201609%202015%20med%20endringer%202509%202015.pdf?epslanguage=no

Norwegian Police University College (2013). *Nordic Computer Forensic Investigators 2.* Downloaded 24.04.16 from: http://www.phs.no/Documents/2_Studietilbud/3_EVU/Studieplan%20NCFI_Module_2_revidert%202706%202013%20med%20pensumendr%201509%202014-1.pdf?epslanguage=no

Rachlew, A. (2009). *Justisfeil ved politiets etterforskning: noen eksempler og forskningsbaserte mottiltak.* Doktorgradsavhandling ved Det Juridiske fakultet, Universitetet i Oslo. Oslo: Unipub. Downloaded 26.05.2016 from: https://www.duo.uio.no/bitstream/handle/10852/22587/Rachlew_avhandling.pdf?sequence=2

Riksadvokaten (2016a). *Mål og prioriteringsrundskriv nr. 1/2016*. Oslo: Riksadvokaten.

Riksadvokaten (2016b). *Politiavhør* (2/2016). Oslo: Riksadvokaten.

Riksadvokaten (2015). *Norsk politi og påtalemyndighets behandling av straffesakene mot Sture Bergwall – Hva kan vi lære? Rapport fra arbeidsgruppe*. (Riksadvokatens publikasjoner nr. 3/2015). Oslo: Riksadvokaten. Downloaded 28.05.16 from: http://www.riksadvokaten.no/filestore/Dokumenter/2015/Riksadvokatenspublikasjoner3_2015.pdf

Sunde, I. M. (2015a). Cybercrime Law. In: *Digital Forensics*. Årnes, A. (ed.) Gjøvik: Gjøvik University College (Preprint)

Sunde, I.M. (2015b). Databevis. Aarli, R., Hedlund, M. & Jebens, S. E. (Red.) *Bevis i straffesaker*. Oslo: Gyldendal

Tilstone, W., Hastrup, M.L., Hald, C. (2013). *Fischer's Techniques of Crime Scene Investigation*. USA: CRC Press

United Nations Office on Drugs and Crime (2013). *Comprehensive Study on Cybercrime*. New York: United Nations.

Årnes, A. (2015). Introduction. In: *Digital Forensics*. Årnes, A. (ed.) Gjøvik: Gjøvik University College (Preprint)

NTNU

Norwegian University of
Science and Technology