Master's thesis

2019

Odin Heitmann

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

Master's thesis

Odin Heitmann

Digital investigation: The malnourished child in the Norwegian police family?

June 2019

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of
Science and Technology

NTNU

Norwegian University of
Science and Technology

Digital investigation: The malnourished child in the Norwegian police family?

Information Security: Digital Forensics and Cybercrime Investigation (MISEB)
Submission date: June 2019
Supervisor: Katrin Franke

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

Acknowledgments

Former NASCAR racing driver Dale Earnhardt once said «*finishing races is important, but racing is more important».* The completion of this thesis marks the finish of three years as a part-time student combined with a full-time job as a police officer. During these three years I have acquired knowledge that I can take advantage of both in a private and a professional context for the rest of my life. It has at times been exhausting, but it has definitely been worth it. Even though a master degree is comprised of a large degree of self-effort, it is decisive to get support from others. I would therefore like to acknowledge and thank the following:

The Norwegian University of Science and Technology and the Norwegian Police University College for providing a master's program in Information Security: Digital Forensics and Cybercrime Investigation. A cooperative program like this is essential for being able to face tomorrows challenges today.

Professor Katrin Franke, my supervisor from NTNU. Your commitment and knowledge have been inspiring and helpful. The digital forensics community are lucky to have you aboard!

The members of our little colloquium; Tor Stian Borhaug and Tom Erik Erlandsen for both professional and moral support in somewhat challenging academic times. Thanks to Stig Andersen for the support, every colloquium of young padawans needs an experienced academician who has done his share of musings.

Harald Engøy, former head of the joint investigation section in Romerike police district. You saw the importance of employees attending higher education within digital forensics, and almost immediately said yes when I applied for the master's program in 2016.

Eivind, my first partner in anti-crime. Your curiosity and determination as an investigator lead to the discovery, and ultimately solving, of a comprehensive criminal case which truly made a difference, especially for those not able to defend themselves. I am grateful that I have had the honour of working with you — I would not be where I am now if not for you.

Aron, thank you for proofreading and for providing valuable inputs related to layout and structure. I think we can agree that sometimes a hint of CDO might be beneficial.

Janne, the cornerstone of my life. You are the most tolerant and patient person I know. Words can not describe how much I appreciate how you have accepted me spending countless hours in front of the computer instead of spending time with you the last three years. I promise I will replace studies with regular trips to the gym from now on.

My beloved son, Sverre. Born during the first year of the master program, you have been a blissful distraction from day one. It was *never* difficult to give less priority to studies when you were around. Thank you for your frequent interruptions, they were most welcome!

My dear parents, for facilitating access to computers for my brother and me when we grew up. Thanks to you we had a computer at home before computers became common property. This foresight enabled us to become proficient in the use of computers from an early age, a trait we surely have benefited from.

All my fantastic colleagues in the Norwegian Police working hard every day, often with limited resources, to make a difference in the society and to make Norway a safer place to live in.

Abstract

We live in a digitised world where technology surrounds us in every aspect of our daily life. Today, the presence of digital evidence is a natural part of most criminal cases, and this means employees in law enforcement agencies must have a certain level of digital competence and digital understanding.

This thesis address how capable the Norwegian Police are to handle the initial phase of a digital investigation. The main goal of the thesis is to present the current state of digital investigation in Norway, and by this aid decision makers in the Norwegian police to initiate relevant actions to further improve the digital competency if needed.

To answer the research problem there has been conducted literature review of official reports. A survey that measured police officers *perceived* competency when faced with aspects from digital investigation has been distributed to over 2200 police officers in three police districts in Norway. There has also been created a practical test which can serve as a proof of concept for a certification for police officers, both executive and managerial, who will touch digital investigation in their line of work.

The findings from the survey gives an indication of deficiencies in the competence among police officers when they are faced with digital evidence. These deficiencies are found in the initial phase of a digital investigation. The findings indicates deficiencies in the examination phase of digital evidence, and there are also indications that a verification system for digital evidence is missing before the evidence is presented in court. It is also found that there are no requirements for police officers that would conduct digital investigation. In regards to digital investigation training in the police districts, the findings indicate there are shortcomings in how the training is conducted.

Based on the findings in the thesis, several recommendations can be proposed. The practical test for certification should be further developed and refined, and a national implementation of the practical test can be included in the compulsory annual training for all police officers. Managers and patrol officers should also undergo the same training so that they have the same basic digital competence as other employees. The framework for competency requirements is recommended to be further developed and implemented in the national role requirements for police investigators. Further research in the digital competency among police officers, with deeper analysis and by surveying police officers from each police district, is also recommended to form a solid basis for decision makers.

The actual content of curriculum that should be *mandatory* for police officers is not included in this thesis, but this topic should be researched further. It is recommended that the Norwegian Police University College (PHS) take lead on this research, as they are familiar with developing curriculum and training programs. However, it is also recommended that PHS include employees from Computer Crime Units when developing the curriculum and training programs. These employees know first-hand what digital challenges police officers face every day. By including employees from the frontline a practical approach, with a theoretical foundation, can be utilised to increase the digital competence.

Keywords

Police, digital investigation, criminal investigation, digital evidence, digital competence, investigative competence, competency requirements, Bloom’s taxonomy of learning, digital forensics.

Sammendrag

Vi lever i en digitalisert verden der teknologi er til stede i alle deler av våre daglige liv. I dag er digitale spor en naturlig del av de fleste straffesaker. Dette medfører at ansatte i politiet må ha et visst nivå med digital kompetanse og digital forståelse.

Denne studien omhandler hvor godt norsk politi håndterer den innledende fasen i en digital etterforskning. Hovedmålet med oppgaven er å presentere den nåværende tilstanden for digital etterforskning i Norge, og med dette bidra til at beslutningstakere i politiet, om nødvendig, kan iverksette relevante tiltak for å forbedre den digital kompetansen.

For å svare på forskningsspørsmålet er offisielle rapporter blitt gjennomgått. En undersøkelse som måler politiansattes *opplevde* kompetanse når de står overfor digital etterforskning har blitt distribuert til rundt 2200 politiansatte i tre politidistrikt i Norge. Det er også utviklet en praktisk test som kan brukes som et utgangspunkt for en sertifisering av politiansatte som har en befatning med digital etterforskning. Sertifiseringen kan gjelde for både ansatte og ledere.

Resultatene fra studien gir en indikasjon på at det er mangler i kompetansen blant politiansatte når de står overfor digitale bevis. Disse manglene omhandler primært den innledende fasen av en digital etterforskning. Funnene indikerer mangler i gjennomgangsfasen av digitale bevis, og det er indikasjoner på at det mangler et system for verifisering av digitale bevis før bevisene blir presentert i rettsapparatet. Det er også funnet at det ikke er krav til politiansatte som jobber med digital etterforskning. Når det kommer til opplæring i digital etterforskning i politidistriktene, indikerer funnene at det er svakheter i hvordan selve opplæringen gjennomføres.

Basert på funnene i studien kan det foreslås flere anbefalinger. Den praktiske testen for sertifisering bør videreutvikles og forbedres, og en nasjonal implementering av den praktiske testen kan inngå i den obligatoriske årlige opplæringen for alle politiansatte. Ledere og operativt mannskap bør også gjennomgå samme opplæring, slik at de har samme grunnkompetanse som øvrige ansatte. Rammeverket for kompetansekrav anbefales videreutviklet og implementert i de nasjonale rollekravene til generalist og etterforsker. Videre anbefales det at det blir forsket ytterligere på den digitale kompetansen blant politiansatte, herunder at ansatte fra alle distrikt og særorgan blir kartlagt. Dette kan muliggjøre dypere analyser og et bedre datagrunnlag som igjen kan danne et solid beslutningsgrunnlag.

Det faktiske teoretiske innholdet i opplæringen som burde være obligatorisk for politiansatte, er ikke inkludert i denne oppgaven, men dette bør undersøkes videre. Det anbefales at Politihøgskolen tar ledelsen i denne forskningen, da de er kjent med å utvikle læreplaner og læringsopplegg. Imidlertid anbefales det at Politihøgskolen også inkluderer ansatte fra seksjon/ avsnitt for digitalt politiarbeid i distriktene når de utvikler læreplanene og læringsopplegg. Disse ansatte kjenner til de digitale utfordringene politiansatte står overfor hver dag. Ved å inkludere ansatte fra førstelinjen kan en praktisk tilnærming med et teoretisk grunnlag benyttes for å øke den digitale kompetansen.

Nøkkelord
Politi, digital etterforskning, etterforskning, elektroniske spor, digitale bevis, digital kompetanse, etterforskningskompetanse, kompetansekrav, Bloom’s taxonomy of learning, dataetterforskning.

"If you approach the ocean with a cup, you can only take away a cupful; if you approach it with a bucket you can take a bucketful."

Ramana Maharshi

Table of Content

1. Introduction

Technology surrounds us in almost every aspect of our daily life. We communicate using mobile phones and we use laptops to browse the Internet. Our fridge is connected to the Internet and lets us know before we run out of milk. Cars have built-in WiFi and lets us know if there is a traffic jam in our path. In 2017, according to Statistics Norway (SSB), 98% of the people living in Norway had access to Internet and 91% had their own smart phone.

The digital footprint is defined by TechTerms as data we leave behind every time we visit web sites or send messages online. This a potential gold mine for law enforcement agencies as it can either support or refute a hypothesis[1] in an ongoing investigation. Furthermore, each time you use the Internet there is a chance that you unintentionally leave information behind. This passive digital footprint can include your current IP address[2] and what software you use. Even a passive digital footprint can be what an investigator needs to identify a suspect, and it is therefore quite interesting and important.

There is an abundance of digital information available for law enforcement, but are the Norwegian Police ready and capable to utilise the possibilities that exist? To paraphrase the quote by Ramana Maharshi; do they approach a digital sea full of data with a small cup to gather information, or do they use a large bucket which has ample room for information?

1.1 Audience

The primarily audience for this study are the executive level in the Norwegian Police and politicians that can influence how the work towards improving digital investigative competence is handled in the future. Another important audience are the educators in digital investigation at the Norwegian Police University College and their collaborative partners, like the Norwegian University of Science and Technology (NTNU). Other educators can also be a relevant audience. Senior managers responsible for Computer Crime Units in the police districts and investigators with an interest in digital investigation can benefit from reading this thesis. Even though digital investigation can be a complex and technical advanced field, this thesis will aim to present the findings in a non-technical way with simplified explanations where needed.

1.2 Motivation

Computers have always fascinated me, and I grew up with easy access to computers. Even though computers was a huge part of my life growing up, I did not dream of working full time with computers - it was always a police officer I wanted to be. After graduating in 2013 I had a short career as an operative police officer before I started working with digital investigation in a comprehensive sexual abuse case. After working with that case for several months I started working at the Computer Crime Unit in Romerike police district as a computer forensics investigator, where I was for almost four years.

When I started working as a computer forensics investigator I had quite limited knowledge about digital forensics and digital investigation. The knowledge I had was gained through experienced-based learning while working the above mentioned criminal case. I had also completed the «*NCFI module 1*» that gave five credits, but I did not understand much of the

[1] An idea or explanation for something that is based on known facts but has not yet been proven

[2] Internet Protocol address, a numerical label assigned to each device connected to a computer network

content in that module when I took it. However, what I did understand was that I wanted to improve within the field of digital investigation, and I applied for the course «*NCFI module 2*» which I finished in 2015. The next year, when I met the requirements to start the master's program that PHS and NTNU had developed, I applied and started the master's program.

Today, after five years of almost continuous post graduate studies within digital forensics, not a single day goes by without realising that I know only a tiny fraction of a field that is enormously complex and varied. Based on my own experiences, both as a newly graduated police officer and later on as a specialised investigator faced with digital challenges, I have often wondered how my fellow colleagues cope with digital investigation and handling of digital evidence. This has inspired me to research the digital investigative competence of my colleagues, in order to enable them to be even better in their daily work. By using a scientific approach in a systematic study of digital investigative competence to establish facts, this thesis will hopefully yield tangible results that can assist relevant decisions makers in the Norwegian police to facilitate for increased digital competence for my colleagues.

1.3 Research problem

The initial research problem for this thesis was:

How capable are the Norwegian Police to handle challenges that might come with (new) technology when conducting an investigation?

While working on the survey, and the practical test, it became clear that the scope for the research problem was too broad and that the thesis would focus on the initial phase of a digital investigation. The revised research problem became:

How capable are the Norwegian Police to handle the initial phase[3] of a digital investigation?

1.4 Research questions

In order to be able answer the research problem, it is necessary to see the research problem in context. This could be done by providing a historical background. It is also interesting to look at how the Norwegian Police manages education within the field of digital investigation and if there is a systemic approach to ensure that investigators possess the necessary skills to investigate digital evidence.

These are the research questions which this thesis aim to answer:

I. What is the present status of the field of digital investigation in Norway?
II. What kind of digital forensics knowledge are the police student taught at the Norwegian Police University College?
III. Are there any requirements for doing digital forensics and digital investigation? If yes, what are they?
IV. How competent does an investigator feel when met with digital evidence during an investigation?
V. What can be done to further improve the competency level?

[3] The initial phase in this thesis is from an incident occurs until evidence is acquired.

1.5 Scope and limitations

It became clear that it was impossible to fit everything I wanted into a master thesis. Initially I wanted to research how digital competent the Norwegian police were by doing an extensive questionnaire with tests that could assess how competent the respondents were. The consequences of how possible low competency could effect due process in court were also found to be too extensive for this thesis, even though it would be a quite interesting topic to include.

The scope for this thesis is narrowed down to how competent the respondents *feel* that they are when it comes to the initial phase of a digital investigation. There was still a need for a practical approach in addition to the survey, and the solution was to create a practical test in addition to the survey that was tested on a selected few colleagues.

1.6 Reader guide

After a brief introduction to criminal investigation and digital investigation, the evolvement of digital forensics and digital investigation in Norway is presented in a historical retrospect. In chapter 2.3 the present state of digital forensics and digital investigation in Norway is presented. The present state includes the curriculum related to digital investigation on the bachelor education at the Norwegian Police University College (PHS) and findings from two bachelor theses from PHS. National role descriptions and requirements for investigators are presented, along with the Norwegian Police's strategic goal towards 2025. The last part of chapter 2 is a presentation a framework for training competency created by EU, models used in digital forensics and digital investigation and a framework used to illustrate possible digital competency requirements.

In chapter 3 the general methodology used in the thesis is presented. The results and findings from they survey and practical test is discussed in chapter 4. An overall summary of the findings and recommendations for future work can be found in chapter 5.

2. Background

In order to understand what digital investigation is, it is necessary to understand what an investigation is. This thesis focuses on investigation of criminal cases, and the definition that follows in the next section is limited to criminal investigation.

2.1 Criminal investigation and digital investigation

The Norwegian Criminal Procedure Act (Straffeprosessloven - strpl) states that the the purpose of an investigation is to gather necessary information to decide the issue of indictment, to serve as a preparation for the court's consideration of the issue of criminal liability and, possibly, the question of the determination of reaction, to avert or stop criminal offences or to execute punishment and other reactions.

Objectives of an investigation

To fulfil the requirements of the Criminal Procedure Act §226 it is common to seek answers to the basic questions known as 5WH defined by (Stelfox, 2013) referred to by Årnes (2016, p. 19). 5WH defines the objectives of an investigation as determining *Who* was involved, *Where*

did it happen, *What* happened, *When* did it happen, *Why* did it happen and *How* did it happen. Answer to these questions can be imperative to conduct a proper investigation.

It can be time-consuming to answer all these questions. In November 2018, the Norwegian newspaper Romerikes Blad reported on an indictment in what they described as Norway's most comprehensive sexual abuse case so far. There was one culprit in the case, and the indictment included rape and threats against over 300 young boys from Norway, and also some victims in Sweden and Denmark. There were additionally 160 victims that were not part of the indictment of various reasons. Using different social media the accused man gained the young boys' trust and after a while they sent him nude pictures and videos. If they refused to send more pictures he threatened to publish already received pictures and videos. The indictment also included physical sexual abuse where some of the abuse had been recorded. Up to 15 investigators are reported to have been working with the case, and the accused was have been in custody from autumn 2016. The District Attorney interviewed said there were large amounts of chat logs, movies and pictures that have been time-consuming to review (Romerikes Blad, 2018).

To be able to fully answer *Who* in the indictment there was a need to minimum investigate 461 people; all the victims and the accused. The *Where* could lead to potentially investigating 461 digital crime scenes if there was needed to examine each victims' computer or phone. In addition, the place(s) where the physical sexual abuse happened might need to be examined. These examinations could answer, at least partially, the questions *What*, *When* and *How*. From the information given in the newspaper it is likely that a large amount of the evidence in the case was digital evidence, and that digital investigation has been a key factor in getting the case to the stage on an indictment.

Digital investigation and the initial phase

Digital investigation is in this thesis defined as conducting traditional investigation to fulfil the purpose with investigation in accordance with the Criminal Procedure Act, but with electronic data and information — digital evidence. The initial phase is used to described investigative steps that has to be done from an incident occurs to evidence is acquired. Models which divides the initial phase into smaller phases exist, and they will be further disclosed in chapter 2.5.

Number of reported offences in 2018

In 2018 there was reported a total of 318 566 offences i Norway (Politiet, 2018). Offences committed abroad, but reported in Norway, is included in the total number of offences. It is worth emphasising this is offences who are reported to the police, and the number of unrecorded criminal offences are naturally not included. Computer crime and Information Communication Technology (ICT) related crime are divided into three areas. The first area is *crime form*, offences which target the actual technology or infrastructure. Examples on crime form is hacker attacks and distributed denial of service attacks (DDoS). The next area is *modus.* Modus is related to *how* the crime is committed. Examples of modus which has a digital aspect is online fraud and selling drugs online. The last area is ICT, technology and Internet as a *source for evidence and information*. This area relates to crime that is committed outside the technology sphere, but where digital evidence can be relevant when investigating the case. An example is a homicide case where online communication prior to the homicide can be important.

As of January 2018, it become mandatory for the police districts to register modus for criminal cases. The registration is not complete, and it will take time before correct registration practices are implemented. Because of this, a reservation about the data's validity has been made in the report. In all the cases registered in 2018 a modus related to ICT was found in 5,1% of all the cases, 16225 cases in total (Politiet, 2018).

2.2 History of digital forensics in Norway

To be better able to understand the present status of digital forensics and digital investigation in Norway, it can be necessary to view the evolvement of the field in retrospect. In the following section the field of digital forensics in Norway from 2007 to 2017 is presented, using one master thesis and official reports from two working groups.

2.2.1 Master thesis 2007

In Marit Gjerde's master thesis (2007) the historical background of digital forensics in Norway is described (p. 9). The first Computer Crime Unit (CCU) was created in 1995, and the first computer crime class were held in 1996 by the PHS in collaboration with the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim). The participants in this course were mostly police officers who had a special interest in computers, but they lacked the professional computer technical training and education. In 2004 the first academic digital forensics course were approved, and 11 students graduated from this course in 2005. The requirements for this course included the students having achieved a basic computer technical education provided by the Norwegian Networked University[4] (NNU), a now closed-down university. PHS funded the basic technical education at NNU. The next course were scheduled in 2005, but now the police districts had to fund the basic technical education themselves. This lead to the number of applicants from the police districts falling from 75 to 25 in 2004. When Gjerde wrote her master thesis there was 15 new students attending the course with graduation in in 2007.

The number of digital forensics investigators in Norway in august 2006 were 45. Gjerde (p. 71) highlights that when «*the Norwegian Police start policing the Internet to a much higher degree than they are doing today, to discover and pursue "grooming cases", the Norwegian police districts must even plan more work towards digital forensic tasks than they actually doing today*». According to SSB the percentage of citizens in Norway who has access to Internet in Norway has increased from 83% in 2007 to 98% in 2017. The number of citizens with access to a smartphone was not even surveyed in 2007, and in 2017 the number is 91%. One can assume that Gjerdes statement that the Norwegian police districts must plan *more* work today digital forensic tasks is still valid today.

	Andel som har tilgang til ulike medier og elektroniske tilbud	
	2007	2017
Internett	83	98
Smarttelefon	..	91

FIGURE 1. NUMBER OF NORWEGIAN CITIZENS THAT HAVE ACCESS TO INTERNET AND SMARTPHONE[5]

[4] http://www.nvu.no

[5] Retrieved from ssb.no 31st of May 2019

2.2.2 Storruste-report

The Norwegian Police Directorate (POD) and the Attorney General created a workgroup in 2011 to survey how the police worked with ICT-crime, digital evidence and how they policed the Internet, both in the present and in the future. The working group delivered a report in 2012 (Storruste et al., 2012). In this report they provide the number of computer forensics investigators in the police districts which varies from zero to three with the exception of the largest police district that has 14 employees who conducts digital forensics investigation. The working group points out that digital evidence can be overlooked because the technological competency to ordinary police officers are not sufficient enough to be able to identify which possible digital evidence can be found using a computer forensics approach. Furthermore, understanding technology and using technology is not a part of the bachelor education for the police students at PHS, and the police districts themselves have to provide this training but this is only partially done (p. 20).

The report from 2012 also mentions data seizures, and how this is normally done by the police generalists, and that *far from all* has the competency to do this this correct (p. 20). The working group points out the police generalists' need for a basic competency about technology and the possibilities and challenges that technology has when fighting crime. Knowledge about how data equipment, cell phones and other technical equipment can contribute to solve an investigation will be more important in future police work. Lastly, they point out that the police generalist should know how to handle technological equipment on a crime scene or during an apprehension. The generalist should also have knowledge about the simplest form of acquisition and extraction of information from equipment which can be used in an acute phase (p. 26).

2.2.3 Lystad-report

In 2017 a working group tasked by POD wrote about capacity and competence need for the Norwegian police for the next ten years to come. When they write about computer crime they state that «*anyone who is going to work with the police's core tasks must therefore have a basic understanding of how computers, computer systems, and computer networks functions*». The police education at bachelor level has ten credits within *digital police work*, and by attending a continuing education it is possible to obtain additional 25 credits with the course «*Nordic Computer Forensics Investigator (NCFI)*». However, the report claims that attending the course NCFI does not give sufficient competency to fight cyber dependant and cyber-enabled crime (Lystad et al., 2017, p. 20).

From Gjerde's master thesis in 2007 and from the working groups reports in 2012 and 2017 it becomes clear the focus on digital investigation has changed and improved as the years has gone by. From 45 specialised computer forensics investigators in 2007 there is in 2012 a desire that the police generalist, the majority of the police force, should know how to handle technological equipment on a crime scene. Lastly, in 2017 the working group states that everyone working with police core task *must* have a basic understanding on how computers, computer systems and computer networks function. It seems the focus on competence has changed from a few specialised computer forensics investigators to where the majority of the police force are expected to have a basic digital competency level.

In the next section the present state of digital investigation in Norway will be outlined.

2.3 Present state of digital forensics and digital investigation in Norway

From the historical retrospective in the previous chapter, the development of the digital investigation and digital forensics can be seen. There has also been an increase in focus on digital investigation. In the following chapter the present state in Norway is presented. The chapter consists of the current status of the various CCUs and the past and current curriculum related to digital investigation from PHS. Relevant findings from two recent bachelor theses from PHS are also presented, as well as a presentation of national role requirements and descriptions set by POD.

2.3.1 Status Computer Crime Units 2018

In October 2018 an inquiry was sent out to the respective heads of computer crime units in each police district in Norway asking the following questions:

- How many employees do you have in your unit
- What is the ratio of civilian/police background for your employees
- For how long have your employees worked with digital investigation
- What kind of formal competency do they have within digital investigation

Number of employees in the CCUs in Norway

The *exact* number of employees in the various CCUs in Norway can not be disclosed in this thesis, as revealing the Norwegian police's capacity within digital forensics investigation can jeopardise the operational safety.

However, what can be done is to compare it with the numbers provided in the Storruste-report from 2012. In 2012 there were 27 police districts in Norway. Today the number of police districts is twelve (Innst. 306 S (2014-2015), p. 7). In 2012 the number of computer forensics investigators in each district, except the largest, varied from zero to three. Today the minimum computer forensics investigator in a district is three, and the average is somewhat higher.

The number of computer forensics investigators might be skewed when the Norwegian police reform, *Nærpolitireformen (2018)*, is taken into account. What seemingly looks like an increase in number of computer forensics investigators in one of the new police districts might be a result of merging old police districts into a new district and thus transferring the computer forensics investigators into the new one.

This can be illustrated with the following example: Øst police district had a job advertisement for two computer forensics investigators at a job advertisement site (KarriereStart.no) where the number of employees at the CCU was listed as seven. This indicates that Øst police district has around nine computer forensics investigators if the two advertised positions were filled. Øst police district is comprised of the old police districts Østfold, Follo and Romerike (Innst. 306 S (2014-2015), p. 48). If all three of the original police districts answered that they had three computer forensics investigators, the maximum amount mentioned in the report, this means there has been no real increase in the number of computer forensics investigators in Øst police district since 2012.

The actual number of computer forensics investigators in the Storruste-report has not been pursued further, partly because it lands somewhat outside the scope of this thesis and partly

because the results combined with the findings in this master thesis can not be disclosed publicly due to operational safety. But research into if there has been a real increase in computer forensics investigators in Norway might nevertheless be something which should be looked closer at in a later study.

Civilian and police ratio
In the Storruste-report the ratio between computer forensics investigators with a police background or technical background is not specified. In October 2018 roughly 62% of the computer forensics investigators in Norway had a police background, while the rest had various technical backgrounds.

Years of experience
Several of the CCUs answered that their investigators have worked for several years within the field of digital investigation. The majority of investigators have worked longer than one year, and several have worked with digital investigation for five years plus.

Formal competency within the CCUs
Each CCU has at least one investigator who has attended the «*Nordic Computer Forensics Investigator module 2*» course at PHS. This course will be covered in the next section.

Most of the CCUs have at least one investigator who has attended courses in digital forensics tools such as EnCase[6] or X-Ways[7].

2.3.2 Curriculum The Norwegian Police University College

PHS is responsible for providing «*fundamental training for service in the police service or county administration, as well as post graduate studies for employees of the police service*» as stated on their webpage.

PHS provide three different main studies; Bachelor in Police studies, various police related master's programs and post graduate studies. One of the master's programs they provide is a Master in Digital Forensics and Cybercrime Investigation that is offered in partnership with NTNU. This thesis is part of that master's program.

Bachelor in Police studies - Curriculum
There have been adjustments the last five years in regard to how much of the curriculum which includes digital investigation and digital evidence. For the reader's benefit these changes will be presented in this section, and not in the section for the historical overview.

Bachelor students that graduated before 2011
According to Ulf Bergum at PHS, the students who graduated before 2011 did not have any mandatory curriculum which included digital evidence. They could, at the end of the semester, choose a specialisation course for digital evidence worth five credits. This specialisation course started around 2003, and it had originally room for 24 students. From 2008 this was expanded to have room for up to two classes, 48 students.

[6] https://www.guidancesoftware.com/encase-forensic

[7] http://www.x-ways.net

Bachelor students that graduated in 2015
These students did not have any element of digital evidence or digital investigation on their curriculum in their first bachelor year (Politihøgskolen, 2012). In their last bachelor year they had digital evidence as one of several subjects in the module «*Investigation*»[8] (Politihøgskolen, 2014, p. 40). The course gave twelve credits, and was divided into the following topics:

4 credits in Criminal law and criminal proceedings
3 credits in Report and investigation theory
3 credits in Psychology
2 credits in Crime Technique[9]

The learning outcome was that the students should have knowledge about the investigation method in digital evidence, among other methods such as investigation, stakeouts, intelligence, witness confrontation and criminal analysis. They should also have knowledge about the Penal Code in selected topics which included computer crime and digital evidence.

It was expected that the students worked around 360 hours with the module «*Investigation*». When looking at the way the credits were divided it is rather easy to see there were simply not enough time, or within the scope, to include comprehensive material about digital evidence and digital investigation.

At the end of the semester, each student could choose a specialisation course which was weighted six credits. «*Electronic evidence*»[10], ETFE350, were one of ten specialisation courses. This means that those students that choose this specialisation course got the same amount of credits just within the field of digital evidence as the total amount of credits for the courses «*Report and investigation theory*» and «*Psychology*» combined.

Bachelor students graduating in 2019
The students who started in 2016 had digital evidence and digital investigation on the curriculum from their first bachelor year. In the module «*Digital Policing and Investigation*» they obtained four credits. The module summarised:

> *In the first year of study, the subject focuses on giving the student an introduction to information technology that lays the foundation for the further work on the subject. Furthermore, after the first year of study, the students will have a practical understanding of how to handle digital devices as evidence as the first unit on site.*

Knowledge the students would have after finished the module was for example:

- How Internet and Network communication works
- What potential evidence value a mobile phone can have in a criminal case
- The process of storing data and how vulnerable data are
- The importance of having notoriety when handling digital units

[8] Direct translation from the Norwegian word «*Etterforskning*»

[9] Direct translation from the Norwegian word «*Kriminalteknikk*»

[10] Direct translation from the Norwegian words «*Elektroniske spor*»

Among the skills the students would obtain was to identify potential evidence on the Internet, and secure (Norwegian: sikre) digital units in a correct and proper way. In the curriculum the Norwegian word *sikre* is used. This word can both be used when you seize *and* acquire an item. Proper acquisition of a physical item requires some degree of training and background knowledge, and since this is an introductory course with four credits it is reasonable to assume the word *sikre* here can be interpreted to the action of *seizing* an item properly, and not to acquire (Politihøgskolen, 2016, p. 20).

In the second bachelor year, where the student is seconded in a police district the whole year, the student should, among other learning outcomes, obtain knowledge about how digital evidence can be identified, acquired, analysed and documented as part of a criminal case (Politihøgskolen, 2016, p. 42). This is formalised in the course «*Digital Policing and Investigation*» which in the second bachelor year gives two credits. The students also have a ten credit course in «*Investigation*» the second year, where knowledge of acquisition of digital evidence and skills of actually acquiring digital evidence are the learning outcomes (Politihøgskolen, 2016, p. 53).

During the last bachelor year the students do not have an option to select a specialisation course within digital evidence. However, the course «*Digital Policing and Investigation*» is mandatory for everyone, and gives four credits. Excerpt from the curriculum (Politihøgskolen, 2016, p. 61):

> *In the third year of study, the students will receive training on how to investigate on the Internet and how they can secure and analyse electronic evidence and how they can use electronic evidence in an investigation. The students will also focus on writing report in regard to securing and analysing digital evidence.*

Some of the skills the students should possess when they graduate are the ability to handle digital units in a way that effects the data in the least way possible and use tools to process and analyse digital evidence. They should also be able to identify and acquire evidence from the Internet. Finally, the students should be able to use a methodical approach when investigating digital evidence.

Based on the findings it can be established that the Norwegian Police University College have changed the curriculum to focus more on digital investigation and digital evidence with a revision of the curriculum from 2015 to 2019. From a course with 12 credits, which were divided on several topics and only included digital investigation in a small scale and a specialisation course within digital investigation who gave six credits (a course not every student were able to attend), to mandatory digital evidence and digital investigation courses throughout every year at the bachelor for a total of ten credits.

What are the Norwegian Police University College’s plans for the future police students?

Bachelor students graduating in 2021

According to the curriculum for students starting in 2019 and graduating in 2021 there have been some revisions when it comes to digital investigation and digital evidence (Politihøgskolen, 2018).

The course «*Digital Policing and Investigation*» is continued, and it still is four credits. One skill that is added are that they students should be able to identify storage medias that can contain

evidence. The students should be able to identify Internet Service Providers (ISP) and obtain Basic Subscriber Information (BSI) according to the study plan (2018).

In the second year the course «*Digital Policing and Investigation*» is continued with two credits. The knowledge learning outcome about how an electronic evidence can be identified, acquired, analysed and documented is removed. It has not been found in is present writing form another place in the curriculum. In the course «*Investigation*» the learning outcomes when it comes to digital evidence is the same.

The third year still include the course «*Digital Policing and Investigation*» with four credits.

Post graduate studies - Digital forensics related studies

PHS provides over 90 different post graduate courses. The courses range from management oriented courses to courses related to investigation and forensics. Ten of the courses they provide are directly related to computer forensics investigation. All those courses are within the «*Nordic Computer Forensic Investigators*» family, and they are divided into modules. Module 1 is mandatory for everyone that wants to pursue the other modules. The target group for module 1 is stated on the PHS website to be «*police staff in the Nordic countries whose main task is or will be handling and investigating digital evidence*». After module 1 is passed there is possible to specialise within a different field within computer forensics, for example Network Forensics and Cybercrime.

TABLE 1. DIGITAL FORENSICS POST GRADUATE STUDIES PROVIDED BY THE NORWEGIAN POLICE UNIVERSITY COLLEGE

Course name	Credits	Fall 2019	Spring 2020	Fall 2020	Spring 2021	Fall 2021
Module 1: Core Concepts in Digital Investigation and Forensics	15	X	X	X		
Module 2A: Advanced Computer Forensics	15	X	X	X	X	
Module 2B: Online Investigation	15	X		X		X
Module 2C: Network Forensics and Cybercrime	15	X				
Module 3A: Forensic Tool Development	7,5		X		X	
Module 3B: Linux Artifacts	7,5		X		X	
Module 3C: Open Source Forensics	7,5	X		X		X
Module 3D: Macintosh Computer Forensics	7,5		X		X	
Module 3E: Windows Forensics	7,5	X		X		X
Module 3F: Memory Investigation	7,5	X				
Tool courses						
Digital forensics with EnCase Forensics - Module 1 Basic	Continuous admission					
Digital forensics with X-Ways Forensics - Module 1 Basic	Continuous admission					
Digital forensics with X-Ways Forensics - Module 2 Advanced	Continuous admission					

There is also a post graduate study for investigation, «*Videreutdanning i etterforskning*». The module gives 15 credits, and the participants are employees who have, or are intended to have, investigation as their primary work task. After graduating from the course the students should have knowledge about digital evidence in an investigation, and they should be able to safeguard digital evidence on a crime scene. They should also be able to acquire (Norwegian: sikre) digital evidence on the Internet (Politihøgskolen, 2017).

2.3.3 Bachelor theses from PHS 2018-2019

In the last year there has been submitted at least two bachelor theses at the Norwegian Police University College related to digital police work. Note: All quotes were originally in Norwegian, and has been translated to English by me. The theses contains information that is relevant to highlight the present state of digital investigation, and have therefore been included in this chapter.

Thesis from 2018

Hondrelis and Ingwersen wrote the thesis «*Digitalt politiarbeid - En teoretisk oppgave*» in 2018. The thesis was top rated with the grade A. Their research problem were related to how the Norwegian police adapt to today's technological development, and how the police has invested in digital police work and the use of modern technology.

The Norwegian police are in this thesis described as a «*professional bureaucracy*» where the organisation contains elements of both hierarchy and bureaucracy (p. 15). The concept of «*knowledge organisations*»[11] is presented, where the general idea is the decentralisation of organisations due to the prevalence of the Internet. Among the different public sectors in Norway the police is possibly one of those that has come shortest in becoming a knowledge organisation. This might be because the police does not want to let go of their over-controlled hierarchies. Another reason is mentioned to be because the police refuses to change the way organisation and management is done, whereas change is necessary to transform into a knowledge organisation.

One leader of a computer crime unit in Norway tells that the police is governed by processes that often take a while to be finished. When something is decided to be implemented, the actual implementation still takes a while (p. 19). Because changes takes a while to be implemented, the technological evolution might be a challenge for the Norwegian police. Even though Moore's law about how fast technology evolves (a doubling in performance every 18 months) might be obsolete, it still might be relevant in order to understand how fast technology evolves and how an organisation should be organised to be able to handle the new and changed technology.

The role «*Professional contact*»[12] is briefly described in the thesis. A professional contact is a regular police officer that receives training from a computer crime unit. After the training the professional contact can guide other colleagues and help them solve technical challenges on a certain level. If the challenge is too great the issue has to be resolved by the computer crime unit (p. 18). The authors point out that the implementation of the professional contact might be a good idea, but they also ask the question if creating professional contacts might amplify the distance between regular police officers and «*those that work with computer stuff and technology*» (p. 19).

A survey, «*Mørketallsundersøkelsen*» conducted by The Norwegian Business and Industry Security Council (NSR) in 2016 showed that only 9% of businesses that experienced digital attacks contacted the police. One reason for not contacting the police was that there was a lack of faith in the police's competency to solve the issue (p. 21). The importance of reporting computer crimes to the police is mentioned. By reporting computer crimes, the number of

[11] Direct translation from the Norwegian word «K*unnskapsorganisasjoner*»

[12] Direct translation from the Norwegian word «*Fagkontakt*»

unrecorded crimes will be reduced, and it will provide documentation the police need to focus both on increasing competency and resources towards digital police work (p. 22).

The importance of digital evidence in criminal cases and the consequences of not improving the digital competency is summarised by a quote from Schjølberg (2017):

> *Digital evidence have become very important and often crucial evidence in criminal cases, and the absence of competence development can have a decisive impact on the police's ability to solve cyber crime.*

Thesis from 2019

E. Grøtan wrote a thesis in 2019 about the professional contacts role within investigation of digital evidence. The thesis was top rated with the grade A. She is one of the many students that graduate in 2019, and she has followed the curriculum that has been mentioned in section 2.3.2. In addition to following the compulsory curriculum she has attended the post graduate study NCFI Core during her second bachelor year as part of a pilot project. Her motivation for choosing the topic was:

> *I experienced that the frontline police have many questions and little knowledge about the general handling of digital evidence for investigation purposes. This leads to a general frustration among many. Much time is lost in the attempt to understand something that one does not have the ability to handle and valuable evidence in important cases are overlooked or lost due to lack of understanding and competence. Cases that could have been handled locally are sent to centralised units where they are shelved because larger cases are prioritised.*

Her research problem is «*How do frontline professional contacts work as a competence boost for the police when securing and analysing digital evidence*». Digital evidence is narrowed down to data from a mobile phone, specifically data that is stored locally; e.g. messages, phone records, pictures, videos and files. She argues that she has narrowed it down to mobile phone because this is a digital evidence that is often found by first responders. A mobile phone is relevant in several criminal cases and it can contain potential important evidence (p. 4).

The professional contacts role is defined by POD in the paper «*Rammer og retningslinjer*» to «*be an advisor for own unit within digital evidence, be a professional contact between own unit and the function for digital police work, be the contact person and communicate new methods and new knowledge within digital investigation into their own unit*» (p. 4).

Grøtan writes that according to Bjerknes and Fahsing (2018) digital evidence should get the same attention as other types of evidence in regards to gathering, and that it is decisive that the investigative competency for handling digital evidence is equal to the competency needed for conducting interviews or acquisition of DNA traces. From her qualitative study she has quoted two interviewed where the first said «*There is not a single criminal case we have today where there are no digital evidence on mobile phones*» and the other said «*For an investigator, it will be very useful to have knowledge of digital evidence. We come across digital evidence in just about every case. Or at least you can find information there, and it is important to know something about it*» (p. 11).

Bjerknes and Fahsing (2018) is on page 17 cited on the importance of notoriety, and that the notoriety requires clear, professional and understandable statements of what has been

acquired. What is deemed to be a fact and what is uncertain must also be stated. Further on the same page the importance of quality assurance is pointed out, as stated by Bjerknes and Johansen (2013). The purpose of quality assurance is to ensure that the digital evidence is legitimate and that they do not contribute to jeopardise the rule of law[13].

Grøtan's findings are that the role of professional contacts in the Norwegian police contributes to a heightened competency level for handling digital evidence. The professional contacts acquire digital evidence in criminal cases that, due to lack of capacity from computer crime units, would not have been prioritised.

2.3.4 National role requirements and descriptions

POD approved national role requirements and descriptions v1.0 on January 10, 2019. The final version has not been found to be published online. However, the Norwegian Association of the Chiefs of Police has posted v0.7 on their website (Politidirektoratet, 2018). Note: The document has been revised from v0.7 to the final version v1.0. The document is one step closer to a unified approach in regards to investigation regardless of which police district, or police station, responsible for the investigation.

> *The purpose of national role definitions is to ensure equal responsibility, authority, content and competence in equal roles across districts and special agencies, as well as security for the police to safeguard their social mission related to criminal proceedings, also in extraordinary incidents. This document clarifies responsibilities, tasks and competence requirements through the preparation of national role definitions and related competence requirements for managers and employees in the field of investigation.*

By implementing national role requirements it will be easier to manage measures for improving the competency, and both internal collaboration in a police district and external collaboration between two police districts will be easier. One example can be if Vest police district suddenly has a need for five extra computer forensics investigators to be able to handle a large criminal case. With national role requirements it will be easy for them to borrow those computer forensics investigators from Finnmark and Agder police distrikt. As long as the investigators meet the minimum requirements Vest will instantly know what kind of capacity they can expect to receive.

In the document there is distinction between position and role. Each employee has a position code (SKO). A police superintendent is normally in the position code 0287, and a special investigator has position kode 1552. According to the Agency for Public Management and eGovernment[14] the position codes is linked to minimum wage, and some position codes gives higher pay the longer you have worked by following the principles of seniority (Direktoratet for Forvaltning og IKT, 2017). The position code are not an obstacle for filling multiple roles. The roles are proposed used as working titles.

POD points out that the number of roles has been kept to a minimum for the first implementation of national role requirements in order to establish an executive description of the roles. The documents will be continuously revised when needed, and new or changed roles could be implemented. A guiding principle is to not use exhaustive role descriptions, and to not

[13] Directly translated from the Norwegian word «*Rettssikkerhet*»

[14] Direktoratet for Forvaltning og IKT, www.difi.no

limit the managerial prerogative. In the future it is a desire to define actual skills and knowledge and not only formal qualifications (Politidirektoratet, 2019, pp. 5-6).

The role requirements and descriptions are divided into managerial and executive roles. In the executive roles prosecutor and chief investigator are mentioned, as well as the police generalist and computer forensics investigator. The scope of this thesis is the police generalist, but the requirements for chief investigator and computer forensics investigator will also be mentioned to put the requirements into context.

Chief Investigator, role requirements and description

The chief investigator (CI) leads the investigation in a criminal case where other investigators are involved. They are responsible for organising and carrying out the investigation with high quality in accordance with current regulations, given directives, professional standards and recognised research methods. The use of relevant specialist competency when needed is also the CI's responsibility.

Among several tasks the CI should contribute so the investigation group is manned with enough personell with the right competency, and the CI should also conduct quality assurance when needed. Note: The listed tasks are all mentioned with «*among other tasks*». As mentioned above the tasks are not meant to be exhaustive.

To be a CI the minimum formal competency is completion of the Norwegian Police University College or other relevant education on a bachelor level. Desirable, but not required, post graduate studies are «*Videreutdanning i etterforskning*» or equivalent, «*Funksjonsrettet ledelse for etterforskningsleder*» or equivalent and «*Veiledningspedagogikk 1*». Of these three only «*Videreutdanning i etterforskning*» has an element of digital evidence, according to the course curriculum.

The role requires minimum five years experience within the field of investigation (Politidirektoratet, 2019, pp. 17-18).

Police generalist, role requirements and description

The generalist is described as being the key player in the Norwegian police. They should have competence to perform overall assessments and get support from relevant specialists when needed. Within the field of investigation the generalist should investigate criminal bases, both technical and tactical, as a first responder on a crime scene. They should also investigate criminal cases on site at a police station.

The only responsibility listed is to ensure that allotted cases or investigative steps are investigated with high quality in accordance with currents regulations, given directives, professional standards and recognised research methods. This means each generalist, as an overall, has the same personal responsibility as the CI.

From listed tasks the generalist's main task is to conduct a wide range of investigative steps, optionally under supervision. Note: The listed tasks are all mentioned with «*among other tasks*». As mentioned above the tasks are not meant to be exhaustive.

In regards to formal competency, the only requirement is graduating from the Norwegian Police University College or other relevant education on a bachelor level. Employees without an

education from PHS must complete the course «*Innføring i begrenset politimyndighet Module 1 and 2*»[15].

There are no requirements for experience or other competency (Politidirektoratet, 2019, p. 21).

Computer forensics investigator, role requirements and description
The computer forensics investigator (CFI) has computer forensics investigation as a primary task. They should identify, acquire (Norwegian: sikre), analyse and document digital evidence to shed a light on, and prove, what has happened.

The CFI's responsibility is to support an investigation with professional competency and to be an advisor for other units in the police district.

Among the tasks the CFI should conduct are collection of digital evidence with high quality in accordance with current regulations, given directives, professional standards and recognised research methods. The CFI should also facilitate so that tactical investigators can review the digital evidence. Note: The listed tasks are all mentioned with «*among other tasks*». As mentioned above the tasks are not meant to be exhaustive.

Formal requirements are that the CFI has to have graduated from PHS, or other relevant education on bachelor level. The post graduate study «*Nordic Computer Forensics Investigator module 1 Core Concepts in Digital Forensics and Investigation*» or equivalent must also be passed. There is a desire, but not mandatory, that the post graduate study «*Videreutdanning i etterforskning*» or equivalent is passed.

The role requires minimum three years experience within the field (Politidirektoratet, 2019, pp. 22-23).

Summary, role requirements and descriptions
Based solely on the requirements outlined in the previous sections, there seems to be no specific requirements for competence within digital investigation in order to investigate digital evidence. A police generalist who graduated before PHS implemented digital evidence in the curriculum can, in the utmost consequence, be tasked to investigate criminal cases with an abundance of digital evidence without having any digital competency.

The generalist can be lead by a chief investigator who also does not have any knowledge about digital evidence, at least not any formal competence. It is important to stress this is a worst case scenario, and that one of the CI's responsibilities is to use specialist competence when needed. Hopefully this ensures that a CI seeks guidance from colleagues who has relevant competency in regards to digital evidence when needed.

The findings above can be backed by Nina Sundes master thesis (2017). She writes «*There are no defined competency criteria for handling digital evidence within a criminal investigation*». Furthermore, she writes «*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.*» (Sunde, 2017, p. 104). The national role requirements outlined above came six months after Sunde wrote her thesis, but there does not seem to be any change when it comes to requirements for handling, or actually investigating, digital

[15] Translates to «*Introduction to limited police authority*»

evidence. The importance of having (enough) competency when seizing evidence is summarised in Sundes thesis (2017, pp. 106-107):

> *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.*

Grøtan (2019) refers to a report from the CCU in Oslo police district from 2018 which recommends all professional contacts attending the post graduate study NCFI Core so they will hold competency within acquisition (Norwegian: sikre) of digital devices at a crime scene, and a general introduction to various digital devices. This means the CCU in Oslo recommends that the professional contacts receive the same amount of formal education within digital evidence that POD has defined to be the minimum for the actual computer forensics investigators. One can ask if the CCU are ambitious for the professional contacts, or if POD have set the threshold for competency too low.

It can be established that competency for digital evidence is important. The Norwegian police does not have any obvious requirements for the generalist investigators who might investigate digital evidence.

2.3.5 The Norwegian Police towards 2025

POD has published the goals for the Norwegian Police towards 2025 (Politidirektoratet, 2017). In the publication there are four main topics, where «*Safety in the digital space*»[16] and «*A modern and competent police*» are two of the main topics.

In 2025 one goal is to face crime effectively in the digital room. The second goal is to utilise technology and expertise, be flexible and have the ability to learn and develop. Some short-term goals for 2020 that are relevant for digital investigation are listed (p. 12):

In 2020, the Norwegian police will:

- investigate and process criminal cases according to standards and expectations, comply with process requirements and have good notoriety
- implement and prioritise the right investigative efforts with competent employees as early as possible (in the initial phase) in criminal cases
- have the necessary capacity, technical and police expertise centrally and locally, for secure storage, sharing and analysis of digital evidence and digital information

In chapter 5 the short-term goals for 2020 will be discussed in context of the findings in chapter 4.

[16] Directly translated from the Norwegian words «*Trygghet i det digitale rom*»

2.4 European Union training competency framework

In March 2018 an interdepartmental working group consisting of members from the European Union Agency for Law Enforcement Training (CEPOL), the European Unions's Judicial Cooperation Unit (Eurojust), European Cybercrime Centre (EC3) and the European Cybercrime Training and Education Group (ECTEG) completed a report related to a training competency framework on cybercrime (CEPOL et al., 2018). They identified competencies, skills and training needs for key actors involved in combating cybercrime. The key actors were both from law enforcement and the judiciary.

The working group identifed twelve profiles where each profile was assigned a recommended competence level from basic to expert. The profiles covered patrol officers, general investigators, procecutors and judges. Managers and political and strategical decision makers were also assigned a profile. Due to the scope of this thesis only the profiles for patrol officers and general investigators will be covered.

First responders

In the report, first responders refers to law enforcement officers who are the first to come in contact with potential digital evidence. For the Norwegian police this will be equivalent to the police officers on patrol duty. It is worth mentioning that the first reponder training is expected to be completed by *all* the twelve profiles.

The first responders require «*basic knowledge of digital forensics tools and practices, including live data forensics, as well as general awareness and knowledge about cybercrime*». Furthermore, the benefits of knowledge about what traces can be recovered by a specialist and how these traces can contribute to the further investigation is highlighted. Lastly, the first responders should be able to ask crime related questions and provide guidance and basic advice to victims of crimes enabled by new technology. The last requirement could enable the Norwegian police officers to ask sufficient, and relevant, questions at an initial phase of a digital investigation. It would also enable police officers to provide guidance, both preventive and reactive, to the Norwegian citizens.

Training requirements recommended for the first responder:

- Standards and best practices in electronic evidence identification and seizing
- Basic live data forensics acquisition
- Basic knowledge on digital forensics (tools, techniques, methods and best practices), including internet technology, the darkweb and cryptocurrencies
- Crime scene management
- Interview techniques
- General cybercrime awareness

General criminal investigators

This profile is described to face an increased use of Internet and digital tools used by criminals. A fundamental understanding of the digital world is recommended. The need for a digital awareness is underlined.

The training for general criminal investigators should include lists on how to conduct digital seizures, how to handle digital material, basic legislation related to digital evidence and the collaboration with specialised colleagues.

Training requirements recommended for the general criminal investigator:

- General cybercrime awareness
- Understanding of networking and tracing IP addresses
- Fundamental knowledge of legal and jurisdiction issues
- Crime scene examination skills
- Requesting and processing data from third parties
- Open source intelligence
- Evidence presentation

Training competency framework summary

The framework illustrates the expected level of skills from key actors who has to face digital investigation. It should be noted that recommended competence for managers and political decision makers are included. The framework can be used in a process of developing a national training programme for Norwegian police employees. This is further described in chapter 5.2.1.

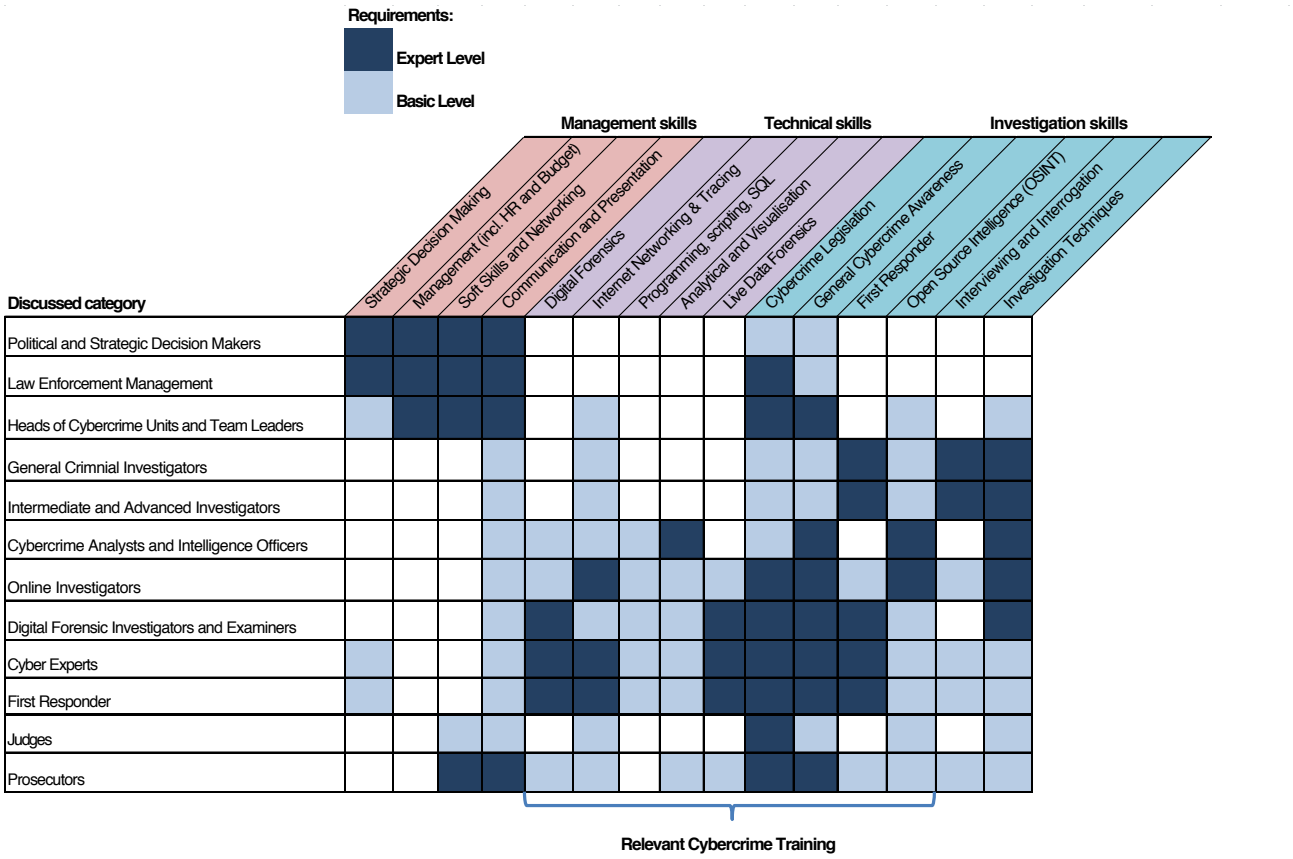


FIGURE 2. MATRIX OF REQUIRED KNOWLEDGE AND SKILLS FOR LE AND JUDICIAL ACTORS (CEPOL ET AL., 2018)

2.5 Digital forensics investigation process models and ISO standard

Two different models related to digital forensics and investigation, and the current ISO standard will be presented in this chapter. The first model is the Digital Forensics Process, which is suitable for a digital forensics investigation, regardless of if it is used by a law enforcement agency or a civil organisation. The other model is a Process Model for Investigation which is well-suited for systematic examination such as a criminal investigation. Lastly, in this chapter an overview of the current ISO standard 27037 will be presented.

2.5.1 Digital Forensics Process

The digital forensics process is a normative presentation of the different phases in a digital forensics investigation. It consists of five consecutive, and iterative, phases and is based on the same principles which adhere to a traditional physical forensics investigation process. The process normally starts with an incident or a crime, and the consecutive phases are *Identification*, *Collection*, *Examination*, *Analysis* and *Presentation*. Based on the crime a hypothesis, or multiple hypotheses, are created which leads to an investigation (Årnes, 2016).

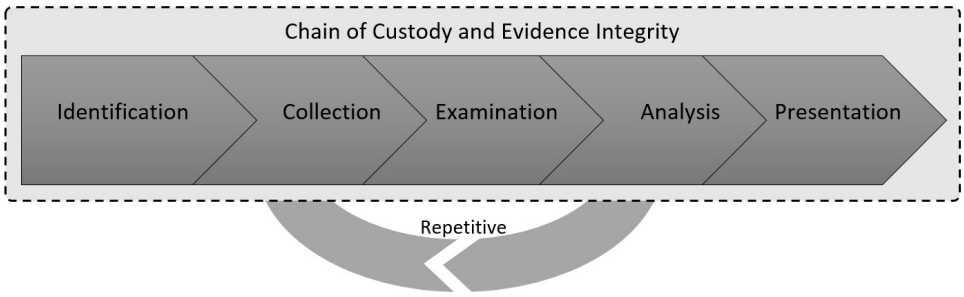


FIGURE 3. THE DIGITAL FORENSICS PROCESS ILLUSTRATED BY FLAGLIEN (ÅRNES, 2016)

To use the digital forensics process in a practical approach, imagine the following scenario: The police have received a complaint regarding Kenneth that allegedly have taken pictures of other people in the shower at the local gym, and the police officers are standing outside his door. To keep it simple the police officers have two hypotheses (H); H1: Kenneth has taken pictures in the shower and H2: Kenneth has not taken pictures in the shower.

The police officers conducting the house search starts working on the Identification-phase of the process. In order to be able to identify relevant devices they first have to have knowledge of the case. They have to know the case is related to pictures in order to properly identity devices which are connected to pictures. Furthermore, they have to have the skills to *remember* how a device that can contain digital evidence like pictures look like. If either case knowledge, or the digital skill of remembering is missing, the police officers can fail to identify digital evidence which would be crucial in the scenario with Kenneth. The scope for this thesis stops after collection, but for the reader's benefit the rest of the scenario will be played out using how the digital forensics process is implemented.

In our scenario the police officers successfully identify a digital camera and one external hard drive. They seize both devices, and turn them over to the local CCU. There, a computer forensics investigator *collects* (acquires) both devices using forensically sound methods. The acquired content is *examined* by the computer forensics investigator, and some deleted pictures are recovered. An investigator conducts the *analysis* of the content from the digital camera and the external hard drive, and writes a formal report on the findings. Finally, the investigator *presents* the findings in court.

2.5.2 A process model for investigation

The digital forensics process presented in chapter 2.5.1 can be used as an executive framework for digital forensics investigation. Designed for a superior level aimed at digital forensics, and due to the absence of a *continuous evaluation* of hypotheses, the digital forensics process might not be suitable for illustrating the detailed workflow in a criminal investigation. Andersen (2019) has developed an investigation process model designed to be applied in situations where a systematic examination is performed. The objectives of an investigation, as outlined in chapter 2.1, will benefit from using a systematic approach to answer the questions related to 5WH. Andersen's model is flexible, and can also be used for any incident response situations by minor adjustments in the phases.

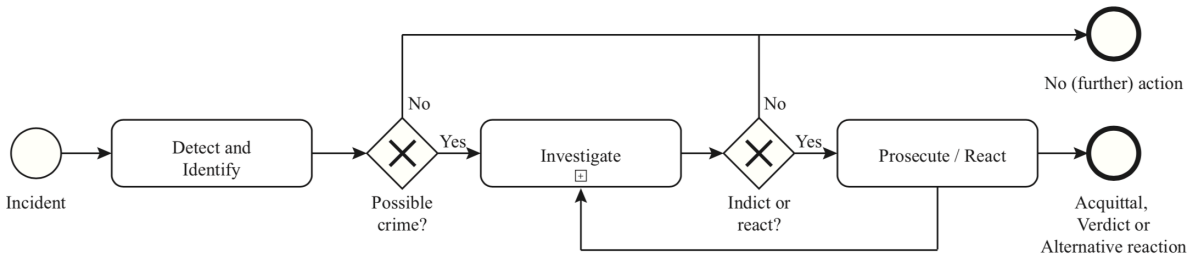


FIGURE 4. CRIMINAL CASE MODEL (ANDERSEN, 2019)

As with the digital forensics process, Andersen's model include an incident or event that leads to at least one hypothesis. After this the two models are different. While the Digital Forensics Process goes directly to identification of evidence, the criminal case model, after having determined a possible crime has occured, starts with the Investigate phase. The first object in the Investigate phase is *formulating hypotheses*. Based on the hypotheses formulated, relevant data sources who can evaluate the hypotheses must be *identified and located*. After information needs are identified, the next main phase is collection and processing of data.

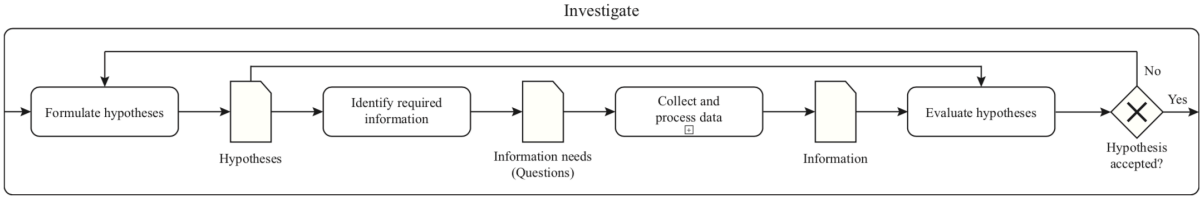


FIGURE 5. CRIMINAL INVESTIGATION MODEL (ANDERSEN, 2019)

In the phase for collection and processing of data, the data sources must be *identified* and *located*. After the data sources are located, the actual data must be *acquired*. The results from the acquisition will generate *raw data*, and it will most likely result in more data than needed to evaluate the hypotheses. The raw data must be *explored* to identify the relevant data,

illustrated as *significant data*. When the significant data is identified, this data must be *analysed* to yield information which can be used to *evaluate the information*. When all the available information is evaluated against the hypotheses, the investigation is completed. The final step in a criminal investigation is to determine if there is sufficient evidence to produce an indictment. It should be noted that the process model is meant to be a continuously looping process which continues until the systematic examination is complete. For a criminal investigation, this means until the case is finally settled, regardless of how the case is settled.

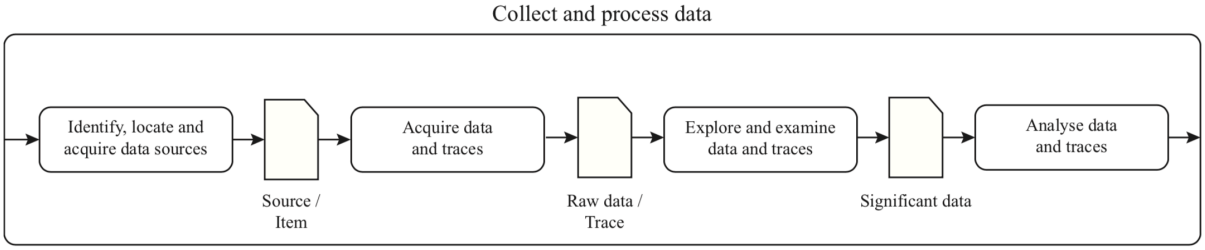


FIGURE 6. DATA COLLECTION AND PROCESSING PROCESS MODEL (ANDERSEN, 2019)

The main scope for this thesis includes the phase with formulating hypotheses and ends after the raw data has been acquired. However, in the survey some aspect from the phases exploration had been included. There are also included elements from giving presentation in court, and these elements comes *after* the final step in the process model for investigation.

The phases from formulating hypothesis to acquisition will be further discussed with the practical test in chapter 4.2.

2.5.3 ISO 27037

The International Organization for Standardization[17] develops standards for various purposes. They have created the ISO standard 27037 that include guidelines for identification, collection, acquisition and preservation of digital evidence (International Organization of Standardization, 2012). Compared with the digital forensics process, the guidelines covers the phases identification and collection. If we look at Andersen's model presented in Figure 6, the guidelines covers the step after hypothesis up to the phase of data exploration. The guidelines can be used in order to produce a framework for what competency can be required to perform initial digital investigative steps.

Scope of the standard
The standard covers traditional devices such as digital storage media, mobile phones, digital still and video cameras and standard computers. These are all devices that a police officers can expect to encounter during a normal investigation. Digital evidence like social media accounts are not specifically mentioned, as the list is not exhaustive.

Definitions
A Digital Evidence First Responder (DEFR) is an «*individual who is authorised, trained and qualified to act first at an incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence*» (International Organization of Standardization, 2012, p. 2). A police officer that arrives first on a crime scene, and is tasked with collecting digital evidence will fall in the same category as a DEFR. The same will an

[17] https://www.iso.org/home.html

investigator that needs to acquire a social media account during an investigation. For the rest of this chapter, whenever DEFR is written it can be directly transferable to a police officer on patrol duty or a police officer conducting investigation.

Principles of digital evidence

According to the standard, digital evidence is comprised of three elements; relevance, reliability and sufficiency. This can also be transferred to traditional evidence. The evidence has be relevant to the case, either to refute or strengthen a hypothesis. Secondly, the evidence has to be reliable, and to be valid it must be able to withstand scrutiny. Lastly, there has to be collected sufficient data in order to have enough information from the evidence which can be analysed.

All actions performed by the DEFT should be validated prior to use, and every action performed should be documented. The reliability can be strengthened if the action performed is repeatable, and if the same result can be achieved by following the same approach at a later stage.

Digital evidence handling processes

Documented procedures should be followed to ensure the integrity and reliability of the digital evidence are maintained. One principle the procedure should contain is that the DEFR should not take actions beyond their competence. Another principle relates to the handling of the potential digital evidence or original digital device, where this should be reduced to a minimum. This is recommended to reduce the effect handling can have on evidence.

Competency

The DEFR is recommended to have proper and adequate training to handle digital devices in the context of investigative activities. Furthermore, the skills and competency in relation to handling digital evidence should be *demonstrated* and *maintained* to appropriate authorities. The standard says the following about the responsibility related to training and competence: «*it is the responsibility of the individual(s) and the employer to ensure that they are adequately trained and the skills and competence maintained*» (International Organization of Standardization, 2012, p. 13)**.** If this is transferred to the Norwegian Police, having sufficient digital competency to handle digital evidence would be a responsibility both for the individual police office and for the upper management in the police.

DEFR core skills and competency description

In the Annex of the ISO 27037 standard, there is a table with examples of competency descriptions. The competence is divided into three groups; awareness, knowledge and skill-proven experience. *Awareness* is competency to recognise and identify and to ask when help is needed. *Knowledge* is acquired through formal training or working in a team. The DEFR can contribute and participate, and manages to perform actions with help. The last is *Skill-Proven experience*. If a DEFR has this competency they can work unsupervised, and perform tasks without assistance.

TABLE 2. DEFR CORE SKILL AND COMPETENCY DESCRIPTION, EXCERPT BASED FROM TABLE IN ISO 27037

No	Core skills	Core skills description		Competency descriptions	
			Awareness (1)	Knowledge (2)	Skill (3)
1	**Digital evidence identification**	Characterize digital device	Investigative procedures at crime scene	Ability to understand impact on volatile and non-volatile evidence	Identify network diagram and access controls mechanisms to understand dependencies
2	**Digital evidence collection**	Tool requirements and implementation of digital evidence packaging	Determine the best method of collection to preserve maximum information related to the incident	Formulate and execute collection process	Document evidence that cannot be acquired due to various constraints
3	**Digital evidence acquisition**	Apply the requirements of potential digital evidence acquisition in logical form, ensuring repeatability, audibility, reproducible and defensible.	Understand the information available in digital devices	Execute imaging acquisition procedure (e.g. partial and full digital storage media acquisition)	Ability to conduct acquisition of digital storage media including RAID, database, appliances and miniaturized devices
4	**Digital evidence preservation**	Apply and assess requirements for preservation of potential digital evidence	Understand requirements and procedures for maintenance of chain of custody against legal requirements	Know-how on generation of evidence audit documents	Apply measures to secure digital evidence, in the form of large devices to miniaturised hand-held devices
	(1) Awareness:	*Recognise and identify, ask when help needed*			
	(2) Knowledge:	*Formal training, working in team*			
	(3) Skill-proven experience:	*Work unsupervised, apply/ demonstrate, do without help*			

The next chapter relates to competency and learning. The skills and competency descriptions from the ISO 27037 standard in a police investigative context will be discussed further in chapter 4.3.

2.6 Competency and learning

> *«Experience is well and good, but if the course is laid out in the wrong direction, without training, correction, reflection or critical thinking along the way, there is a real danger that experience can fortify misunderstandings so that they eventually appear as truths»*[18]

Rachlew (2009) used the above quote in a critical article about police interviews in Norway. The article was based on his master thesis from 2003. One way the statement from Rachlew can be interpreted, is the need for something more than experience in order to succeed with an interview. Other than experience an academic approach could be beneficial, as this approach will most likely encourage critical thinking. Critical thinking is when you evaluate the accuracy, credibility and worth of information, and it is reflective and evidence-based (Leedy and Ormrod, 2015, p. 35). In simpler terms; by utilising critical thinking you do not blindly

[18] My translation from Norwegian

trust what is presented to you without asking yourself if the information, and the source, is reliable and trustworthy.

There is a need for a system that handles the way digital evidence and digital investigation are taught, as relying on experience without a proper platform are not a successful way to achieve best practice. As mentioned in chapter 2.5.3, using non-validated approaches are not recommended by the ISO standard related to digital evidence. A suggestion for a system will be discussed in chapter 5.

Bloom's Taxonomy of learning objectives

One of the research question this thesis aim to answer is what can be done to further improve the competency level in the Norwegian police when it comes to digital investigation. As mentioned in the previous paragraph there is a need for a system ensuring that digital investigation is not based solely on experience.

Taxonomy is a scientific process of classifying things and arrange them into groups, and learning objectives is what the learner is expected to know and understand after going through a learning process. Benjamin S. Bloom and a group of psychologists created several educational objectives in 1953, where they divided learning into six different levels. The levels were knowledge, comprehension, application, analysis, synthesis and evaluation. Bloom's original Taxonomy scheme were revised by Anderson and Krathwohl in 2001. The revised scheme were less strict, and the levels were changed from nouns to verbs (Gogus, 2012).

The six levels in the revised scheme is illustrated in Figure 7. Gogus (2012) refers to Krathwol (2002) in that the scheme is cumulative hierarchical; in order to climb the pyramid you have to master the level below. Each level is more complex either in skill or ability.

In the illustration the three lowest levels are green, whereas the top three levels are red. This is done purely to illustrate which levels are within the scope for this thesis. The levels remembering and understand is relevant for the survey presented and discussed in chapter 4.1. The three lowest levels must be seen in correlation with the practical test covered in chapter 4.2. All definitions of the terms are made by Anderson and Krathwohl (2001) as presented by Gogus (2012).

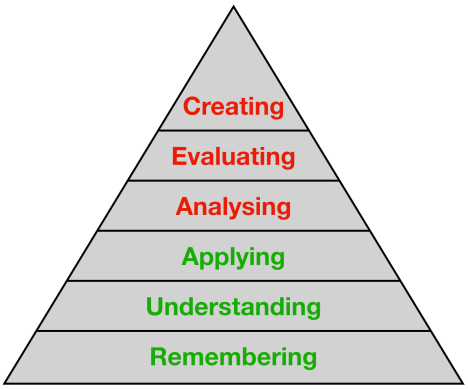


FIGURE 7. BLOOM'S TAXONOMY OF LEARNING, SIX LEVELS

On the bottom in Bloom's revised Taxonomy of learning objectives *remembering* can be found. This is the skill of recognising or recalling relevant knowledge from the long-term memory. An example of remembering can be to recognise digital devices which might contain digital evidence or to describe what an IP-address is.

The next level is *understanding*. This skill can be to demonstrate an understanding of relevant facts. For the readers benefit the examples with the digital device and IP-address will be used again. To master the level of understanding one can be asked to describe what kind of digital evidence can be present on a digital device and to explain how an IP-address works in conjunction with a computer system that uses the Internet.

The last level relevant for this thesis is *applying*. When faced with an actual situation, how is the knowledge *remembering* and *understanding* applied to approach the situation? In order to successfully acquire a digital device which might contain digital evidence one has to recognise the device. It is also necessary to understand what kind of digital evidence can be present. When the device is recognised and it is understood what kind of digital evidence which can be present, the device can be acquired using appropriate techniques and procedures, depending on the type of device and the kind of digital evidence you want to acquire.

3. Methodology

In this chapter the general research methodology used is described. In chapter 3.2 the general research approach is disclosed. The first topic is the overall topics for the survey and the practical test. To better enable the reader to scrutinise the approach, strengths and weaknesses with knowledge in advance are described and discussed. A description of the literature review that has been conducted can also be found in this chapter. The research procedure and data material is discussed in chapter 3.3. Here the sampling procedure, the sample selection, bias and potential error sources in the responses are discussed. The approval process for the survey is described in detail. Quality assurance for the thesis are located in chapter 3.4. Following the quality assurance, is a chapter related to ethical and legal considerations. Finally, errors and weaknesses in the survey and practical test are described before further survey analysis is recommended.

3.1 Introduction

The aim for this thesis is to research how capable the Norwegian Police are when handling digital investigation in the initial phase of an investigation. This research problem can be characterised as a practical approach and not a theoretical conceptualisation. The definition for applied research is that it informs human decision making about practical problems. Action research are applied research projects that addresses questions in the immediate work environment, with the goal of solving an ongoing problem in that environment (Leedy and Ormrod, 2015, p. 45). By using this definition one can argue that it is established that there is a problem with the way the Norwegian Police handles digital investigation in the initial phase. One can also argue that the thesis as a whole is prejudged to come to the conclusion that there in fact *is* a problem with the way the Norwegian Police handles digital investigation. This makes it even more important to be transparent and detailed in the methodology used.

From the basic police education at the Norwegian Police University College, and especially in the post graduate studies within digital forensics investigation courses, the need for notoriety have been inculcated frequently. To deliver a thesis, and a digital forensics report, which can handle thorough scrutiny, the methodology used is imperative. The methodology chapter should contain sufficient information and details so others can replicate the study and, in most

cases, get similar results (Leedy and Ormrod, 2015, p. 350). This principle is similar to the requirements of a digital forensics report.

As a final note in the introduction chapter credit is due to Sunde's master thesis (2017) for giving inspiration in regards to how a methodology chapter can be structured.

3.2 Research methodology

Digital investigation competency in the Norwegian police is a specific and narrow area of research, and to my knowledge there has not been conducted any in-depth research on this field. However, there has been written reports about the field from various authors and organisations. Due to little previous research within the field, written reports were used as a support to get the background of the field in Norway.

When I started planning the thesis I wanted to develop a single product which could be used to test both theoretical and practical knowledge within digital investigation for the first responders in the Norwegian Police. Quite early in the design process it became clear this product would be too time-consuming for the respondents to participate in during regular work hours. Therefore I decided to design a survey that would map the respondents *perceived* knowledge within digital investigation. Initially I abandoned the test of practical knowledge due to the mentioned time constraints. After discussing with my supervisor a new approach was found. Instead of including the practical test in the survey which would be distributed to several hundred employees, a separate practical test was designed and created. This tests purpose was to create a proof of concept for a way to approve investigators who will work with digital evidence and digital investigation.

3.2.1 Research approach

The approach used to partly answer how competent the Norwegian Police are to handle digital evidence and digital investigation, and what could be done to further improve the competence level, was divided into two parts. The first part was a survey where the aim was to research how competent the respondents *perceived* themselves in regards to several topics within digital investigation. The second part was a practical test intended to be a proof of concept for a certification for each investigator who will conduct digital investigation must pass before they are allowed to conduct digital investigation. The practical test could also be relevant as a tool to ensure that other employees, e.g. managers, have a minimum set of skills and knowledge within digital investigation. In this chapter the overall concept and content from the two approaches will be presented.

Survey overall topics and type of questions

In the survey both open and closed questions were used. Closed questions makes a survey easier for the respondent to complete than by using open-ended questions. The use of closed questions makes comparisons between respondents answers easier, as variations outside the predefined answer possibilities will naturally be absent. Open-ended questions can be useful when you want the respondent to answer something that you have *not* thought about, or if you want an elaborate answer. Leedy and Ormrod (2015, p. 167) emphasises that open-ended questions which demand lengthy answers from the respondents should be kept to a minimum. In the survey open-ended questions were mostly used to allow the respondent to provide brief answers which were not from a predefined list. This would not require a huge effort from the average respondent.

Under each topic it is specified what kind of questions were used, and a short explanation of why the question type has been used. A more detailed presentation of the questions asked in the survey and practical test, and discussion of the results, can be found in chapter 4.

Demography
The demography of the respondent was included to be able to do a deeper and more comprehensive analysis. Some of the questions asked made is possible to filter on when the respondents graduated from PHS and what role that described their daily tasks. The questions used were closed. Closed questions would enable easier filtering, and it would assist to achieve a set of answers for the respondents roles that were uniform.

Earlier education within information security
This question was included to see how many police officers that had an earlier education within information security *before* they started at PHS. Those who answered «*Yes*» to this question received an additional open question asking them to name the education(s).

Completed formal education after graduation
To assess how widespread further education within information security or computer forensics investigation was after graduation, the respondents were asked if they had completed such education. The question were closed, with the post graduate studies from PHS as answer options. In addition, the respondents could choose «*Other*» as an alternative. Those who answered this last alternative were asked an open question asking them to name the education(s). The last open question was used to capture responses that fell outside the answer alternatives I had decided to include.

Completed courses or training after graduation
A complete overview of what internal/local courses or training offered in the various police districts can be difficult to get an overview of. However, by including this in the survey it could be possible to get a general overview of what courses/training the police districts provide. The respondents who answered that they had received such training were presented with a closed questions asking them to select from a predefined list of digital investigation topics. The option with selection «*Other*» was also present here, which lead to an open questions asking them to name the courses/training.

Delivery method of training
The respondents were asked what the training or courses included. The respondents had five predefined answer possibilities which described the delivery method of the training/courses. The «*Other*» alternative did not lead to an open question where they could elaborate further.

Social media accounts
The respondents were asked if they had accounts on social media. Those that answered that they had an account got a closed question with a list of predefined social media platforms. The option «*Other*» lead to an open question where they could add social media platforms not mentioned in the predefined list.

Smartphone
To gauge how many police officers who has a smartphone, they were asked if they owned one. They were only able to answer yes or no.

Time used on the Internet
To map how many hours police officers use the Internet, this question asked the respondents to answer how many hours *on average* they spent using the Internet on a daily basis. They could select from a list of four alternatives.

Self-assessment of competency - if a link or an attachment in an e-mail is safe to open
This question was the first question in the survey which asked the respondents to evaluate their own competence. The question had two purposes. The first was to gently introduce the concept of self-assessment to the respondents, and secondly it would be interesting to look further at how they rated their competence. The question type was closed, and they had to choose between an ordinal scale from *Very poor* to *Very good*.

Experience with various technology
Using an ordinal scale from *No experience* to *Very much experience*, the respondents were asked to assess how experienced they were with various technology.

Number of potential digital evidence in the last three criminal cases
To get an indication of the extent of digital evidence in criminal cases, the respondents were asked how many potential digital evidence were present in the last three criminal cases they worked on. Those who answered one or more, were asked to choose which items that were present.

Set of scenarios 1 - Receive a complaint and write a police report
The respondents were presented a varied range of scenarios, where they were asked to assess how competent they were to receive and write police report. The answer alternatives were closed, and used an ordinal scale from *Not competent at all* to *Very competent.*

Set of scenarios 2 - Initial investigative steps
Using the same scenarios as the previous set did, the respondents were asked to assess how competent they were to conduct initial digital investigative steps. The answer alternatives were closed, and used an ordinal scale from *Not competent at all* to *Very competent.* The answer alternative *Will never do, or order, investigative steps*, where also included to account for managers who most likely never will conduct these tasks. In retrospect the last alternative could have been removed, as it would be interesting to survey what level of competence in initial digital investigative steps managers have.

Set of scenarios 3 - Digital evidence handling
In the last set of scenarios, the respondents were presented various digital evidence, e.g. an iPhone 8 with a lock code the owner of the phone willingly provided. The respondents were asked to assess how competent they were to handle the evidence properly. The answer alternatives was closed, and used an ordinal scale from *Not competent at all* to *Very competent*.

Technology and concepts from digital investigation
This question was similar to the earlier question about the respondents experience with various technology. However, this question focused on technology and concepts which could be relevant when conducting a digital investigation. The questions was closed, using an ordinal scale from *No knowledge/skills at all* to *Very much knowledge/skills.*

Assessment of competency when reviewing evidence with commercial tools
Using an ordinal scale from *Not competent at all* to *Very competent*, the respondents were asked to assess how competent they were to review evidence using a predefined set of forensics tools. The alternative *Have never heard of* was also included for those respondents who did not have any knowledge of the forensics tools.

Testimony in court
Testifying in court is perhaps the last thing an investigator does in a criminal case. The respondents were asked if they had testified in court about digital evidence, and those who had were asked to describe how confident they were and if their testimony was questioned by the members of the court. Using an open-ended question, the respondents who had given more than one testimony were asked to briefly describe how they felt when they gave their testimonies. The open-ended question were used to let the respondents describe in their own words how they felt when they testified. A closed question would not be able to include all possible aspects, and was therefore not used.

Crowdsourcing input on the challenges with digital investigation and possible ways of improving the competency level
The last two questions in the survey were open-ended questions asking the respondents to write what they meant were the biggest challenges with digital investigation. They were also asked what could be done to further improve the competency level in digital investigation in the Norwegian Police. The reason for asking these two questions was to receive direct feedback from police officers, that due to work experience are not biased the same way that I am, on how they view challenges with digital investigation. It was also a golden opportunity to receive creative inputs on how the competency level can be further improved.

Practical test overall topics and learning goals
The goal of the practical test was, as mentioned earlier, to be a proof of concept for a certification for employees that would either conduct digital investigation or employees that could benefit from having a minimum set of competency and skills within digital investigation. In this chapter the overall topics and the general learning goals will be presented. The practical test will be discussed in depth in chapter 4.2.

The structure of the test was based on both the digital forensics process model and the process model for investigatio by Andersen, both of whom were presented in chapter 2.5. The first topic is *hypotheses*, which after an incident or event has occurred, is the first phase in Andersens model. The next topic is *identification of digital evidence.* This phase is the next in Andersens model, and the first in the traditional digital forensics process. The final topic in the practical test was *acquisition of data,* which is the subsequent phase of both models. Admittedly, it is within the same phase in Andersen's model, but in this phase acquisition comes naturally after the actual identification. The learning goals are connected to the levels from Bloom’s Taxonomy of learning, presented in chapter 2.6.

Demography
At the very beginning of the practical test, there were questions to survey the demography of the participants. These questions were identical to the questions used in they survey, and was also here included to be able to do a deeper and more comprehensive analysis. Questions were asked to enable filtering on when the respondents graduated from PHS and what role described their daily tasks. The questions used were closed. The last question in the demography section asked the participants if investigating digital evidence was one of their

primary work tasks. This question was included to make it possible to analyse the results from the test based on if the participants primarily worked with investigating digital evidence or not.

Topic 1 - Formulate hypotheses and initial digital investigative steps
The participants were presented three different scenarios with various amount of information, and they were tasked to formulate which hypothesis/hypotheses they could make from the information. In each scenario they were first asked to formulate hypotheses, and then they were asked to explain which initial digital investigative steps they would like to conduct, and why they would conduct them. All questions were open-ended.

Andersen's model starts with an incident or event, and the next phase is formulating of hypotheses. The questions asked in topic 1 provided the participants with an incident or event, and the answers can be used to assess if the participants are able to provide hypotheses. The set limit for numbers of hypotheses were ten. The maximum number of investigative steps were limited to six. The last part of topic 1 was an open-ended question asking the participants what the purpose of hypothesis in an investigation is.

Topic 2 - Identification of digital evidence
In this part of the practical test the participants were first asked a closed question related to the time period it is possible to identify a user of an IP address in Norway. Then they were asked to describe what an IP address is, and why it is important for a police employee to have knowledge about this. The first question could be used to assess the *remembering* level in Bloom's Taxonomy, while the second could be used to assess the *understanding* level. An assessment of the *understanding* level could also be used for the next question. Here the participants were presented a list of items, and they were tasked to select the items they thought might contain potential digital items.

In the last question in topic 2, the participants were presented with a scenario that contained limited information. They were then asked to identify what potential digital evidence could be present, and what information could be extracted from the digital evidence. The identification part of the question could be used to assess the participants skills and knowledge to the *remembering* level in Bloom's Taxonomy, while the second part of the question could be used to assess the the next level, namely *understanding.* The participants could provide up to six different digital evidence and the corresponding potential information.

Topic 3 - Acquisition of digital evidence
The last topic the participants were tested in was acquisition of digital evidence. The main content of this topic required the participants to conduct actual acquisition of various social media accounts which had been created in advance. The purpose of these exercises was to assess the *application* level in Bloom's Taxonomy. They were also asked theoretical questions to assess the level of skills and knowledge for both the *remembering* and *understanding* level.

In the first part of this topic, the participants were asked open-ended questions about various topics within digital investigation. They were asked to name acquisition methods of data from the Internet which could be accessed through a web browser. Furthermore, they were tasked to describe what Order of Volatility[19] is when it comes to digital evidence. Lastly, they were asked to list pros and cons with activating flight mode on a phone after is is seized, and pros and cons with doing live forensics on a computer. All these questions were open-ended.

[19] The prioritization of the potential evidence source to be collected according to the volatility of the data

The next part of this topic was related to practical handling of digital evidence. Presented with five different types of digital evidence, e.g. an Apple iPhone X with a known lock code, they were asked in what order they would handle the evidence. They could choose from a predefined list of alternatives, where there were added some alternatives that are not forensically correct. After each evidence, there was an open-ended question asking the respondents why they chose to handle the evidence in the order they did.

After being provided with a username and password to three different social media accounts, namely Gmail, Facebook and Instagram, the participants were asked to acquire them using a defined method. When several people across the country try to access an online account, there might be security measures in place from the content provider preventing access to the account. To give the participants a real opportunity to complete the test even if they experienced problems with accessing the account due to above-mentioned security measures, a Word-document containing already acquired content was attached to the question. The participants were asked if they managed to download the content. They could answer yes and not, but they could also answer that they encountered technical difficulties, and that the content from the Word-document was used. Using a practical approach, the participants skills on the *application* level could be assessed.

Those who answered that they managed to acquire the content, or who had encountered technical difficulties, were asked theoretical questions only answerable by examining the acquired content. Examination, or exploring data, is somewhat outside the scope for this thesis, but was still added to the practical test as it can be a natural next step of competency after the content has been acquired. As the practical test was intended to be a proof of concept of digital competency certification, it was unnatural to omit the examination part.

To assess what method the participants would acquire a video from YouTube, they were provided with an URL to a video and then asked to explain how they would acquire this video. In the next question they were asked to explain how they would acquire a forum post from a given forum thread. The answers could be used to assess the *application* level of their skills and knowledge.

The participants were presented with a picture containing *Exchangeable image file format data* (EXIF-data). Using open-ended questions they were asked to answer what two specific EXIF-data fields contained in the image. Lastly, they were asked which tool/method they used. The answers could be used to assess the *application* level of their skills and knowledge.

Using a provided e-mail address, the participants were asked to describe which step(s) they could perform to find out who the owner of the e-mail address was. This was an open-ended question. Regardless of what they answered, the next question gave a prerequisite where they had sent a request to the content provider asking for basic subscriber information. The content provider returned an IP address belonging to an ISP. The participants were asked an open-ended question about what they would do next. Again, regardless of what they answered they were given a prerequisite where the ISP returned a name and address of the person who had the IP address at the time. They were also informed that there lived several people at the address. The participants were asked an open-ended question about what assessment(s) they should make before they suspected and arrested the person who had the IP address. The intention of these questions was to assess how the participants approached a situation, and how they evaluated the information they were given.

The last question was an open-ended question asking the participants to give inputs or suggestions for improving the practical task.

3.2.2 Strength and weaknesses with knowledge in advance

Experienced-based knowledge or knowledge in advance, and the effects it can have, both positive and negative, is a recurring theme in scientific research. When conducting research on your own profession you have prior knowledge about the structure, culture and language. This is timesaving, as you do not need to spend time to learn how the profession works. However, knowledge in advance can lead to a closed mindset where your prior knowledge might be so extensive it stops new and unexpected knowledge (Sunde, 2017, referring to Rachlew 2010). For me the experience-based knowledge was positive since it was crucial to identify digital competency amongst police officers was a topic which I wanted to address. It was also effecting my mindset negatively, as I falsely assumed that *every* police officer would come across acquisition of social media as part of their job.

Grøtan (2019) reflects on how her knowledge in advanced effected how she designed her interview guide with questions based on what she expected to find out. The same is relevant for the way my survey was designed. On one side my knowledge about digital investigation might enable me to create scenarios which are relevant from a digital forensics investigator perspective. On the other it can limit, or even miss, what scenarios are relevant for a regular police officer in their daily job.

3.2.3 Literature review

The work with the master thesis started in autumn 2018, and the research problem in general was clear even before the fall semester started. From the very beginning I knew I wanted to approach the research problem with a survey. Due to a well known long processing time for approval to conduct a survey, the actual design of the survey was one of the first priorities. This was done because the survey questions, and design, had to be finalised before the applications were sent. The different topics in the survey were designed based on my experience with regular police officers' knowledge about digital investigation, and what challenges I had experienced they faced on a regular basis. I knew there had been revisions in the curriculum from PHS regarding digital investigation. The students graduating in 2011 or earlier had another curriculum than the students graduating in 2012, and there had also been an additional revision for the students graduating from 2017.

After the survey was complete, and while waiting for approval for the applications, I began with the literature review. One of the research questions was in regards to the history of digital investigation in Norway. To answer this question several official reports were found online, and some reports were kindly presented by colleagues from the digital investigation field. One pitfall with relying solely on official reports is that they might be influenced by political forces and not necessarily show the true picture. My aforementioned experience within the digital forensics field, and personal knowledge with some of the authors from the report, could to a degree help understand if the official reports were lacking vital information or if they presented a realistic view of the status.

Another research question seeked to answer if there are any requirements for completing digital investigation. In order to find out this official reports from POD were used. The findings in those reports were scrutinised to see if they concurred with my experience.

The main purpose of the survey was to research how competent an investigator feel when they are faced with digital evidence during an investigation. Another purpose was to see what can be done to further improve the competence level regardless of what the actual level of competence turned out to be. This made it necessary to research what competence is and how a theoretical framework can be applied to ensure that the learning is not only experience-based. This lead to research into Bloom's Taxonomy of learning, and the development of a practical test. With perceived competency, the Dunning-Kruger effect also became relevant to research. The Dunning-Kruger effect is further discussed in section 3.3.

What kind of digital investigation knowledge, both past and future, graduates from the PHS are taught were researched using curriculum from PHS.

3.3 Research procedure and data material

Status of employees in Computer Crime Units
To find out how many employees that work full-time as digital forensics investigators, I reached out to the leaders of the various Computer Crime Unit via e-mail 25th of October 2018. They were informed of the research project, and asked to provide information about how many employees they had in their unit. They were also asked the ratio of civilian/police background for their employees, how long the employees had worked within the field and what kind of formal competency the employees had. The request sent out should be viewed upon as informal, as I have personally met all the leaders in earlier contexts. The e-mail sent out can be found in the Appendix. Note that the recipients have been redacted for privacy.

3.3.1 Survey, research procedure and data material

In this chapter the sampling procedure and sample selection for the survey will be presented. Bias and potential error sources will be discussed, and the approval process is described in detail. The delivery method for the survey is also presented. An English version of the survey can be found in the Appendix. The respondents were presented with a Norwegian version, but the design were otherwise identical.

Sampling procedure
A descriptive survey can be used to gather information about one, or several, group of people's previous experiences or attitudes. When using a descriptive survey your goal is to learn about a large population by surveying a *sample* of the large population (Leedy and Ormrod, 2015, p. 159).

The survey was initially meant to be distributed to every police employee in Norway, but after dialogue with POD it became clear this would be too much workload for the police. The original idea behind sending out the survey to every police employee was to increase the odds to ensure the response rate would be high enough that the responses could be used to generalise the digital competency level in the Norwegian police. The number of police employees in Norway is over 9000 (Politiet.no, 2019), and in order to get a representative sample I would need 400 respondents (Leedy and Ormrod, 2015, p. 184). Another aspect by receiving responses from each police district, was to find potential differences in competency due to local training. In retrospect it was wise the original idea was not pursued further, as it is unknown if each police district is actually autonomous enough that generalisation across police districts would lead to skewed and wrong results.

The survey was tested as a pilot on colleagues, and the feedback was used to improve the wording on the questions before it was finalised. This was done to reduce confusion among the respondents due to badly written formulations. The colleagues were selected based on what role they had, including patrol officers, both specialised and non-specialised investigators and one manager. The program used to deliver the survey was Questback[20], licenced through NTNU.

Sample selection

The police districts Øst, Trøndelag and Møre og Romsdal were chosen primarily due to their size. Øst is one of the largest police districts in Norway when it comes to number of employees, whereas Trøndelag is a medium sized and Møre og Romsdal is a small district (Politiet.no, 2019). The districts were not selected randomly, even though the number of employees were the main focus when selecting which district would be part of the survey.

Øst police district was chosen both because of its size, but also because it is the police district where I used to work. This might have influenced the number of responses from people who, because of their earlier acquaintance with me, were motivated to answer to survey in order to help me. While I worked at Øst police district I primarily worked with digital investigation, and those who might answer due to earlier acquaintance with me would most likely be colleagues I have met when working with digital investigation. This can lead to a skewed result from Øst police district, if people that are more familiar with digital investigation answer because they want to help me opposed to people with less digital investigation skills that does not know me.

The fact I actively chose which districts which should be a part of the survey removed the possibility of a randomly selected sample population, and it can not be argued that probability sampling was used. The sample used for the survey can be defined as a combination of convenience sampling and purposive sampling, both subsets of a non-probability sampling. By using the approach of selecting three police districts, the employees in the remaining nine police districts had no chance of being selected. Three police districts were within the boundaries of what was allowed by POD, and in order to follow through with a survey it was convenient to use the population sample that was available. Because the police districts chosen were chosen due to their size, there was a purpose in selecting them. The purpose was to have at least three police districts with various size represented in the sample.

Bias and potential error sources in the responses

There are several factors that will influence the responses from an online survey. Leedy and Ormrod (2015, p. 176) points out that people answering online surveys are those comfortable with computers and people who enjoy participating in research studies. They also show an interest in the actual topic you are researching in order to spend time answering the survey. All in all, the answers will already be biased even before the researcher adds their own biases.

To my knowledge, every police employee has access to ICT and e-mail, and surveys are sent out to police employees at irregular intervals. What might influence who answers the survey and not is how interested the police officers are to participate in research studies. If they are interested in research studies, it might also be relevant if they are interested in a study that concerns digital investigation.

[20] https://www.questback.com

A potential error source with a survey based on the respondents *perceived* competency within digital investigation, is the Dunning-Kruger effect. When asked to self-evaluate how competent people are, people with low competency, *low information individuals*, tend to overrate their skill and expertise (Schlösser et al., 2013). If the results from the survey show that the majority of police officers perceive themselves as highly competent when met with a certain challenge, the actual competency level might be lower due to the Dunning-Kruger effect if the majority of the respondents belong to the group of low information individuals.

Another potential error source is that the respondents *know* they are part of a research project, and thus answer differently than what they would have done if their answers were not scrutinised by a researcher. This is known as the Hawthorne effect (Leedy and Ormrod, 2015, p. 104).

Two respondents stated procecutor to be their primary role. It is unclear if these two have a police education in addition to an education within law. The answers from these two has been included in the results from the survey.

When reviewing and analysing the results from the survey it is imperative to take into account both the starting biases from the dataset mentioned above, as well as the possibility that the Dunning-Kruger effect has affected how the respondents have responded to the survey.

The approval process broken down in dates

The process of getting approval to conduct the survey turned out be tedious affair, and the approval process took far longer than what I have planned for. In order to show the process to gain the actual approval each step along the way is described below. The final letter of exemption can be found in the Appendix.

2018

28th of November

A request to send out the survey, and thus gather data from the Norwegian Police, was sent to POD

3rd of December

Answer from POD with information about what an application must contain.

10th of December

An application with the requested information sent to POD. In the request the scope for the survey was every police employee in Norway.

2019

11th of January

Answer from POD. Relevant respondents have to be identified, and the total number of respondents have to be significantly reduced.

12th of January

Updated application sent to POD. The respondents have been identified to only police employees, both patrol officers and investigators and also leaders. The number of respondents have been reduced to police employees in Øst, Trøndelag and Møre og Romsdal police district.

25th of February
An e-mail sent to the caseworker in charge of the application in POD to find out the status of the application. No answer received.

9th of April
The caseworker is reached by phone, and after explaining that the deadline for the master thesis is 1. June 2019 she informs me she will look at the application the next day.

10th of April
The caseworker called and required a formal statement from someone with formal responsibility within digital investigation regarding the content of the questions in the survey. This was forwarded to Thomas Stærk at NC3, and the formal statement was sent to the caseworker the next day.

24th of april
Letter of exemption, and approval to conduct the survey, received from POD. The letter is dated 11th of April 2019, but was not sent via e-mail until 24th of April. It is highlighted in the letter that a permission from the respective Police Chiefs is needed before the survey is sent out. There were no practical guidelines for how the link to the survey could be sent out.

25th of april
An e-mail is composed to the Police Chiefs in Øst, Trøndelag and Møre og Romsdal with information about the project. In the e-mail permission is asked to send out the e-mail. The Police Chief in Øst and Trøndelag answered by e-mail, and the Police Chief in Møre og Romsdal gave his consent by phone in the evening. The Police Chief in Trøndelag and Møre og Romsdal consented to me sending out the information letter and link directly to their employees. This was done the same day. The e-mail was sent from my work e-mail, and directed to a mail list that would reach every employee in the police districts. In Øst the Police Chief, through his staff, asked me if it were acceptable that they published the information letter and link to the survey on their Intranet instead of sending out an e-mail to every e-mail. They would also inform their leaders about the survey. I consented to this, and underlined the importance of making the letter of exemption from POD available for the respondents together with the information letter about the survey.

29th of april
Øst police district published an article on their Intranet with information about the survey.

3.3.2 Practical test, research procedure and data material

In this chapter the design process and content for the practical test will be presented. The sampling procedure and sample selection, as well as potential error sources in the responses will be covered. An English version of the practical test can be found in the Appendix. The participants were presented with a Norwegian version, but the design were otherwise identical.

The design process and content
The purpose with the practical test was to create a proof of concept for a way to approve investigators who will work with digital evidence and digital investigation, as mentioned in chapter 3.2. It was originally created based on practical challenges which I had experienced investigators struggling with on a nearly daily basis. During the design process I reviewed a recent exam from PHS with assessment guidelines. The exam was kindly provided by Police

Superintendent Robert Furuhaug from PHS. Furuhaug also gave me feedback when the test was almost complete, and suggested EXIF-data to be included as one assignment in the practical test. EXIF-data was knowledge the bachelor students at PHS had as part of their curriculum, and therefore it would be wise to add this.

After a meeting with Stig Andersen, where he presented his process model for investigation, shown in chapter 2.5.2, I realised hypotheses should have a natural part of the practical test. Assignments containing hypotheses were then added to the practical test.

Sampling procedure and sample selection
The practical test was rather time-consuming, and as the main purpose of the test was to be a proof of concept for a certification test it was tested on a small group of people. The people asked to take the practical test were people I knew to be proficient in digital investigation and proficient to handle digital evidence. Two colleagues that I knew *not* to be proficient in digital investigation were also kindly asked to take the test to see how they managed to solve the tasks.

The people invited to take the test were informed about the research project as a whole, and it was emphasised that participation were voluntarily and that they would remain anonymous. When the e-mail was sent the recipients were added to blind carbon copy (BCC) on the e-mail. In the Appendix the invitation e-mail can be found.

Out of nine people asked to take the survey, six took the test.

Potential error sources in the responses
With a rather comprehensive, voluntarily test online there might be possible that the respondents answer less than they actually know because they want to finish the test. There is also no option for the respondents to ask questions if they are unsure of what is asked of them in the assignments, which can cause misunderstandings and possible errors in the answers. Ideally I should have been nearby the respondents when they took the test. This way I could have guided them and cleared up any misunderstandings.

No questions in the survey were mandatory, and it was not possible for the respondents to go back to a previous question if they either forgot to answer, or if they wanted to make changes. This might have led to blank answers. It might also have led to respondents answering wrong with no possibility to go back and correct their first answer.

3.4 Quality assurance

Validity
Research data should be accurate and credible, and it should aim to address the research problem. Validity can be divided into internal validity and external validity. A degree of internal validity can be achieved when the researcher take precautions, and are aware, of various *other* explanations for the results that are observed. External validation will say to what degree the results can be used in other contexts, and if the results can be used for generalisation (Leedy and Ormrod, 2015, pp. 103-104).

Survey validity
To improve the internal validity for survey awareness of both the Dunning-Kruger and Hawthorne effect was imperative. This might influence the responses by the respondents self-

evaluating themselves as more competent when they in reality had low competence. The Hawthorne effect might cause them to answer what they thought I wanted them to answer. My background, and knowledge in advance, both of whom will lead to predetermined bias, are presented in the thesis. Openness about my background and knowledge in advance will help the readers to measure those biases. The sample procedure is also described in detail, making it verifiable.

The English version of the survey is made available in the Appendix. The answers from the survey has been included in the thesis as tables. This will assist the readers, and others, to assess the validity of the results which has been drawn from the questions.

Practical test validity
The practical test, with both design and results, is presented in the same way as the survey, and the mechanisms to improve the validity are the same. Openness about the methodology is essential for the validity measurement.

Reliability
When a measurement method or approach returns a consistent result each time it is tested on the same material, the method is reliable (Leedy and Ormrod, 2015, p. 116).

Even though the actual results from the survey and the practical test will vary based on the respondents, the method for collecting the data will be the same regardless of who takes it and when. The reliability for the method is consistent.

Generalisability
External validity is the extent you are able to use your findings to draw generalisations to other contexts. One key factor for enhancing the external validity is a representative sample. If a valid representative sample is used, it can be possible to draw conclusions for a population as a whole (Leedy and Ormrod, 2015, p. 105).

In the sample population used for the survey and the practical test there are several factors that do not substantiate external validity to a degree that the findings can be used to generalise.

- The sample selection for the survey was limited to three police districts. There might be substantial differences in the various police districts when it comes to digital investigation and training, and the sample selection might not be representative for the other police districts.
- There has been collected too few responses to the survey to be able to generalise for a population that is over 5000.
- The practical test has only been completed by six police employees. It should be noted it never was the intention that the results from the practical test would be used to generalise.

However, the results from the survey can be used as an *indication* on the status of competency in digital investigation in the Norwegian police. The practical test can be used as a *starting point* for further development of a certification within digital investigation.

3.5 Ethical and legal considerations

As a police officer, ethical and legal considerations and restraints are incorporated in my daily tasks. Following ethical and legal regulations and guidelines with the research project was therefore important.

When the survey was designed, it was taken into account that the respondents answer would be voluntarily and how their privacy would be respected. Leedy and Ormrod (2015, p. 121) also highlights protecting participants in a research project from harm. Furthermore, giving credit to other people's work when used was also emphasised. Whilst this thesis was written a large effort was done to properly cite other people's work where it was appropriate.

An application was sent to the Norwegian Centre for Research Data (NSD) to receive approval for the survey before it was sent out. This was required because the way the survey was delivered, even though it did not require name or other personal identifiers from the respondents, led to a theoretical chance that the respondents could be traced through their IP address. The approval from NSD can be found in the Appendix.

Due to the research project would research Norwegian police officers, an application was sent to POD to gain permission to conduct a survey. Gaining access to data from the police is regulated by the Police Register Act (Politiregisterloven, 2010). Among the requirements set by POD was that the exemption letter must be made available to the respondents and that each police chief gave their permission to conduct the survey in their police district. Another requirement was the need for a pre-approval from The National Criminal Investigation Service (NCIS) related to the questions and results from the survey. The person selected for approving the results from the survey was Thomas Stærk, who is the assistant director for the National Cybercrime Centre (NC3) at NCIS. The information could contain data that could reveal the police's total capacity in digital investigation, which again could lead to damage to the police if the information got publicly known. The results from the thesis was discussed with Thomas Stærk before the thesis was submitted. The application process is described in detail in chapter 3.3.1, and the exemption letter permitting the survey can be found in the Appendix.

3.6 Errors and weaknesses, survey and practical test

Survey

Tuesday 30th of April 2019 I was contacted by one respondent from Øst police district. He informed me of a flaw in the question where the respondent could select what kind of digital evidence they have encountered in the last cases they worked. There was only possible to choose *one* digital evidence from the given list, while the intention behind the question was to allow the respondents to choose more than one item. At that time over 60 respondents had answered to survey, and I judged it to be unwise to change the answering possibilities after so many responses. When analysing the results from the survey it was taken into consideration that the answers from this question would not yield an accurate answer.

There was also found an inconsistency in the survey when the data was analysed. In the survey there were different scenarios where the respondents were asked to assess their own competency. The same scenario were used twice. First, it was used to cover the aspect of receiving and writing a police report, and secondly it was used to perform initial investigative steps. In the different phases the respondents did not have the exact same answering possibilities. When analysing the results, I found the answering alternative *Somewhat*

competent should have been present when the respondents were asked to perform investigative steps. Instead, this had been replaced with the answer *Will never do, or order, investigative steps*.

Recieve and write report	Perform investigative steps
Not competent at all	Not competent at all
Very little competent	Very little competent
Little competent	Little competent
Somewhat competent	Competent
Competent	Very competent
Very competent	Will never do, or order, investigative steps

Practical test
In the question where the participant are asked how long it is possible to identify a user of an IP address, it was possible to select more than one answer. This was an error made when designing the test, and was not detected until analysis of the practical test was conducted. The intention was to only have one possible answer. The very first question in topic 2, where the participants are asked what the purpose of hypothesis thinking in an investigation is, should have been placed as the last question in topic 1. This is only a cosmetic error, but nevertheless an error in the design.

3.7 Recommended survey analysis

As mentioned earlier the survey was published in the end of April, and the thesis was due 1st of June. A deep analysis of the results from the survey was therefore not possible to achieve within the available time frame. The answers from the survey could be correlated with factors like age, what year the respondents graduated and their primary job role. The answers from the survey could e.g. be analysed to see if police officers perceive their own competency differently based on when they graduated from PHS, and by what curriculum they had.

4. Experimental results and discussion

In this chapter the result from the survey and the practical test will be presented. For the ease of the reader, the questions the respondents from the survey and the participants from the practical test received will be repeated before the results is presented. The interpretation, and discussion, will follow right after the results. The general results and the implications is discussed in chapter 5.

4.1 Survey

In this section the results from the survey will be presented. Due to time restraints, the results have not been cross-matched in a deep analysis with e.g. time graduated and perceived knowledge. However, a deeper analysis is recommended to be done in further research.

4.1.1 Experimental design

The survey was designed to cover several areas related to digital investigation. The first area was related to the level of education within digital investigation. How familiar the respondents were with social media platforms and concepts from digital investigation was another area the survey aimed to cover. Lastly, it was a concrete motivation to map how competent the respondents *perceived* themselves when faced with the initial phase of a digital investigation.

Timeframe for the start and end of collecting data

The survey was sent out to Trøndelag and Møre og Romsdal police district on Thursday 25th of April 2019 using e-mail. Øst police district published the survey on their Intranet on Monday 29th of April 2019.

The cut-off for responses, and download of data from survey, was done 6th of May 2019. This was done to have time to analyse the data and discuss the findings. There were totally 99 responses on the survey when the cut-off was done. After the cut-off additionally eight responses came, but they were not included in the analysis.

4.1.2 Material critics - data

The results from the survey can, and will, **not** be used to generalise for the Norwegian police force as a whole, as discussed in chapter 3.4. It could, as pointed out, be used as an *indication* on the status of digital investigation competency among Norwegian police employees.

4.1.3 Results

When data from the survey was downloaded, a total of 99 respondents had answered the survey.

General info about the respondents answers

The survey was distributed to about 2200 police educated employees. There were 99 respondents who answered the first question. On the final question which was asked everyone, there were 97 respondents. The response rate was low, about 4,5%. The response rate could have been improved by sending out a gentle reminder two weeks after the initial distribution of the survey. However, due to time limitations that occurred due to the late approval from POD, it was not possible to achieve this and still have time to analyse the results before the thesis was due for hand in on June 1st.

Demography

The first eight questions were related to the demography of the respondents. The respondents current role was included to see if there were any differences in perceived competency level amongst different roles. When the survey was originally created, prosecutors and employees without a police education were included. When the scope changed to only police employees and their competence, eventual results from prosecutors and non-police employees would be overlooked. The respondents were asked when they graduated from the Norwegian Police University College. This was done to be able to correlate their answers with what the curriculum from PHS were at the time they graduated. As mentioned above, there was no time to do this correlation.

The majority of the respondents (59,6%) graduated in 2011 or before. 26 respondents (26,3%) graduated between 2012-2016, and the rest (11,1%) graduated in 2017 or later. Three respondents (3%) answered that they have not graduated from PHS.

Almost half of the respondents (47,9%) answered that they have been employed ten years or more in the Norwegian Police.

Trøndelag was the police district with the highest response rate (41,8%), and Øst police district had the second largest response rate (32,7%).

The respondents roles were spread across all roles, except *civilian duty*. This was as intended, as the information letter stated that the target respondents for the survey were employees with a police education. As mentioned in chapter 3.3.1, two respondents stated that their main role was prosecutor. It is unclear if these two have a police background. Their answers have been included in the results.

TABLE 3. COMPOSITION OF ROLES AMONG RESPONDENTS IN SURVEY

Role	Count	Percent
Investigator, general investigation	15	15.2%
Investigator, specialised investigation	28	28.3%
Crime prevention	8	8.1%
Computer forensics investigator	6	6.1%
Patrol	24	24.2%
Management	13	13.1%
Operations center	3	3.0%
Prosecutor	2	2.0%
Civilian duty	0	0.0%
N	99	

Earlier education within information security

The respondents were asked if they had any earlier education within information security before they started at PHS. This was asked to see how frequent a police officer has an education within information security before s/he decides to become a police officer.
Information technology was defined as «*the use of computers to store, retrieve, transmit, manipulate and present data and information*».

Discussion

Only 3% of the respondents had any earlier education within Information Technology before they started at PHS. This indicates that completed education within Information Technology before starting at PHS is *not* common among police officers.

Completed formal education within information security or computer forensics investigation after graduating from PHS

As presented in chapter 2.3.2, PHS has ten post graduate studies within digital investigation. This question seeked to find out how many of the respondents had completed a formal education, and on what level. Formal education was defined as «*attendance at a college or university that leads to credits*».

15 respondents (15,2%) have completed a formal education within information security or computer forensics investigation after they graduated from PHS. Of those 15 respondents, eight (53,3%) have completed the now obsolete *«Nordic Computer Forensics Investigator: Module 1»* that gave five credits. This module was web-based, and served as an entry point to the old *«NCFI Module 2»* which gave 25 credits. Two respondents have completed the old *«NCFI Module 2»*, and four have completed the new *«NCFI: Core module»* that gives 15 credits.

Six respondents answered that they have completed *other* formal educations. Two of those free text responses indicate that the educations falls outside the definition of formal education, that were «*attendance at a college or university that leads to credits*». Among the other formal educations is legacy educations within computer forensics investigation from 1996 to 1998, and legacy educations in digital evidence from 2004 to 2009.

Discussion
Based on the respondents answer 15,2% have completed a formal education within information security or computer forensics investigation after graduation from PHS. Around half of those respondents have only completed a NCFI module that gave five credits. If this number would be representative for the Norwegian Police as a whole, the number of police employees who have completed a education with minimum five credits would equal around 700 police officers, whereas the total number of police officers who have completed a formal education within information security or computer forensics investigation would be around 1400 police officers.

Completed courses or training within digital investigation after graduating from PHS
From my experience within digital investigation, internal training and workshops are frequently used to transfer knowledge from one officer to another. This question's goal was to establish how many of the respondents have received internal training or workshops, and what kind of training they have participated in. A follow-up question about how the training and course were conducted was asked. The purpose was to see if the training was organised, and to see how widespread informal training provided by a colleague was.

The number of respondents who have completed courses or training within digital investigation was 40. Of those 15 respondents who had completed a formal education after they graduated from PHS, 11 (73,3%) have also completed courses or training within digital investigation.

Of other training and courses, some respondents answered OÅO spring 2019. OÅO is an abbreviation for «*Obligatorisk Årlig Opplæring*», and is a compulsory annual training for every investigator in the Norwegian police. It is described as a first step towards a defined minimum standard (Politidirektoratet, 2016, p. 25). The course material for digital evidence in OÅO spring 2019 is web-based, and it is estimated that each participant will use two hours to complete. The actual course material is not publicly available, and can contain information which should not be distributed to the public. It will therefore not be presented further in this thesis.

Of the 40 respondents who answered they had attended training or courses after graduation from PHS, 38 respondents answered the question related to which delivery method was used. 20 respondents (52.6%) have attended one or more training sessions or courses where the delivery method was informal training with a colleague. The practical approach with learning by doing was used for 14 respondents (36,8%) in one or more training sessions or courses. It is

important to notice that the respondents could choose more than one option, as one person can have attended more than one course or training where the delivery method varied.

Discussion

Around four of ten respondents (39,6%) have attended training or courses in digital investigation after graduation from PHS. Informal training with a colleague has been the delivery method in one or more of the training sessions for half the respondents. Only a practical approach has also been used on several occasions. The most used delivery method is however a combination of theoretical lesson(s) with a practical approach.

TABLE 4. COURSES OR TRAINING AFTER GRADUATING FROM PHS

Name	Count	Percent
Acquisition of mobile units using XRY products (from MSAB)	21	52.5%
Acquisition of mobile units using Cellebrite products	13	32.5%
Acquisition of hard drives from computers using write-blocker and software like FTK Imager	12	30.0%
Professional contact for digital police work (Norwegian: fagkontakt)	9	22.5%
Open Source Intelligence (OSINT)	25	62.5%
Social media acquisition, e.g. «My Archive» from Facebook	20	50.0%
Review of evidence using Griffeye	15	37.5%
Review of evidence using Internet Evidence Finder/Axiom	16	40.0%
Review of evidence using Cellebrite Reader/Cellebrite Physical Analyser	15	37.5%
Other	20	50.0%
N	40	

TABLE 5. WHAT THE TRAINING INCLUDED

Name	Count	Percent
Only practical approach (learning by doing)	14	36.8%
Informal practical training* with a colleague	20	52.6%
Only theoretical lesson(s)*	6	15.8%
Combined theoretical lesson(s)* with a practical approach	24	63.2%
Other	2	5.3%
N	38	

** All training and courses are internal, i.e. local training in the police district, not provided by the Norwegian Police University College*

Social media accounts

Familiarity to a concept or a product can make it easier to learn new aspects of the concept or product. I have met police officers who does not have a Facebook account, thus making it

somewhat more difficult to guide them through an acquisition of said platform. Those without Facebook accounts were not necessarily familiar with the jargon used or how to navigate a Facebook account. The idea behind the question about which social media account(s) the respondents have was to see how many of the respondents have social media accounts. Those numbers could again be used to assess how familiar one can expect an average police officer is with different social media platforms.

Of the 96 respondents who answered this question over 90% answered they had an account on Facebook, Facebook Messenger and Snapchat. Seven of ten (70,8%) had a Google account, and at least seven of ten (76%) had an Instagram account. The more communication based platforms had fewer users. 29 of the respondents (30,2%) had an account on Telegram, and 19 (19,8%) had an account on Signal.

Discussion
Based on the answers from the respondents, it can be argued that the majority are familiar with the social media platforms Facebook, Messenger and Snapchat. Around three of four are also familiar with Google and Instagram. This means the majority have the possibility to acquire their own accounts for testing purposes, and after acquisition review content which they are familiar with. The answers also indicate the use of communication platforms like Signal and Discord are not as widespread among police officers as the social media platforms, even though several respondents report they have an account on various communication platforms.

TABLE 6. WHAT SOCIAL MEDIA ACCOUNTS THE RESPONDENTS HAD

Name	Count	Percent
Facebook	89	92.7%
Facebook Messenger	88	91.7%
Google	68	70.8%
WhatsApp	40	41.7%
Instagram	73	76.0%
Twitter	40	41.7%
Telegram	29	30.2%
Discord	15	15.6%
Signal	19	19.8%
Snapchat	91	94.8%
Other	9	9.4%
N	96	

Smartphone or not

The same idea behind this question as for the question with social media accounts. If the majority of police officer owns a smartphone, can those numbers be used to assess what can be required of an average police officer?

Discussion
Almost every respondent (98%) answered they have a smart phone. This high number indicates most police officers have a smart phone, and it can therefore be expected they are familiar with basic usage concepts like turning the device on and off, enabling flight mode, entering pass code and navigating the menu on the device. It should be mentioned there are

rather large variations between different operating systems, for example Android and iOS, and this might complicate the familiarity with the basic usage on an operating system which is not frequently used.

Time used on Internet

Frequent use of the Internet for social media, reading newspapers, gaming and online shopping can indicate how comfortable the respondents are with using Internet and services online.

None of the respondents answered zero hours on average for online activities. 64 of 99 respondents (64,6%) uses one to two hours per day on average for online activities, while 31 (31,3%) use three to four hours. Only 4% answered that they use five or more hours online on average.

Discussion

All respondents use at least one hour per day on average for online activities. This can indicate a certain degree of familiarity with using the Internet.

Self-assessment of competency to determine if a link or an attachment in an e-mail is safe to open or not

Inspired by an online test where you can see how good you are at determining if a link or an attachment in an e-mail is legitimate or not[21], the respondents were asked how skilled they rated themselves to determine if a link or an attachment is safe to open or not.

The majority (69,7%) rated their own competency to be either good or very good, while five of 99 rated their competence to be poor or very poor.

Discussion

95% of the respondents assessed their competency to determine if a link or an attachment in an e-mail is safe to open or not to be fair or better. Only 5% assessed their competence to be poor or very poor. A report from the US communication company Verizon (2019) found that 30% of phishing messages gets opened by targeted users, internal threat actors, in the public sector, and 12% of those users click on the malicious attachment or link and thereby compromise their credentials. If the numbers from Verizon's report are correct and representative, the answers from the respondents in the survey can indicate they are either more competent than the average, or that they assess their competency to be higher than it actually is. I would argue that evaluating if a link or an attachment in an e-mail is safe to open or not can be difficult. It is recommend that you access the test mentioned above, and test your own skills when faced with different potential fraudulent e-mails.

TABLE 7. SELF-ASSESSMENT ON COMPETENCY TO DETERMINE IF A LINK OR AN ATTACHMENT IS SAFE

Name	Count	Percent
Very poor	2	2.0%
Poor	3	3.0%
Fair	25	25.3%
Good	50	50.5%
Very good	19	19.2%
N	99	

[21] https://phishingquiz.withgoogle.com

Experience with digital concepts

This topic relates to how much experience the respondents have with digital concepts like using both Norwegian and International online market places, digital currency, IP-telephony, application-based communication, creation of new e-mail addresses and Peer-to-peer (P2P) technology. All of these concepts *can* be present in a regular criminal case, and the purpose of the question is to find out how versed the respondents are with the different concepts.

Discussion

For each concept the answer alternative which received the most answers are highlighted with a colour. The alternatives marked with red can indicate major deficiencies in the experience with the concept, while the alternatives marked with green can indicate sufficient experience. It is important to emphasise that the answers are based on the respondents *perceived* experience, and therefore should only be used as an indication.

Colour scheme	Indications
No experience	Major deficiencies in experience
Very little experience	Major deficiencies in experience
Little experience	Deficiency in experience
Some experience	Deficiency in experience
Much experience	Sufficient experience
Very much experience	Sufficient experience

One concept which stood out with low self-assessed experience was digital currency. 86 of 99 (86,9%) of the respondents answered that they had no experience with buying digital currency from exchanges, and 84 of 99 (85,7%) had no experience with sending or receiving digital currency. No respondents assessed that they had much or very much experience with digital currency. The low self-assessed competency level can indicate that digital currency is an area within digital investigation where increased focus on training and competency should be implemented.

Another concept where the self-assessed experience were rated as very little or non-existent was the use of P2P technology to download files. 42,9% reported they had no experience, and 17,3% reported they had very little experience. On the other side of the scale, 14,3% reported they had much experience and 4,1% had very much experience. This technology is, or at least was, used to a degree in sexual abuse cases to share illegal content. In order to be able to investigate the initial phase of cases where P2P technology is present, the self-assessment indicates the general competency for this topic should be increased.

The remaining concepts received most answers on the option *Some experience*. This can indicate the remaining concepts are all topics where the competency level could be improved if deemed relevant for investigating criminal cases. I would argue that experience with the concepts would better enable the police generalist to receive, and perform initial digital investigative steps, when faced with a criminal case that contains elements from these concepts.

TABLE 8. EXPERIENCE WITH VARIOUS TECHNOLOGY

	No experience	Very little experience	Little experience	Some experience	Much experience	Very much experience	N
Buy or sell items using Norwegian web sites (e.g. Finn.no)	2	4	12	44	31	6	99
Buy or sell items using non-Norwegian web sites (e.g. Amazon or eBay)	30	16	15	23	11	4	99
Buy digital currency like Bitcoin and Ethereum from exchanges, e.g. Kraken and Coinbase	86	4	4	5	0	0	99
Send or receive digital currency like Bitcoin and Ethereum using a digital wallet	84	5	5	4	0	0	98
VoIP (Voice over IP) calls like FaceTime, Skype and Messenger	9	12	17	39	16	6	99
Communicating with other people using applications like Telegram, WhatsApp and Skype etc	9	8	13	32	22	14	98
Using P2P (Peer to Peer) technology to download files, by using clients like LimeWire and BitTorrent	42	17	8	13	14	4	98
Create a new e-mail address from a site like Gmail and Yandex etc.	8	7	18	37	19	10	99

Number of potential digital evidence in the last three criminal cases

To be able to give an indication of the extent of digital evidence present in criminal cases, the respondents were asked how many potential digital evidence were present in the last three cases they worked. If they answered «*1*» or more, they were also asked what kind of evidence were present.

Note: Due to an error when designing the survey, the respondents were only able to choose *one* item that were present in the last cases. This error has been identified and discussed in chapter 3.6.

One of ten respondents (11,1%) answered in the last three criminal cases they had worked on, one case had potential digital evidence present.

15 of 99 respondents (15,2%) answered two of the three latest cases they had worked on had potential digital evidence present.

Over half over the respondents (51,5%) answered in the last three cases they had worked on, or were involved in, there was at least one potential digital evidence present in each case.

Four of 99 respondents (4%) answered there were no potential digital evidence present, and ten of 99 (8,1%) was not sure.

Discussion

In chapter 2.1 there was referred to a report of the number reported offences in Norway in 2018, where an ICT-related modus was found in 5,1% of all the cases. This modus was registered for a total of 16.225 cases. In the survey around 3 of 4 answered that in the last three cases they had worked at least one potential digital evidence was present. When the

number of total reported offences in 2018 was 318.556, the answers from the survey indicate the actual number of cases which should have had an ICT-related modus might be significantly higher than the reported 5,1%. The number of criminal cases with a ICT-related modus could influence how prioritised digital evidence are, and it is important that this number reflects reality. It is important to underline that it is unclear if registration of modus includes the actual presence of digital evidence in the statistics. If the modus does not include the presence of digital evidence, the registration regime should be improved to be able to survey the extent of digital evidence present in criminal cases.

TABLE 9. NUMBER OF CASES THAT HAD AT LEAST ONE POTENTIAL DIGITAL EVIDENCE PRESENT

Name	Count	Percent
0	4	4.0%
1	11	11.1%
2	15	15.2%
3	51	51.5%
Unsure	10	10.1%
Have not worked three criminal cases	8	8.1%
N	99	

As mentioned above, the follow-up question was flawed, and the results from *what kind* of potential digital evidence was present will not be used in the discussion section. However, 77 respondents still answered by selecting only one potential digital evidence. Of the two options that scored highest, 39 of 77 (50,6%) selected cell phone and eleven of 77 (14,3%) selected social media.

Set of scenarios - Receive and write a police report and perform investigative steps
In this set of questions the respondents should assess their own competency when it comes to a wide range of scenarios. The same scenarios were divided into two phases:

1. Receive and write an initial police report

    Scenario: Receive and write an initial police report. In the following scenarios your job is to receive and write a police report from various people/companies. Police report is equivalent to «mottatt anmeldelse». When receiving the police report sufficient follow-up questions should be asked so that the police report is as complete and full of details as possible.

2. Perform initial investigative steps

    Scenario: Initial investigative steps. In the following scenarios the police report is written, and you are tasked to do, or order, initial digital investigative steps. Initial digital investigative steps can be location and preservation of evidence, send requests to third-party actors like Finn.no and ask for account information and basic subscriber information etc.

The purpose of phase 1 was to measure how competent the police officers felt they were in the absolute beginning of the initial phase of an investigation.

Using the same scenarios as the previous scenario set, the respondents were in phase 2 asked to assess how competent they perceived themselves when they were tasked to do initial investigative steps.

In each scenario, the answer alternative which received the most answers are highlighted with a colour. An assessment of possible indications is linked to the levels on the self-assessed competence. If the respondents assess they do not have competence or that they have very little competence, this can indicate major deficiency in their digital competence. The results from each scenario is discussed after each scenario, while a summary of the findings is presented in the end of this section.

Color scheme	Indications
Not competent	Major deficiencies in competency
Very little competent	Major deficiencies in competency
Little competent	Deficiencies in competency
Somewhat competent	Deficiencies in competency
Competent	Sufficient competency
Very competent	Sufficient competency

Note: Due to a weakness in the survey design, the answers the respondents could choose are not identical in phase 1 and phase 2. This is discussed in chapter 3.6.

Scenario 1: A company wants to report a denial-of-service attack on their computer systems

When tasked to receive and write a police report in a criminal case involving a DDoS attack[22], Three of four (75%) respondents consider themselves *very little competent* or *not competent at all*. Seven of 96 (7,3%) respondents assess they are *competent* or *very competent*.

When asked to perform initial investigative steps, 79,8% answered they are *very little competent*, or not competent at all. The number of respondents who consider themselves *competent*, or *very competent*, to perform initial investigative steps are 12,1%.

Discussion

The answers from the survey indicates there is a major deficiency in the self-assessed competency level when it comes to receiving a complaint and writing a police report, and also to perform initial digital investigative steps in a criminal case which involves distributed denial of service attacks.

TABLE 10. SELF-ASSESSED COMPETENCY, RECEIVE AND WRITE AN INITIAL POLICE REPORT, DDOS-ATTACK

Name	Count	Percent
Not competent at all	59	61.5%
Very little competent	13	13.5%
Little competent	7	7.3%
Somewhat competent	10	10.4%
Competent	6	6.3%
Very competent	1	1.0%
N	96	

[22] DDoS: A distributed denial of service attack is a malicious attempt to make a server or a network resource unavailable

TABLE 11. SELF-ASSESSED COMPETENCY, INITIAL INVESTIGATIVE STEPS, DDOS-ATTACK

Name	Count	Percent
Not competent at all	60	60.6%
Very little competent	19	19.2%
Little competent	5	5.1%
Competent	10	10.1%
Very competent	2	2.0%
Will never do, or order, investigative steps	3	3.0%
N	99	

Scenario 2: A young girl wants to report a nude picture of her that has been distributed using a mobile app

One of three respondents (32,3%) perceive themselves to be *competent*, or *very competent*, to receive and write a police report in a criminal case where a nude picture has been distributed using a mobile app. While receiving and writing the police report one prerequisite was that sufficient questions were asked so the report would be as detailed and complete as possible. 3,1% reports they are *not competent at all*. 64,5% of the respondents report they are *very little* to *somewhat competent*.

One of three respondents (34,3%) reports they are *competent* or *very competent* when tasked to do initial investigative steps. However, in the other end of the scale 14,1% of the respondents assess they are *not competent at all* to do initial investigative steps.

Discussion

The alternative that received the single most answers was *Competent.* The high number of respondents which assess that their competency is below competent, indicates there are deficiencies in the competence level related to receiving a complaint and writing a police report in a case where a nude picture has been spread by a mobile application. Deficiencies in the competency can also be indicated when it comes to performing initial digital investigative steps in the same criminal case.

TABLE 12. SELF-ASSESSED COMPETENCY, RECEIVE AND WRITE AN INITIAL POLICE REPORT, NUDE PICTURE

Name	Count	Percent
Not competent at all	3	3.1%
Very little competent	20	20.8%
Little competent	20	20.8%
Somewhat competent	22	22.9%
Competent	25	26.0%
Very competent	6	6.3%
N	96	

TABLE 13. SELF-ASSESSED COMPETENCY, INITIAL INVESTIGATIVE STEPS, NUDE PICTURE

Name	Count	Percent
Not competent at all	14	14.1%
Very little competent	23	23.2%
Little competent	26	26.3%
Competent	24	24.2%
Very competent	10	10.1%
Will never do, or order, investigative steps	2	2.0%
N	99	

Scenario 3: A man wants to report that his online bank account has been depleted of money

One of five respondents (22,9%) answered they are *competent*, or *very competent* to receive and write a police report where an online bank account has been depleted of money. One of three respondents assess that they are *very little competent* (24%) or *not competent at all* (8,3%).

To conduct initial investigative steps, one of three (31,3%) rate themselves as *competent* or *very competent*, while one of three (34,4%) rate themselves as *very little competent* and *not competent at all*.

Discussion

Faced with a man that reports a depleted online bank account, the self-assessed competency level indicates deficiencies when it comes to receiving and writing a police report. It also indicates deficiencies in performing initial digital investigative steps.

TABLE 14. SELF-ASSESSED COMPETENCY, RECEIVE AND WRITE AN INITIAL POLICE REPORT, DEPLETED ONLINE BANK

Name	Count	Percent
Not competent at all	8	8.3%
Very little competent	23	24.0%
Little competent	19	19.8%
Somewhat competent	24	25.0%
Competent	20	20.8%
Very competent	2	2.1%
N	96	

TABLE 15. SELF-ASSESSED COMPETENCY, INITIAL INVESTIGATIVE STEPS, DEPLETED ONLINE BANK

Name	Count	Percent
Not competent at all	16	16.2%
Very little competent	18	18.2%
Little competent	32	32.3%
Competent	24	24.2%
Very competent	7	7.1%
Will never do, or order, investigative steps	2	2.0%
N	99	

Scenario 4: An elderly man that wants to report that he has been defrauded on FINN.no

36 of 99 respondents (37,9%) assess they are *competent* or *very competent* to receive and write a police report in a fraud case on the market place finn.no. One of 99 (1,1%) reports that they have *no competency at all*.

The number of respondents who report they are *not competent at all* to conduct initial investigative tasks in a fraud case on the market place finn.no are one of ten (10,2%). Respondents who answered they were *competent*, or *very competent* was one of three (34,9%).

Discussion

When tasked with receiving and writing a police report in a criminal case related to a market place fraud, the single option which received the most answers was *Competent*. However, when the other answers are examined, it becomes clear the assessed competency level indicates there are deficiencies in the competency.

The *Competent* option received the single most answers when the respondents were asked to perform initial digital investigative steps. The number of respondents who assessed their competence to be lower than *competent* indicate there are deficiencies in the competency level. It can be worth noting there was only one count which separated the option *Competent* from being equal to the option *Little competent* when asked to perform investigative steps.

TABLE 16. SELF-ASSESSED COMPETENCY, RECEIVE AND WRITE AN INITIAL POLICE REPORT, MARKET PLACE FRAUD

Name	Count	Percent
Not competent at all	1	1.1%
Very little competent	15	15.8%
Little competent	21	22.1%
Somewhat competent	22	23.2%
Competent	30	31.6%
Very competent	6	6.3%
N	95	

TABLE 17. SELF-ASSESSED COMPETENCY, INITIAL INVESTIGATIVE STEPS, MARKET PLACE FRAUD

Name	Count	Percent
Not competent at all	10	10.2%
Very little competent	16	16.3%
Little competent	28	28.6%
Competent	29	29.6%
Very competent	13	13.3%
Will never do, or order, investigative steps	2	2.0%
N	98	

Scenario 5: A woman wants to report that her identity has been stolen
In the scenario with identity theft, 26,3% of the respondents assessed they were *competent* or *very competent* when receiving and writing a police report, and 28,4% assessed they were *not competent at all* or *very little competent*.

One of three (33,7%) reported to be *competent* or *very competent* when conducting initial investigative tasks. 35,7% reported to be *not competent at all*, or *very little competent*.

Discussion
With the scenario of identity theft, the self-assessed competency level was quite equal spread out when asked to receive and write a police report. Three different levels of competency received 21 answers, while the level which received the most got 22 answers. The majority of the answers still fell in the category that indicates the competency has deficiencies (45,3%). When it comes to initial digital investigative steps, the answers indicate there are major deficiencies in the competence level for over one third of the respondents (35,7%).

TABLE 18. SELF-ASSESSED COMPETENCY, RECEIVE AND WRITE AN INITIAL POLICE REPORT, IDENTITY THEFT

Name	Count	Percent
Not competent at all	6	6.3%
Very little competent	21	22.1%
Little competent	22	23.2%
Somewhat competent	21	22.1%
Competent	21	22.1%
Very competent	4	4.2%
N	95	

TABLE 19. SELF-ASSESSED COMPETENCY, INITIAL INVESTIGATIVE STEPS, IDENTITY THEFT

Name	Count	Percent
Not competent at all	17	17.3%
Very little competent	18	18.4%
Little competent	28	28.6%
Competent	25	25.5%
Very competent	8	8.2%
Will never do, or order, investigative steps	2	2.0%
N	98	

Scenario 6: A man has received an e-mail that claims his computer is hacked, and the hacker has recorded the man while he watched pornography. The hacker threatens to send the video to the man's family and friends if he does not pay 0,1 Bitcoin to an address.
In the example with a sextortion e-mail, twelve of 96 respondents (12,5%) assessed that they were *competent* or *very competent* to receive and write a police report. Almost one of three (29,2%) reported they were *not competent at all*.

When tasked to do initial investigative tasks in the sextortion scenario, 21,3% of the respondents perceived themselves to be *competent* or *very competent*, while 27,3% believed they were *not competent at all*.

Discussion
The scenario with a possible sextortion e-mail gave answers that, based of self-assessed competency, indicates there are major deficiencies in the competency level.

TABLE 20. SELF-ASSESSED COMPETENCY, RECEIVE AND WRITE AN INITIAL POLICE REPORT, SEXTORTION

Name	Count	Percent
Not competent at all	28	29.2%
Very little competent	23	24.0%
Little competent	17	17.7%
Somewhat competent	16	16.7%
Competent	10	10.4%
Very competent	2	2.1%
N	96	

TABLE 21. SELF-ASSESSED COMPETENCY, INITIAL INVESTIGATIVE STEPS, SEXTORTION

Name	Count	Percent
Not competent at all	27	27.3%
Very little competent	29	29.3%
Little competent	19	19.2%
Competent	15	15.2%
Very competent	6	6.1%
Will never do, or order, investigative steps	3	3.0%
N	99	

Set of scenarios - summary of self-assessed competency level
Based on results from the respondents self-assessment of their competence in the six scenarios, each scenario indicates there are deficiencies when receiving a complaint and writing a police report and also when tasked to perform initial digital investigation steps. The two scenarios that stands out with indications of major deficiencies are *DDoS-attacks* and *sextortion via e-mail*. The scenarios which involved *distribution of a nude picture* using a mobile application, *online bank fraud*, *market place fraud* and *identify theft* had an average indication of deficiencies in the competency level.

Set of scenarios - Digital evidence handling
The pre-requisite for this question was that the respondent was the first unit on a crime scene, and the respondent was responsible for handling the digital evidence which were present. Handling was defined to be identification, any initial examination of the evidence on-site and actual seizure of the evidence. The respondents were asked to assess their own competency. The digital evidence varied from a turned on iPhone 8 where the lock code was known to a Linux server belonging to a large company. There was also a scenario where the respondents were asked by the local Computer Crime Unit to do live forensics.

When asked to handle a turned-on iPhone 8 where the passcode is provided, 56 of 84 respondents (64,6%) of the respondents believe they are *competent* or *very competent*. Nine of 84 (10,7%) report that they are *not competent at all*, or *very little competent*.

If the turned-on iPhone 8 is switched out with a Samsung Galaxy S7 where the passcode is *not* provided, the number of respondents who report they are *competent* or *very competent* is 33

of 82 (40,3%), and the respondents who are *not competent*, or *very little competent* is up to 27 of 84 (33%).

36 of 84 respondents (42,9%) assess they are *competent*, or *very competent*, to handle an Apple iMac that is turned off. In the other end of the scale, 32 of 84 respondents (38,1%) assess they are *not competent at all*, or are *very little competent* to handle the iMac.

37 of 81 respondents (44,7%) assess they are *competent*, or *very competent*, when they are faced with a running Dell laptop they must handle. 21 of 81 respondents (25,9%) answer they are *not competent*, or *very little competent*, to handle the running Dell laptop.

A company Linux server and a turned-on computer with an open TorBrowser, are two types of digital evidence where 39 of 83 (47%) believes they are *not competent at all* to handle. On the Linux server, eight of 83 (9,6%) believe they are *competent*, or *very competent*, to handle it. When it comes to the turned-on computer with a TorBrowser open, 14 of 83 (16,8%) rate themselves *competent*, or *very competent*.
To handle a video surveillance system, and export a video from a given time frame, 52,4% of the respondents report they are *competent*, or *very competent*, whereas 26,2% report *no competency as all*, or *very little competency*.

Over half of the respondents (55,9%) assess they are *competent*, or *very competent*, to handle an external hard drive that is not running and is not connected to a computer. One of four (25%) reports they are *not competent at all*, or that they are *very little competent*.

When tasked to check a running Windows computer for encryption, 36 of 84 respondents (42,9%) report *no competency at all*. 16 of 84 respondents (19%) assess they are *competent*, or *very competent*, to check for encryption.

Lastly, when asked to do a Triage on a running Windows computer, using a live forensics tool like osTriage, 60 of 84 respondents (71,4%) answer that they are *not competent at all*. Eleven of 84 (13,1%) reports they are *competent*, or *very competent*.

Discussion
The pre-requisite was that the respondents should rate their own skills faced with various evidence in regards to handling of the evidence. Handling was defined to be identification, any initial examination of the evidence on-site and actual seizure of the evidence. 37 of 81 respondents assess they are *competent*, or *very competent*, when faced with a Dell laptop which is running, and where there is no screen saver enabled. This means they assessed they were *competent*, or *very competent* to handle this evidence, including initial examination of the evidence on-site. However, when the computer crime unit asked them to check for signs of active encryption, only 16 of of 84 respondents answered they were *competent*, or *very competent*, to do this. The number of respondents who answered they were *not competent at all* increased from four to 36 in the same questions. Checking for sign of active encryption is one of the tasks that naturally occurs under the initial examination of the evidence on-site, and there is a inconsistency between the respondents assessment of their own skills in these two questions that should not be overlooked.

It is also interesting to note the number of respondents who assess they are *not competent at all* are higher when faced with an Apple iMac that is turned off (15 respondents), compared to the number who assess they are *not competent at all* when faced with a running Dell laptop

(four respondents). A turned off Apple iMac can, as a general rule, be handled like any other traditional evidence, there is normally no need for any initial examination on site. A running Dell laptop, however, might require initial examination where it for example is checked for active encryption.

The scenarios where the respondents are faced with a running Linux server, a turned-on computer with a TorBrowser and a computer that Triage should be performed on all received a high number of respondents assessing that they did not have any competency at all. This indicates these three scenarios contains elements where increased competency and training could be beneficial. It should be noted that the scenario with a Linux server belonging to a large company is not a task which would normally be handled by first responder from the police, this would either be handled by computer forensics investigators from the various computer crime units or from personell from NCIS.

Faced with mobile phones, a video surveillance system and an external hard drive that is not running and not connected, the assessments which got the highest individual score was *Competent*. This might be related with the likelihood that these kind of digital evidence is what the average police officer faces most often.

TABLE 22. SELF-ASSESSED COMPETENCY, EVIDENCE HANDLING

	Not competent at all	Very little competent	Little competent	Competent	Very competent	N
A turned-on iPhone 8 that the owner willingly give you the passcode to	1	8	19	37	19	84
A turned-on Samsung Galaxy S7 mobile that the owner refuses to provide passcode to	13	14	22	25	8	82
An Apple iMac that is turned off	15	17	16	23	13	84
A Dell laptop that is running, and no screen lock is turned on. You have full admin access to the computer	4	17	23	26	11	81
A large company's Linux server that is running, you have the user name and password for the suspect's user account. It is only the suspect's user account that is relevant for your case.	39	25	11	7	1	83
A turned-on computer where you see that a web browser named TorBrowser is running displaying the URL http:// zqktlwi4fecvo6ri.onion/wiki/index.php/ Main_Page	39	18	12	7	7	83
A video surveillance system in a grocery store where you are tasked to export a video from a given time frame	11	11	18	34	10	84
An external hard drive that is not running and is not connected to a computer	11	10	16	27	20	84
A running Windows computer where the computer crime unit asks you to check if there are signs of encryption	36	14	18	9	7	84
A running Windows computer where the computer crime unit asks you to do triage using a live forensics tool like osTriage	60	8	5	8	3	84

Technology and concepts from digital investigation

Presented with various technology and concepts from digital investigation, the respondents were asked to assess their own skills.

In each technology, and concept, the answer alternative which received the most answers are highlighted with a colour.

No knowledge/skills at all
Very little knowledge/skills
Little knowledge/skills
Some knowledge/skills
Much knowledge/skills
Very much knowledge/skills

On all the questions for this topic, except the questions about how to find an Internet Service Provider based on an IP-address and how the Internet works in theory, the answer alternative with *No knowledge/skills at all* was the alternative most frequently selected by the respondents.

The average perceived knowledge and skills for the questions were between *No knowledge/skills* and *Little knowledge/skills*. The exceptions were the question about finding ISP, as mentioned above, and the question about why time sone settings can be crucial. For those two questions the average response was between *Little knowledge/skills* and *Some knowledge/skills*.

TABLE 23. SELF-ASSESSED COMPETENCY, TECHNOLOGY AND CONCEPTS FROM DIGITAL INVESTIGATION

	No knowledge /skills at all	Very little knowledge /skills	Little knowledge/ skills	Some knowledge/ skills	Much knowledge /skills	Very much knowledge /skills	N
E-mail acquisition	28	16	20	22	9	4	99
Crypto currencies, e.g. Bitcoin and Ethereum	68	13	9	7	0	1	98
Order of Volatility (how volatile digital evidence are - in what order should they be acquired)	46	12	9	22	6	2	97
Logical vs physical acquisition of devices	35	24	6	19	10	4	98
Finding an Internet Service Provider, e.g. Telenor, based on an IP address	25	8	12	25	13	14	97
Live data forensics (investigation on an actual evidence)	51	12	9	19	5	2	98
Computer network functionality	48	24	9	11	4	2	98
Ransomware	64	15	12	5	0	1	97
Why time zone settings can be crucial	28	12	13	19	19	7	98
Write and send a request to a content provider like Google, to get basic subscriber information (BSI)	30	22	11	18	10	7	98
Malware	63	16	11	4	2	1	97
Dark web	50	25	10	11	2	1	99
How the Internet works in theory	20	23	21	22	12	1	99
VPN (Virtual Private Network)	38	20	13	19	7	2	99

Discussion
Based on the results from the self-assessment of knowledge and skills related to various topics related to digital investigation, there is a clear indication there is deficiencies in most of the listed skills and knowledge among the respondents. Except for the question about finding an Internet Service Provider based on an IP-address, the alternative which got the most individual answers were either *No knowledge/skills at all*, or *Very little knowledge/skills*. This indicates there is a need for further training and for raising competence within the listed topics and concepts.

Assessment of competency when reviewing evidence with commercial tools
The use of commercial tools for reviewing evidence is widespread in the Norwegian police, and most likely in other law enforcement agencies across the world. One of the earlier questions asked was related to if the respondents have received training, and what that training included. The question with competency when reviewing evidence with commercial tools might be influenced by how training is provided, and was therefore a natural addition the the survey.

Griffeye Analyze[23] is one of the most used programs in Norway to review and categorise pictures and videos, mostly in sexual abuse cases. 55,6% of the respondents answered they are *not competent at all*, while 19,2% of the respondents report that they are *competent*, *or very competent*.

Internet Evidence Finder (IEF) / Axiom[24] is one tool used to analyse digital evidence. This tool processes various artefacts and present them in a human readable format. 57,7% of the respondents answered that they are *not competent at all*, while 18,6% of the respondents report that they are *competent*, or *very competent* to review evidence using IEF and/or Axiom.

Cellebrite Physical Analyser[25] and Cellebrite Reader is a tool mainly used for reviewing and analysing acquisitions from mobile phones. Here, 48,5% answered they are *not competent at all*, while 21,2% answered they are *competent*, or *very competent* in reviewing evidence by using Cellebrite Physical Analyser and/or Cellebrite Reader.
XRY Reader[26] is mainly used for reviewing, and to some extent, analyse acquisitions from mobile phones. 40,4% answered they are *not competent at all* to review evidence using XRY Reader, while 25,3% reports they are *competent*, or *very competent*, to review evidence using this tool.

The answer alternative which received the most answers are highlighted with a colouring scheme based on the reported level of competency.

Discussion
Around 10% of the respondents had never heard of the programs Griffeye, Internet Evidence Finder/Axiom and Cellebrite, while around 4% had never heard of XRY Reader. The majority of the remaining respondents assessed their knowledge to review evidence with the tools to be low. The single most selected option for all three tools were *Not competent at all*. This

[23] https://www.griffeye.com

[24] https://www.magnetforensics.com/products/magnet-axiom/

[25] https://www.cellebrite.com/en/home/

[26] https://www.msab.com

indicates that training and courses in the use of these tools should be considered to raise the competence level.

It is important to note that in order to use these programs, a theoretical understanding, and interpretation, of the *results* the program gives the user is crucial. The results should, as a minimum, be reviewed and approved by a peer before it is used in the investigation and presented to the court as evidence.

Not competent at all
Very little competent
Little competent
Competent
Very competent

TABLE 24. SELF-ASSESSED COMPETENCY, REVIEWING EVIDENCE WITH COMMERCIAL TOOLS

	Not competent at all	Very little competent	Little competent	Competent	Very competent	Have never heard of	N
Griffeye Analyze	55	7	9	9	10	9	99
Internet Evidence Finder/Axiom	56	7	7	13	5	9	97
Cellebrite Physical Analyser/Reader	48	8	14	11	10	8	99
XRY reader	40	14	16	19	6	4	99

Testimony in court

Based on my own experience testifying in court, there are asked few critical questions regarding digital evidence and analysis from the members of the court. Even though testimony in court falls outside the scope of the thesis, it is well-connected with digital competency. The respondents were asked if they have testified in court regarding digital evidence and how confident they were. They were also asked if someone else verified their findings before they testified. Finally, they were asked if the members of the court asked questions. All in all, the answers from these questions can point to a topic that should be pursued further by other researchers.

Out of 97 respondents, 27 (27,8%) answered they have given testimony in court about digital evidence.

Of those who have given testimony in court with digital evidence, 17 respondents (60,7%) report they were *confident* when giving testimony. None of the respondents answered they were *not confident at all*. Three respondents (10,7%) answered they were *very little confident*, and the same amount of respondents answered they were *very confident*.

The respondents who had given testimony, were asked if someone else had verified their findings before they gave their testimony.

Of 25 respondents, 14 (56%) had not verified their findings with some else before they gave their testimony. Nine respondents (36%) had verified the findings with a colleague from a computer crime unit, while two respondents (8%) had verified with a colleague who did not work at a computer crime unit.

Discussion
Peer review of digital evidence is important to reduce chances of miscarriage of justice. Even though the results from the survey have too few respondents to be conclusive, the findings that over 50% of the respondents did not verify their findings with someone else before they testified still is an interesting result. Further research is recommended to examine the extent of damage usage of digital evidence with potential low, or even incorrect evidential value, can have on the rule of law. Further, requirements for peer review of digital evidence before they are presented in court should be considered implemented. This is mentioned again in chapter 5.

TABLE 25. VERIFICATION OF FINDINGS BY OTHERS BEFORE GIVING TESTIMONY

Name	Count	Percent
Yes, a colleague from a computer crime unit	9	36.0%
Yes, another colleague that does not work at a computer crime unit	2	8.0%
No	14	56.0%
N	25	

The respondents who had given more than one testimony in court with digital evidence, were asked to briefly describe how they felt when they gave their testimony. From the answers provided there were three topics which were mentioned by several.

Collaboration with a computer crime unit
One respondent writes that s/he was confident because there was a close collaboration between prosecutor and the CCU. S/he was sure what s/he could be sure of and honest about uncertainty. Another respondent writes that s/he had double-checked the findings with employees from the computer crime unit, and there was an agreement of the significance of the findings.

Lack of competence among the legal actors
Several respondents point out the lack of competency among the legal actors. One respondent even points out how the lack of competency can lead to problems with the Rule of Law[27]:

> *The court's participants are often not very competent in the field of study and rarely ask critical questions to my findings. Only resourceful people and companies have used their own people with expertise in some very few cases. May be a problem with the Rule of Law.*

A respondent had the feeling that the members of the court understood little, and therefore they had little opportunity to ask good questions.

Another respondent experience that the the courts, the defences and co-judges' competency is very low, and that a police witness' testimony gets too much reliance without it being sufficiently questioned. S/he writes that «*Sometimes one can feel that one can say what one wants without the actors in the court having the competence to ask the right questions*». S/he also writes that if the person giving testimony is too stout it can affect the Rule of Law.

[27] Directly translated from the Norwegian word «*Rettssikkerhetsproblem*»

Lastly, a respondent writes that testimony regarding digital evidence is challenging, as most actors in court lack an understanding about the field of study and technology. The questions which are asked are «*often absurd*» and impossible to answer, especially without a forewarning about questions that could give a possibility to examine further or conduct investigative steps. The respondent also writes «*the biggest challenge is that actors in the judiciary do not follow technological developments*».

Focus areas from the actors in court
Time, and artefacts related to time, is mentioned to be important to the actors in court.

The respondents who had testified in court were asked if their testimony were questioned from the parties in court. 21 of 27 respondents (77,8%) answered that a few questions were asked, while four of 27 respondents (14,8%) answered that many questions were asked. The remaining two respondents (7,4%) answered that no questions were asked from the parties in court.

Of the 25 respondents who were questioned during their testimony, 24 of 25 (96%) felt they were competent to answer the questions in a sufficient matter.

Discussion
A close collaboration between the investigator and the local computer crime unit regarding the significance of the findings prior to testifying is indicated to enhance the confidence for the investigator. This approach seems reasonable, and peer review can also act as a safeguard against usage of evidence which has been wrongly interpreted.

The reported lack of competence among the legal actors is a topic which definitely should be researched further. It is utmost important that all the actors in the court system either has sufficient digital competence, or that they have enough digital competence to understand when they need to ask for help by someone else who has the correct competence.

Crowdsourcing inputs on the challenges with digital investigation and possible ways of improving skills
Two heads are often better than one. To highlight the greatest challenges with digital evidence and digital investigation one hundred heads are definitely better than one. The two final questions served as a gauge on what a large group of police employees believe is the greatest challenges with digital investigation, and also suggestions on what can be done to further improve the competency level in digital investigation.

The listed challenges with digital investigation are varied. Two challenges stand out; a lack of competence and a rapid technological development which makes it difficult to keep up. Other challenges mentioned are lack of specialised computer investigators, and the fact that digital investigation is a comprehensive and demanding field. Several respondents answered that a lack of priority from the management is a challenge. Insufficient time for competence for further education during work hours was also mentioned. Based on the answers, further research on this topic is recommended.

When asked of ways to further improve the digital competence, several respondents highlight OÅO as a good initiative to enhance the level of competence. The need for available time for competence-raising measures during work hours are listed by several respondents. There is

also mentioned a need for systematic experience learning to show what works and potential for improvement, and that this learning should also include patrol officers.

One respondent gave a statement which sums up the need for competence in a structured system: «*Must end that one should be able to do things without any kind of training*». From that statement one can interpret there is an expectation that work tasks will be solved, regardless of whether training is actually facilitated or not

4.2 Practical test

In this section the results from the practical test will be presented. For the readers convenience, the interpretation is presented right after the results, and the main topics are presented again. The general results and the implications are discussed in chapter 5.

4.2.1 Experimental design

The test was designed to fulfil three main purposes. The first was a concrete motivation to assess how able the participants were to solve different tasks that I had experienced that investigators met during their daily work. To answer the first motivation, three different scenarios to assess a *variation* of competency were created. Secondly, the test was designed to be able to assess the different competency levels according to the levels in Bloom's Taxonomy presented in chapter 2.6. Finally, the test strived to reflect the structure of the Digital Forensics Process Model and the process model for investigation presented in chapter 2.5.1 and 2.5.2.

It can be worth to emphasise that the practical test's purpose is to be a proof of concept for a certification for employees who will face digital investigation. It has therefore not been tested on a large audience, and further research and development is necessary.

Timeframe for the start and end of collecting data

The invitation to take the practical test was sent out 15th of April 2019. Cut-off for responses, and download of the results, was done 8th of May 2019. This was to allow time to analyse the data and discuss the findings. There were a total of six (6) answers.

4.2.2 Material critics - data

The purpose of the practical test was never intended to be used to generalise about the digital competency level in the Norwegian police, as discussed in chapter 3.4. The main purpose was to create a proof of concept for a certification which could be developed further. The practical test can be used as a *starting point* for further development of a certification within digital investigation.

4.2.3 Results

General info about the respondents answers

The survey was distributed to nine employees in the Norwegian Police. Of those nine employees, seven were either proficient or were known to be familiar with digital investigation. Two were selected because they were known not to be proficient with digital investigation. These two did not have digital investigation as one of their primary work tasks.

Demography
At the very beginning of the practical test, there were questions to survey the demography of the participants. These questions were identical to the questions used in they survey, and was also here included to be able to do a deeper and more comprehensive analysis. Questions were asked to enable filtering on when the respondents graduated from PHS and what role described their daily work tasks. The questions used were closed. The last question in the demography section asked the participants if investigating digital evidence was one of their primary work tasks. This question was included to make it possible to analyse the results from the test based on if the participants primarily worked with investigating digital evidence or not.

The participants roles included *Investigator, specialised investigation* (2), *Computer Forensics Investigator* (2), *Patrol Duty* (1) and *Manager* (1).

Of those six participants who completed the test, two reported that investigating digital evidence was *not* one of their primary work tasks. This is a strong indication that those two participants who were selected because they were not proficient with digital investigation, and was known to not have investigation of digital evidence as one of their primary work tasks, completed the test.

Topic 1 - Formulate hypotheses and initial digital investigative steps
The participants were presented three different scenarios with various amount of information, and they were tasked to formulate which hypothesis/hypotheses they could make from the information. In each scenario they were first asked to formulate hypotheses, and they were then asked to explain which initial digital investigative steps they would like to conduct, and why they would conduct them. All questions were open-ended.

Andersen's model starts with an incident or event, and the next phase is the formulating of hypotheses. The questions asked in topic 1 provided the participants with an incident or event, and the answers can be used to assess if the participants are able to provide hypotheses. The set limit for numbers of hypotheses were ten. The maximum number of investigative steps were limited to six.

When the test was designed, a set of hypotheses for each scenario were created to see if the participants developed the same, or new, hypotheses. The main purpose with this question was to see if any hypotheses were developed, and the number of hypotheses. The *quality* of the hypotheses was not intended to be evaluated, as this is beyond my competency.

In each scenario, the participants were asked to formulate up to ten hypotheses based on the information provided. The main purpose of these questions was, as mentioned earlier, not to evaluate the quality of the hypotheses provided, but to see the number of hypotheses the participants generated. One challenge with open-ended questions is that an assembly of the answers can be difficult as even similar answers are not identical. The answers from each scenario were structured in a table, and where the hypothesis clearly did not fit into an existing hypothesis a new hypothesis were added.

Scenario 1.1
In this scenario the participants were presented with the following background information:

> *It is Monday April 1, 2019 and the rain is pouring down. Fortunately you have office duty inside a police station in the vicinity of Oslo. One of your tasks is to receive complaints*

and write down statements from the members of the public. Around 5:00 pm, 20-year old Linda enters the police station and arrives at the counter where you are sitting. She shows you a picture of a gun she has on her iPhone. Linda explains that she got this picture from her boyfriend Ronny around 14:00 the same day. The picture was sent without preamble and she says she hasn't talked to Ronny in a month. She believes Ronny sent the picture because they will meet in court next week in an ongoing child custody case. Now Linda is afraid of her life and she wants to report Ronny to have threatened her.

Of the six participants, all of them generated at least four hypotheses. Four participants generated six hypotheses, and two generated a total of nine hypotheses.

As a curiosity, the participants provided eleven new hypotheses which were not part of the example hypotheses created when designing the scenario.

TABLE 26. PRACTICAL TEST: HYPOTHESES FROM SCENARIO 1.1

Example hypotheses	**Times the same/similar hypothesis was mentioned**
H1: Ronny has sent the picture to Linda	
H1.1: Ronny has sent the picture to frighten Linda due to the upcoming child custody court hearing	2
H1.2: Ronny has sent the picture to scare Linda, but it is a April fools joke that has gone terrible wrong	0
H1.3: Ronny has sent the picture with other motive	9
H2: Ronny has not sent the picture to Linda, someone else did	
H2.1: Someone else that has access to Ronny's phone or social media etc. has sent the picture acting alone	2
H2.2: Someone else that has access to Ronny's phone or social media etc. has sent the picture on request from Ronny	2
H2.2: Linda has fabricated the picture	
H2.2.1: Linda has fabricated the picture to harm Ronny due to the upcoming child custody court hearing	1
H2.2.2: Linda has fabricated the picture to prank Ronny	0
H2.2.3: Linda has fabricated the picture to gain sympathy from her surrounding and/or the authorities	0
New hypotheses provided by the participants	
Ronny has sent the picture to the wrong person	7
Linda has fabricated the evidence	3
Linda has received the picture from someone else than Ronny by a mistake	1
Linda has received the picture from someone else than Ronny, but in relation to another case	1
Linda uses a phone and message that belongs to someone else in order to produce false allegations	1
Ronny plans to take his own life	1
Ronny has sent the picture, but does not threaten Linda or anyone else	1
Ronny plans to kills Linda	1
Ronny plans to kill someone else	1
Ronny pressed the wrong button, and sent a random picture to a random person	1
Ronny has access to weapons	1

After the hypothesis/theses had been formulated, they were asked which initial digital investigative steps they would like to conduct, and why they would conduct them. The participants were informed that their job was complete when the police report was written, and after they had conducted initial investigative steps. An example of an initial investigative step was to seize a hard drive or an e-mail account.

Five of six participants answered they would seize Linda's phone. The purpose was to preserve the evidence and/or facilitate for analysis of the picture to determine the origin of the picture. None of the participants answered they would interview Linda to get an overview of social media accounts and e-mail addresses. Two of the participants wrote they would seize Ronny's phone, while one participant implicitly would do the same as s/he wrote that one investigative step would be «*Look at Linn and Ronny's phone*».

TABLE 27. PRACTICAL TEST: INVESTIGATIVE STEPS FROM SCENARIO 1.1

Example investigative steps	**Purpose/reason**	**Number of times mentioned**
Seize Linda's phone	Acquire evidence to be analysed further	5
Seize Ronny's phone	Acquire evidence to be analysed further	2 (3)
Interview Linda	Get an overview of social media accounts and e-mail addresses	0
Seize e-mail and online accounts belonging to Linda	Acquire evidence to be analysed further	2
New investigative steps provided by participants		
Seize online accounts belonging to Ronny	Preserve digital evidence	1
Take a picture of the picture on the phone	As a backup if other evidence should get lost	2
Consider apprehending Ronny	Ensure that Ronny can not tamper/destroy evidence	1
Save the message history (SMS/MMS) between Ronny and Linda	Find out if the picture is coming from Ronny. Search for the image.	1
Gather traffic data from Ronny's phone	See if his phone was active at the actual time	1
Gather traffic data from Linda's phone	See if her phone was active at the actual time	1
Interview Linda and Ronny	Determine how the picture was sent and the circumstances around the transfer	1
Investigative steps that goes outside the limitations given in the question		
Analyse digital evidence belonging to Linda	Determine the origin of the picture and how it was sent	1
Analyse digital evidence belonging to Ronny	Determine if there are traces from the picture on the unit(s), or other data that can either support or support the hypotheses	1
Analyse the metadata and other information about the picture	Determine the 5WH related to the picture	1

Scenario 1.2
In this scenario the participants were presented with the following background information:

> *You're out on patrol. Together with your colleague you drive through Oslo city center on a Friday night. A man is frantically waving and it is clear that he wants you to stop. You go out of the car and the man says he was scammed when he was buying a MacBook Pro. He also says that he came in contact with the seller of the computer at Finn.no. They agreed that he would transfer NOK 10,000 in advance via bank transfer. The actual handover of the computer would happen at a McDonalds restaurant at 8pm tonight, but the seller never met. Now the man wants to report the fraud.*

All six participants provided at least three different hypotheses. Four participants created four hypotheses, while the remaining two participants created five hypotheses.

After the hypothesis/theses had been formulated, they were asked which initial digital investigative steps they would like to conduct, and why they would conduct them. The participants were informed there was plenty of patrols at work, and that they could carry out initial digital investigative steps. There were not given any limitations to how far they could go.

None of the participants wanted to seize the man's phone. Four of six wanted to get access to the man's finn.no account either to acquire the content or to have access to the account.

TABLE 28. PRACTICAL TEST: HYPOTHESES FROM SCENARIO 1.2

Example hypotheses	**Times the same/similar hypothesis was mentioned**
H1: The man has been defrauded	6
H2: The man has not been defrauded	
H2.1: There has been a misunderstanding, possibly the date, time or McDonalds has been wrong	1
H2.2: The man falsely reports a crime that has not happened for unknown reasons	3
New hypotheses provided by the participants	
The victim is receiving stolen goods, and is selling stolen goods	1
The man has psychological problems	2
The seller has encountered something that prevented him from showing up	4
The money has not been transferred to the seller, and the seller did not show up because of this	1
The man has been defrauded, but in relation to another item than a MacBook Pro	1
The man has been defrauded, the seller intends to show up later an defraud the man once more	1
The man is a scammer, and intends to fraud finn.no for 10.000,- NOK	1
There is more than one victim for the fraud	1
The person that has defrauded the man is operating alone	1
The person(s) that has defrauded the man has taken precautions that make them hard to track	1

TABLE 29. PRACTICAL TEST: INVESTIGATIVE STEPS FROM SCENARIO 1.2

Example investigative steps	Purpose/reason	Number of times mentioned
Seize the man's phone	Acquire evidence to be analysed further	0
Get access to the man's finn.no account	Enable acquisition of messages from the original source	4
Identify the username of the seller and other information of the seller	To enable further investigative steps	0
Contact finn.no	Request information about the seller	3
Contact the man's bank	Request information about where the money has been transferred, to identify the owner of the account	2
New investigative steps provided by participants		
Obtain bank records	Possible identify the person that received the money	3
Obtain bank records	Verify if there has been a money transfer or not	1
Screen shot of the man's money transfers	Document that a payment has occurred, and to which account	1
Contact the man's bank	Stop the money transfer	1
Preserve the SMS the buyer has from the deal	Look at communication, and trace sellers phone number	1
Preserve the message history between buyer and seller on finn.no	Examine the communication	1
Document the message history with a photo	To document the communication	2
Acquire e-mails from seller, if any	Get information about seller, and potential IP address	1
Acquire data from other communication platforms, if any	?	1
Confirm the course of action with finn.no and the man's bank	To first confirm what has actually happened	1

Scenario 1.3

In this scenario the participants were presented with the following background information:

> *Oslo Central Station (Oslo S) is a busy area with thousands of travellers every day. Lately, there have been challenges with a criminal gang, consisting of young men, who are staying at Oslo S. The gang is known to rob people either inside Oslo S or in the immediate vicinity.*
>
> *You work at the police station at Oslo S. It is Saturday around 13:00 and like always Oslo S is crowded with people. A young girl comes to the police station and tells you that a few minutes ago she saw that an elderly man was robbed by several young men in the main terminal, right by the information board.*
>
> *When you arrive, you immediately see an elderly man standing alone and he appears confused. He repeatedly shouts «my iPhone, it's gone .. it's gone».*

Only five participants answered this question. Each participant had a hypothesis that the man was robbed; three of the participants included the gang in their hypothesis, while the remaining two did not specify by whom the man was robbed. Three of five participants had a hypothesis that the young girl had misunderstood the situation, where one of the three included in the hypotheses that the gang tried to help the old man.

Like the two previous scenarios, the participants were then asked to list which initial digital investigative steps they would like to conduct, and why they would conduct them. The participants were tasked with finding relevant digital evidence that could be acquired. They were also informed that they could ask witnesses for help or information if needed.

TABLE 30. PRACTICAL TEST: HYPOTHESES FROM SCENARIO 1.3

Example hypotheses	**Times the same/similar hypothesis was mentioned**
H1: The man has been robbed	
H1.1: Robbed by someone from the gang	5
H1.2: Robbed by someone not belonging to the gang	2
H1.3: Robbed by someone the man knows	0
H2: The man has not been robbed	
H2.1: The young girl misunderstood the situation	3
H2.2: The young girl reports a crime that has not happened for various reasons	1
H2.3: The man is senile, but other than that he is ok	0
New hypotheses provided by the participants	
The girl was an accomplice in the robbery	1
The man has lost his phone	3
Nothing has happened	1
The man has not lost his phone, but can not find it	1
The man lies about being robbed	1
The man has not been robbed, but he is psychologically ill and believes he has been robbed	1

TABLE 31. PRACTICAL TEST: INVESTIGATIVE STEPS FROM SCENARIO 1.3

Example investigative steps	**Purpose/reason**	**Number of times mentioned**
Ask witnesses / bystanders if they have recorded the incident	Get a better overview of what has happened	2
Acquire video surveillance	Get a better overview of what has happened	3
Track the man's iPhone using «Find my iPhone» or equivalent	Locate the phone	4
New investigative steps provided by participants		
Interview the female witness	Find out more what has happened in order to start preserving evidence	1
Interview witnesses	Find out more what has happened in order to start preserving evidence	1
Call the man's mobile phone	Try and locate the evidence	1
Contact mobile operator	Try and locate the phone using IMEI and IMSI	1
Base station data	Locate devices used by the perpetrators	1

The last part of topic 1 was an open-ended question asking the participants what the purpose of hypothesis formulation in an investigation is. The scope for the practical test was not to evaluate the quality of provided hypotheses, and the answers have therefore not been analysed in-depth. However, it can still be worth mentioning that three of the six participants answered, among other things, that one important purpose with hypothesis formulation is to avoid focusing on just one possible explanation. Two other participants answered, among other

things, that hypothesis thinking reduces (confirmation) bias. The last participant provided a long answer, where s/he also pointed out that by working systematically you reduce the possibility for reaching the wrong conclusions.

Summary of topic 1
In the first scenario, the participants provided minimum four hypotheses. In the next two scenarios, the participants provided minimum three hypotheses. The initial digital investigative steps they suggested had some variations, but also several similarities.

When asked what the purpose of hypotheses thinking is, the participants all had reasonable answers. The answers can be found in the preceding section.

Topic 2 - Identification of digital evidence
In this part of the practical test the participants were first asked a closed question related to the time period it is possible to identify a user of an IP address in Norway. Then they were asked to describe what an IP address is, and why it is important for a police employee to have knowledge about this. The first question could be used to assess the *remembering* level in Bloom's Taxonomy, while the second could be used to assess the *understanding* level.

The question that asked how long is was possible to identify a user of an IP address was flawed by that it was possible to select more than one answer, as mentioned in chapter 3.6. Five of six participants selected the option for 21 days, but four of six also answered the option *Varies from ISP to ISP*.

All six participants answered the question with what an IP address is and why it is important for a police officer to have knowledge of this, however with variations in how thoroughly they explained what an IP address is. All wrote that an IP address is an identifier. When they explained why it was important to have knowledge about what an IP address is, the common denominator, for five of six participants, was that an IP address could be important to identify a user. One participant did not provide an explanation of why it was important to know this.

An assessment of the *understanding* level could also be used for the next question. Here the participants was presented a list of items, and they were tasked to select the items they thought might contain potential digital items. When the test was designed there was purposely added items which did not meet the criteria for being digital evidence, as defined by Årnes (2016): «*any digital data that contains reliable information which can support or refute a hypothesis of an incident or crime*». The items which *fall outside* this definition is notepad, camera lens, news paper, plant, drugs, analog watch, water bottle, clothes and power cable. The items within this definition is marked bold and with an asterisk (*) in Table 32. To visualise the answers from the participants, a colouring scheme has been used.

With the exception of headphones, where one participant did not select the item, all participants correctly chose all the items which can contain potential digital evidence. Headphones can contain an internal storage device. One can also imagine that a mobile phone found on a crime scene has an active bluetooth pairing with a pair of headphones found in a suspects apartment, and therefore connects the suspect somewhat to the crime scene.

A plant, drugs and an analog watch were not selected by any participants. One participant answered there could be potential digital evidence in a water bottle, clothes and in a power

cable. Normally one can not *expect* to find digital evidence in either of these six items, even though almost everything *can* be possible.

On a notepad passwords and other relevant information might be found, but digital information is normally not present. Digital information is usually not present on a camera lens, even though it can still be a valuable evidence to connect the camera lens to a crime. A newspaper does not contain digital evidence. Lastly, when it comes to the cuddle toy, I will not argue that it is all wrong to choose this item as a source of containing potential digital evidence. Like with the plant, the drugs and the analog watch one can not expect to find digital evidence in a cuddle toy, but I acknowledge that a USB device can be fitted almost everywhere.

0 answers
1-2 answers
3-5 answers
6 answers

TABLE 32. PRACTICAL TEST: ITEMS CONTAINING POTENTIAL DIGITAL EVIDENCE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	N
Notepad	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	3
Car*	4	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6
Mobile phone*	0	4	2	0	0	0	0	0	0	0	0	0	0	0	0	0	6
Hard drive*	0	0	3	2	0	0	0	1	0	0	0	0	0	0	0	0	6
Camera lens	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	3
News paper	0	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	4
Plant	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cuddle toy(*)	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	3
Drugs	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Analog watch	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Playstation 4*	0	0	0	3	0	0	1	1	1	0	0	0	0	0	0	0	6
Water bottle	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1
Clothes	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1
Headphones*	0	0	0	0	3	0	1	1	0	0	0	0	0	0	0	0	5
SIM-card*	0	0	0	0	0	4	0	0	2	0	0	0	0	0	0	0	6
Power cable	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1

In the last question in topic 2, the participants were presented with a scenario that contained limited information:

> *A brand new Tesla model S has hit a pedestrian, and the pedestrian died after the collision. The driver of the Tesla has explained that the pedestrian jumped into the road. The only witness to what happened was explaining that the pedestrian walked normally on the road shoulder when he was hit.*

They were then asked to identify what potential digital evidence could be present, and what information could be extracted from the digital evidence. The identification part of the question could be used to assess the participants skills and knowledge to the *remembering* level in Bloom's Taxonomy, while the second part of the question could be used to assess the next level, namely *understanding.* The participants could provide up to six different digital evidence and the corresponding potential information. One reason this particular scenario was chosen in the practical test, was that this type of criminal case is quite interesting. A car which collides with a pedestrian can be just an unfortunate car accident, but in the other end of the scale it can also be a homicide camouflaged as an accident.

All the six participants answered that the Tesla contained potential digital evidence, with variations in how detailed the answers were. Three of six participants answered the drivers phone could be relevant. It was interesting to note one participant's answer, where both the drivers and pedestrians mobile phones could potentially illuminate if the driver and pedestrian knew each other. If the driver and pedestrian knew each other, it is not given they were on good terms and this should be investigated further. The same participant also answered that the pedestrians mobile phone could potentially answer if the pedestrian was suicidal.

Two of the potential digital evidence sources that fell outside the prerequisite of the scenario are marked with red in Table 33, and are not discussed further.

TABLE 33. PRACTICAL TEST: POTENTIAL DIGITAL EVIDENCE AND INFORMATION EXTRACTION FROM SCENARIO 2.1.

Example potential digital evidence	**Example information**	**Additional information added by the participants**	**Number of times mentioned**
The Tesla car	How fast the car went, if the driver talked on the phone	Information about the direction the car was driving, sensors that show potential dangers, GPS, turning radius, technical errors with the car, collision data, internet history in the car to see recent use, use of automatic brakes, sensors that register if the driver falls asleep	8
The drivers mobile phone	Talking on phone/unfocused	Find out it the driver knew the pedestrian	3
The pedestrians mobile phone	Suicidal, talking on phone/ unfocused	App usage to see the pedestrians movements, knowledge to the driver, if the pedestrian was suicidal, video of the event, GPS information with info about speed	4
New potential digital evidence added by the participants			
Camera from the Tesla car		Can show the event itself	3
Internet Service Providers/ Telephone operators		Can indicate if the driver used online services	1
Video surveillance from the area		To see if there is video of the event	1
Automatic Traffic Control		Can indicate if the driver has been speeding	1

Summary of topic 2

Tasked with identifying items containing potential digital evidence, the participants correctly selected all the right items, with the exception of one participant who did not select the headphones. In addition to select the correct items, several participants also selected other items which clearly does not contain potential digital evidence, e.g. a news paper and a notepad. They might have selected those items due to an unclear question, or just because they believe that a news paper contain digital data.

In the scenario with the Tesla car and the pedestrian that were hit, all six participants correctly identified the Tesla car itself as a source of potential digital evidence. The drivers phone were also mentioned by three of the participants. It was interesting to note the one participant's answer that both the drivers and pedestrians mobile phones could potentially answer if the driver and pedestrian knew each other, where a possible motive could be identified. To help answer the question related to this scenario, hypothesis thinking would assist the participant.

Topic 3, Part One - Acquisition of digital evidence

The last topic the participants were tested in was acquisition of digital evidence. In the first part of this topic, the participants were asked open-ended questions about various topics within digital investigation. They were asked to name acquisition methods of data from the Internet accessible through a web browser. Furthermore, they were tasked to describe what Order of Volatility is when it comes to digital evidence. Lastly, they were asked to list pros and cons with activating flight mode on a phone after is is seized, and pros and cons with doing live forensics on a computer. All these questions were open-ended. These theoretical questions were used to assess the level of skills and knowledge for both the *remembering* and *understanding* level.

Methods for acquiring data from the Internet

The idea behind the question asking the participants to list up to three methods for acquiring data from the Internet, accessible using a web browser, was to assess if they would list up to three of the following methods: *Screenshot*, *download complete page as web archive*, *save as PDF* or *using a camera to record the content*. Each of these methods has strengths and weaknesses, and a combination of all can be required.

Five of six participants listed methods for acquisition of data from the Internet. The most frequent listed method was screenshot, and all five participants listed this method. Downloading the complete webpage using various approaches was listed by three of five participants. One participant answered that content like video and pictures could be downloaded directly. If this last question is combined with a screenshot it might be sufficient to document the evidence properly. In retrospect the wording of the question could be more precise, to make sure the participants did not answer outside what was the intended scope of the question.

TABLE 34. PRACTICAL TEST: METHODS FOR ACQUISITION OF DATA FROM THE INTERNET

Method	Number of times mentioned
Screenshot	5
Directly from service provider, e.g. Facebook	4
Download complete page as web archive or by using wget	3
Download content directly, e.g. video og pictures	1
Use of commercial tools like Cellebrite Cloud Analyzer	1

Order of Volatility

When asked to describe what Order of Volatility is when it comes to digital evidence, four of six participants described this, with various wording, to be a ranking on how volatile digital evidence is from most to least volatile. Two participants also mentioned that the most volatile digital evidence should be prioritised first. Two of the participants answered that they had never heard of Order of Volatility before.

Pros and cons with activating flight mode on a phone

Five of six participants answered that a benefit by activating flight mode on a mobile phone, is to remove the possibility to remotely wipe the phone. The last participant answered that by activating flight mode there is no external influence on the phone. Negative consequences the participants listed were that by using flight mode no new data comes onto the phone, and by activating flight mode the evidence will be somewhat tampered with.

Pros and cons with conducting live forensics on a computer

Pros and cons by doing live forensics on a computer was answered by all six participants. All six listed, as a consequence, by doing live forensics you will alter the original evidence, either by leaving traces or overwrite data like RAM. The pros of doing live forensics on a computer was listed to be easy access to data, and access to data that is not available with a traditional acquisition.

TABLE 35. PRACTICAL TEST: PROS AND CONS WITH DOING LIVE FORENSICS ON A COMPUTER

#	Pros	Cons
1	Find volatile data, determine if encryption is active, Triage to find relevant items for seizure	Evidence will be tampered with, RAM will be altered
2	Access to evidence you normally would not get, e.g. RAM	Content will be changed
3	Quick access to information that can be time critical to get access to	Leave traces, can destroy the collection of data and the use of this in court
4	Can acquire data that potentially can get lost while waiting for full acquisition	Can alter content before acquisition
5	Access to data that would otherwise be unavailable due to encryption, RAM and connected USB devices	Content will be changed, can overwrite RAM
6	Quick access to data, easy access to logged on online services, access to encrypted data	Content will be changed, risk that some data are lost

Handling of digital evidence

The next part of this topic was related to practical handling of digital evidence. Presented with five different types of digital evidence, e.g. an Apple iPhone X with a known lock code, they were asked in what order they would handle the evidence. They could choose from a predefined list of alternatives, where there were added some alternatives which is not forensically correct. After each evidence, there was an open-ended question asking the respondents why they choose to handle the evidence in the order they did.

3.1. Apple iPhone X with a known lock code

All six participants would take a picture of the iPhone, check time setting, enable flight mode and write down serial number/IMEI number. However, there was not a uniform approach to what order the handling should be done. None of the participants would turn the phone off or forward messages or e-mails directly from the phone. One participant would screenshot content using built functions of the seized phone.

Based on the six respondents answer, the highest ranked approach would be:

1. Take a picture of the phone (5/6)
2. Enable flight mode (3/6)
3. Check time settings and write down serial number (2/6)
4. Acquire the phone using tools like Cellebrite/XRY (3/6)
5. Manual review of the phones content (2/6)

The approach has not been written further, as the next options only had one vote each.

Note: The options to enable flight mode and write down serial number in column four has not been included in the highest ranked approach as step four. The reason is that both options were higher ranked higher up in the approach, and they could not be used twice.

As can be seen from Table 36, there were variations in how the participants would handle the iPhone starting from the second action.

TABLE 36. PRACTICAL TEST: HANDLING OF AN APPLE IPHONE X WITH KNOWN LOCK CODE

	1	2	3	4	5	6	7	8	9	10	11	N
Take a picture of the phone	**5**	1	0	0	0	0	0	0	0	0	0	6
Turn the phone off	0	0	0	0	0	0	0	0	0	0	0	0
Check time settings on the phone	0	2	**2**	1	1	0	0	0	0	0	0	6
Enable flight mode	0	**3**	1	**2**	0	0	0	0	0	0	0	6
Manual review of the phone's content	0	0	0	0	0	**2**	1	0	0	0	0	3
Forward messages to your service telephone	0	0	0	0	0	0	0	0	0	0	0	0
Forward e-mails to an e-mail that you control	0	0	0	0	0	0	0	0	0	0	0	0
Screenshots of content using the built in functions on the seized phone	0	0	0	0	0	0	0	1	0	0	0	1
Write down serial number/IMEI number	0	0	**2**	**2**	0	1	1	0	0	0	0	6
Acquire the phone using tools like Cellebrite/XRY	0	0	0	1	**3**	1	0	0	0	0	0	5
Bag and tag the phone and hand over to competent personell for acquisition	1	0	1	0	2	0	1	0	0	0	0	5

3.2 Samsung Galaxy S6 where the lock code is unknown, and the phone is locked

Five of six participants would take a picture of the Samsung, write down the serial number/ IMEI number and tag the phone before it was turned over to competent personell. Only one participant would turn the phone off. None of the participants would forward messages or e-mail or screenshot using the built in function.

Based on the six respondents answer, the highest ranked approach would be:

1. Take a picture of the phone (5/6)
2. Enable flight mode (3/6)
3. Check time settings (2/6)
4. Write down serial number/IMEI number (4/6)
5. Aquire the phone with tools like Cellebrite/XRY (2/6)

The approach has not been written further, as the next options only had one vote each.

As can be seen from Table 37, there were variations in how the participants would handle the Samsung starting from the second action.

TABLE 37. PRACTICAL TEST: HANDLING OF A LOCKED SAMSUNG GALAXY S6 WITH UNKNOWN LOCK CODE

	1	2	3	4	5	6	7	8	9	10	11	N
Take a picture of the phone	**5**	0	0	0	0	0	0	0	0	0	0	5
Turn the phone off	0	1	0	0	0	0	0	0	0	0	0	1
Check time settings on the phone	0	1	**2**	0	0	1	0	0	0	0	0	4
Enable flight mode	0	**3**	1	0	0	0	0	0	0	0	0	4
Manual review of the phones content	0	0	0	0	1	1	0	0	0	0	0	2
Forward messages to your service telephone	0	0	0	0	0	0	0	0	0	0	0	0
Forward e-mails to a phone that you control	0	0	0	0	0	0	0	0	0	0	0	0
Screenshots of content using the built in functions on the seized phone	0	0	0	0	0	0	0	0	0	0	0	0
Write down serial number/IMEI number	0	0	1	**4**	0	0	0	0	0	0	0	5
Acquire the phone with tools like Cellebrite/XRY	0	0	1	0	**2**	1	0	0	0	0	0	4
Bag and tag the phone and hand over to competent personell for acquisition	1	1	0	1	1	0	1	0	0	0	0	5

3.3 Older MacBook Pro without screen saver, username and password are known

Five of six participants would consider their own competence as the first thing they did, and five of six would also document the evidence with photo, including active windows etc.

Based on the six respondents answer, the highest ranked approach would be:

1. Consider own competence (5/6)
2. Call a colleague from a computer crime unit for assistance (3/6)
3. Check for active encryption/document the evidence with photo, active windows etc. (2/6)
4. Acquire RAM (2/6)
5. Copy relevant files to external hard drive (2/6)

The approach has not been written further, as the next options only had one vote each.

Note: The option *Check for active encryption* has been put in third place for the highest ranked approach even though the option had equal number of votes as *Acquire RAM* as the fourth task. The reason is that the participants were asked to rank in what order they would handle the evidence, and *Check for active encryption* shared the third place with documentation of the evidence, and therefore was prioritised higher than acquisition of RAM.

As can be seen from Table 38, there were variations in how the participants would handle the MacBook Pro starting from the second action.

TABLE 38. PRACTICAL TEST: HANDLING OF AN OLDER MACBOOK PRO, USERNAME AND PASSWORD ARE KNOWN

	1	2	3	4	5	6	7	8	9	10	11	12	N
Turn the device off	0	0	0	0	0	0	0	0	1	0	0	0	1
Remove the battery	0	0	0	0	0	1	0	1	0	0	0	0	2
Check for active encryption	0	0	**2**	**2**	0	0	0	0	0	0	0	0	4
Copy relevant files to external hard drive	0	0	0	0	**2**	0	1	0	0	0	0	0	3
Send relevant files from the laptop using e-mail	0	0	0	0	0	0	0	0	0	0	0	0	0
Check time settings	0	2	0	1	0	0	1	0	0	0	0	0	4
Acquire RAM	0	0	0	**2**	1	0	0	1	0	0	0	0	4
Call a colleague from a computer crime unit (DPA) for assistance	0	**3**	0	0	0	0	0	0	0	0	0	0	3
Consider your own competence	**5**	0	0	0	0	0	0	0	0	0	0	0	5
Turn off encryption if present	0	0	0	0	1	1	0	0	0	0	0	0	2
Bag and tag the computer and hand over to competent personell for acquisition	0	0	1	0	1	0	0	0	1	0	0	0	3
Document the evidence with photo, active windows etc.	1	1	**2**	0	0	1	0	0	0	0	0	0	5

3.4 Hewlett Packard stationary PC with Windows 10 Pro, admin credentials available

Four of six participants would consider their own competency before they handled the device. None of the participants would turn the computer off normally.

Based on the six respondents answer, the highest ranked approach would be:

1. Consider own competence (4/6)
2. Call a colleague from the computer crime unit for assistance (2/6)
3. Document the evidence with photo, active windows etc (2/6)

The approach has not been written further, as the next options only had one vote each.

As can be seen from Table 39, there were variations in how the participants would handle the Hewlett Packard starting from the second action.

TABLE 39. PRACTICAL TEST: HANDLING OF HEWLETT PACKARD STATIONARY PC W10, ADMIN CREDENTIALS KNOWN

	1	2	3	4	5	6	7	8	9	10	11	12	N
Turn off the device normally	0	0	0	0	0	0	0	0	0	0	0	0	0
Check for active encryption	0	0	1	1	0	0	0	0	0	0	0	0	2
Copy relevant files to external hard drive	0	0	0	1	0	0	1	0	0	0	0	0	2
Send relevant files from the computer using e-mail	0	0	0	0	0	0	0	0	0	0	0	0	0
Check time settings	0	1	0	1	0	0	0	0	0	0	0	0	2
Acquire RAM	0	0	0	0	1	1	0	0	0	0	0	0	2
Call a colleague from the computer crime unit (DPA) for assistance	0	**2**	0	0	0	0	0	0	0	0	0	0	2
Consider your own competence	**4**	0	0	0	0	0	0	0	0	0	0	0	4
Turn off any encryption	0	0	0	0	1	1	0	0	0	0	0	0	2
Turn off the device by removing the power cable	0	0	0	0	0	0	1	1	0	0	0	0	2
Bag and tag the computer and hand over to competent personell for acquisition	0	0	0	0	1	0	0	1	1	0	0	0	3
Document the evidence with photo, active windows etc.	0	1	**2**	0	0	0	0	0	0	0	0	0	3

Faced with a Dell server running Windows 2012, four of six participants would first consider their own competence. After that, two of six would document the evidence with photo while two would call a colleague from the computer crime unit for assistance. One participant would turn off the device normally, and one would turn off the device by removing the power cord.

Based on the six respondents answer, the highest ranked approach would be:

1. Consider your own competence
2. Document the evidence with photo / call a colleague from the computer crime unit

The approach has not been written further, as the next options only had one vote each.

As can be seen from Table 40, there were variations in how the participants would handle the Dell server starting from the second action.

TABLE 40. PRACTICAL TEST: HANDLING OF DELL SERVER WITH WINDOWS 2012, ADMIN CREDENTIALS KNOWN

	1	2	3	4	5	6	7	8	9	10	11	12	N
Turn the device off normally	0	0	0	0	0	0	0	1	0	0	0	0	1
Check for active encryption	0	0	1	1	0	0	0	0	0	0	0	0	2
Copy relevant files to an external hard drive	0	0	0	1	0	0	1	0	0	0	0	0	2
Send relevant files from the device using e-mail	0	0	0	0	0	0	0	0	0	0	0	0	0
Document the evidence with photo, active windows etc.	0	**2**	1	0	0	0	0	0	0	0	0	0	3
Check time settings	0	0	1	1	0	0	0	0	0	0	0	0	2
Acquire RAM	0	0	0	0	1	1	0	0	0	0	0	0	2
Call a colleague from the computer crime unit (DPA) for assistance	0	**2**	0	0	0	0	0	0	0	0	0	0	2
Consider your own competence	**4**	0	0	0	0	0	0	0	0	0	0	0	4
Turn off any encryption	0	0	0	0	1	1	0	0	0	0	0	0	2
Turn off the device by removing the power cable	0	0	0	0	0	0	1	0	0	0	0	0	1
Bag and tag the server and hand over to competent personell for acquisition	0	0	0	0	1	0	0	0	1	0	0	0	2

Topic 3, Part Two - Practical acquisition

The last part in this topic was practical, and actual, acquisition. After being provided with a username and password to three different social media accounts, namely Gmail, Facebook and Instagram, the participants were asked to acquire them using a defined method.

When several people across the country try to access an online account, there might be security measures in place from the content provider that prevent them to access the account. To give the participants a real opportunity to complete the test even if they experienced problems with accessing the account due to above-mentioned security measures, a Word-document containing already acquired content were attached the question. The participants were asked if they managed to download the content. They could answer yes or no. They could also answer that they encountered technical difficulties, and that the content from the Word-document was used. Using a practical approach, the participants skills on the *application* level could be assessed.

Those who answered they managed to acquire the content, or that they had encountered technical difficulties, were asked theoretical questions which could only be answered by examining the acquired content. Examination, or exploring data, is somewhat outside the

scope for this thesis, but was still added to the practical test as it can be a natural next step of competency after the content has been acquired. As the practical test was intended to be a proof of concept of digital competency certification, it was unnatural to omit the examination part.

Acquisition of Google, Facebook and Instagram account
Five participants completed the following questions. The participants were provided usernames and passwords belonging to three different test accounts. The accounts were from Google, Facebook and Instagram. It was specified that they should acquire the Google account using the Takeout function. After they acquired the Facebook account they were asked how they acquired it.

Two of the five participants answered on each account that they managed to acquire them. One participant answered on each account that s/he had encountered technical difficulties and had used the attached Word document that contained already acquired material. Two participants answered on each account that they did not know how to acquire the accounts.

Those who answered they managed to acquire the account, or that they had technical difficulties, were asked questions from the acquired data. The participants provided correct answers in all the questions except in two questions. One participant answered the serial number instead of the model name for the device. One participant answered «*None*» when asked which application the Facebook account was associated with.

The questions asked assessed the participants in several things, and on different levels in Bloom's Taxonomy of learning pyramid. They had to utilise what they remembered and understood about each of the three social media platforms, and master that knowledge, in order to apply it to an actual acquisition. When asked what the MD5 hash value[28] of the profile picture in the Instagram acquisition was, the participants had to remember what an MD5 hash value is, and they had to understand how an MD5 hash value is created. Finally, they had to have enough knowledge and understanding to create said hash value using the profile picture.

Application is the highest level that will be covered in this thesis. There were also questions which required use of other knowledge and skills from digital investigation. When asked what encryption tool the account user had search for, they had to have sufficient knowledge about encryption tools to recognise that it had been searched for Truecrypt. This is knowledge on the lowest level, the *remembering* level.

TABLE 41. PRACTICAL TEST: RESULTS FROM QUESTIONS BASED ON EXAMINATION OF ACQUIRED DATA

Google acquisition			
Question	**Correct answer**	**No. of correct answers**	**Source file**
What brand is the device used when creating the Google account?	*Huawei*	3	*Device-3906668817941716909.html*
Which model name is the device?	*CLT-L29*	2	*Device-3906668817941716909.html*
What is the IMEI for the device?	*866264047026922*	3	*Device-3906668817941716909.html*
The account user has searched for an encryption tool - which tool?	*Truecrypt*	3	*My Activity.html*

[28] A hash value is a checksum which can be used to verify data integrity, MD5 is one of several variants

Facebook acquisition			
Question	**Correct answer**	**No. of correct answers**	**Source file**
Briefly explain how you acquired the Facebook account	*Facebook archive, with or without detailed explaination*	3	N/A
What is the personal numeric ID for this account?	*100035112526357*	3	*profile_information/ profile_information.html*
There is a picture of an American football player; what is the number the player has on his jersey?	*21*	3	*photos_and_videos/ your_photos.html*
What year is Linda Hansen born (in the format 19**)?	*1986*	3	*profile_information/ profile_information.html*
Based on earlier logins, what kind of computer brand has Linda most likely used when accessing Facebook?	*Apple*	3	*security_and_login_information/ account_activity.html)*
Which application is this Facebook account associated with?	*Instagram*	2	*apps_and_websites/ apps_and_websites.html*
During your investigation you find the IP address 92.220.22.13. Which Internet Service Provider does this IP belong to?	*Altibox*	3	*security_and_login_information/ used_ip_addresses.html)*
Instagram acquisition			
Question	**Correct answer**	**No. of correct answers**	**Source file**
What is the MD5 hash of the profile picture?	*bb70beb20c3dade970437d53995236d8*	3	*profile/ 201903/098e710c2ecd3ead9588c5570f0310b9.jpg*
When did Linda Hansen join Instagram?	*2019-03-29T03:21:13*	3	*profile/profile.json*
Which celebrity has Linda followed since 2019-03-29T 03:21:27?	*justinbieber*	3	*profile/connections.json*

To assess what method the participants would acquire a video from YouTube, they were provided with an URL to a video and then asked to explain how they would acquire this video. The answer could be used to assess the *application* level of their skills and knowledge.

Two participants chose to use a Linux terminal and the program *youtube-dl*[29]. One participant did not specify *how* the video would be downloaded, and another answered that s/he had no knowledge of how to acquire the video. The two participants who either did not know how to acquire, or did not specify how to download the video, both answered they could record the video manually as an alternative. The last participant answered in detail. S/he would use the web service savieo.com to download the video, and thereafter generate hash value of the downloaded the video. This participant also mentioned *Hunchly*[30]. Hunchly is a tool that can be used for automatically capturing web pages when the pages are accessed.

In the next question they were asked to explain how they would acquire a forum post from a given forum thread in a way that it could be used in a police report. The answer could be used to assess the *application* level of their skills and knowledge.

[29] One version can be found here https://ytdl-org.github.io/youtube-dl/index.html. On an Ubuntu-based Linux distribution **$ sudo apt-get install youtube-dl** can be used.

[30] https://www.hunch.ly

Four participants would acquire the forum post using screenshot, and one would use a snipping tool. One of the participants who would acquire the post using screenshot would also acquire the post by saving the complete web page.

TABLE 42. PRACTICAL TEST: APPROACH TO ACQUIRE A YOUTUBE VIDEO

Participant #	Acquisition method
1	Linux terminal: youtube-dl https://www.youtube.com/watch?v=dQw4w9WgXcQ
2	Download the video, alternatively record the video with another device
3	No knowledge. Would alternatively take screenshots of the video, and record the video manually
4	1. Screenshot that documents a snapshot of the video, with URL, number of times played/likes and relevant comments 2. Use savieo.com, paste in the URL to the video and download 3. Generate hash value of the screenshot and video 4. Write a police report that documents the approach used, the result, used equipment (computer, IP, browser etc)
5	youtube-dl https://www.youtube.com/watch?v=dQw4w9WgXcQ and screenshot/Hunchly of the page

TABLE 43. PRACTICAL TEST: APPROACH TO ACQUIRE A FORUM POST

Participant #	Acquisition method
1	1. Copy URL https://forum.kvinneguiden.no/topic/1266744-hjeelp-wifi-funker-ikke-etter-jeg-slo-av-routeren/ 2. Screenshot. 3. Create a user on the forum and see if any more information about the user that wrote the forum post. 4. Check the source code and see if it was possible to download more information by altering the javascript on the site.
2	Do not know. Screenshot of the forum post.
3	Screenshot of the forum post.
4	1. Take a photo of the forum post with a snipping tool. 2. Generate a hash value from the photo. 3. Write a report that describe the approach, the result, used computer, IP etc.
5	1. Screenshot and «save page as». The source code might provide a date instead of just the day. Anonymous code might be used to find other posts from the same user. On some forums there was hash(ip). 2. Consider contacting the owner of the forum to get information about IP, browser and other information from logs.

The participants were presented with a picture[31] that contained EXIF-data. Using open-ended questions they were asked to answer what two specific EXIF-data fields contained. Lastly, they were asked which tool and method they used. The answers could be used to assess the *application* level of their skills and knowledge. In order to answer this question they had to *remember* what EXIF-data is. They also had to *understand* what EXIF-data is, and where it can be found.

Six participants answered these questions. Four participants correctly answered both questions, while two answered that they did not know. Of the four participants who were able to answer the questions, three had used either the program *exiftool* or the program *exif*. One participant right-clicked on the picture and showed details. It can be worth mentioning that if the last participant had used this approach using a Mac with the latest operating system, the «*Image Description*» would not be visible under picture information. The camera brand would be found using this approach.

[31] The picture can be found at http://www.opanda.com/en/pe/images/sample_001.jpg

TABLE 44. PRACTICAL TEST: FINDING EXIF-DATA FROM A PICTURE WITH METHOD USED

Question	Correct answer	No. of correct answers	No. of wrong answers
What is the «Image Description» for this picture?	*Door to the Soul*	4	2x «I do not know»
What camera brand is used to capture the image?	*Nikon*	4	2x «I do not know»
Method used			
Participant #1	wget http://www.opanda.com/en/pe/images/sample_001.jpg && exiftool sample_001.jpg		
Participant #2	Right-click on picture and show details		
Participant #3	Linux program exif v. 0.6.21		
Participant #4	wget and exiftool. Did not verify further.		

Using a provided Gmail e-mail address, the participants were asked to describe which step(s) they could take to find out who the owner of the e-mail address was. This was an open-ended question. All six participants answered they would contact Google and request basic subscriber information. Four participants also included that they would do initial investigative steps to find out more about the e-mail address. These steps included open source intelligence (OSINT); searching in open sources online with the address.

Regardless of what they had answered, the next question gave a pre-requisite that they had sent a request to the content provider asking for basic subscriber information. The content provider returned an IP address belonging to an ISP. The participants were asked an open-ended question about what they would do next. All six participants answered they would contact the ISP and request information about the IP address.

Again, regardless of what they answered they were given a pre-requisite that the ISP returned a name and address of the person who had the IP address at the time. They were also informed that there lived several people at the address. The participants were asked an open-ended question about what assessment(s) they should make before they suspected and arrested the person who was registered to have had the IP address. The intention of this question was to assess how the participants approached a situation, and how they evaluated the information they were given. It could also be necessary to imagine different hypotheses to answer this question sufficiently. A criminal case where the only information available is an IP address is not unusual. It requires that the police officers has knowledge of what an IP address is and its functionality. If they do not have knowledge about this, wrongfully arrests can happen.

One participant pointed out that it can be difficult to be certain of who in the household could be suspected, and s/he would seize all the equipment after acquiring the router. Another participant asked a rhetorical question if it is safe to send a pen pusher out in the field. I would argue that as long as the pen pusher has sufficiently training and competency, it would be rather safe. The other participants all include the need to establish who can be users of the device(s) related to the IP address. One participant, which I assume has a programming background, summarised his or hers assessment with «*IP != person*». In a way, that statement summarise the main intention behind this question. It is impossible to properly identify a person just by using an IP address and try to correlate this with the registered user of the IP address. Other investigative steps must be conducted to substantiate who the actual user was.

TABLE 45. PRACTICAL TEST: ASSESSMENT(S) BEFORE SUSPECTING THE REGISTERED USER OF THE IP ADDRESS

	Summary of assessment(s) given
Participant #1	Difficult to be certain of who in the household that can be suspected, all of the computer equipment should be seized. Router should be acquired live to map MAC-addresses and users to the time of the crime.
Participant #2	If it is safe to send a pen pusher out in the field.
Participant #3	Who uses the device connected to the IP address? Does anyone else has access to this device?
Participant #4	If anyone else can have used equipment connected to the IP address at the given time. The two adults can be registered on the address even though they do not actually live there and they might not have access to a computer there.
Participant #5	It has to be probable cause before someone is arrested. It has to be predominantly likely that it is Nicolay that has used the e-mail, and not any of the other three persons.
Participant #6	IP != person. Population register != who lives in the house.

The last question was an open-ended question asking the participants to give inputs or suggestions for improving the practical task. One participant suggested there could be added more questions regarding acquisition, processing of acquired data and analysis of acquired data from computers and/or mobile phones. Another feedback was that the test could be used as a background for an interview used to assess someones competency.

Summary of topic 3

The theoretical questions in topic 3 all yielded answers from the participants which could be used to assess the participants level of skills and knowledge for both the *remembering* and *understanding* level within digital investigation.

When tasked with prioritising in what order various digital should be handled, the respondents approach varied largely. The options with documenting the evidence with a photo and consider one's own competence were among those alternatives that were chosen most frequently. The results from this assignment can indicate that a uniform approach towards handling digital evidence might be necessary. A implementation of an overall standard operating procedure (SOP) for digital investigation methodology can be considered.

The practical acquisitions were completed by four of six participants. The two who did not complete the practical acquisition were likely to be the two participants chosen because they did not have digital investigation as one of their primary work tasks. The examination of the acquired data were completed by the four participants with only two wrong answers in total.

To download a video from YouTube the participants would use different approaches, from recording the movie using a camera to a Python program. This can indicate that a SOP should be developed and implemented to ensure that digital evidence from YouTube is acquired using an uniform approach.

Faced with acquisition of a forum post, most of the participants would acquire the post using a screen shot. Downloading the entire page was also suggested. Acquisition of forum posts can be relevant as a digital evidence, and also here a SOP should be developed and implemented.

Four of six participants managed to extract the EXIF-data from a given picture. The approach varied from right-clicking on the picture and show description to the Linux program exiftool.

During the last questions the participants were tasked to describe which steps they would take to identify a user of a Gmail address. The final question asked the participants which assessments they would do before they suspected and arrested the registered user of the IP

address. The answers from these questions, and the assessments provided in the last question, can indicate how much understanding the participant has about digital investigation and digital evidence. The answers could be used as *part* of a conversation before the police employee are certified to conduct digital investigation.

4.3 First responder skills and competency framework

Based on the process models and the ISO standard presented in chapter 2, a competency framework for first responder skills and competency can be used to illustrate the various skills and competence which can be relevant. Using a framework with core skills can help visualise how comprehensive the competence necessarily has to be if a general police officer should be able to handle a digital investigation, even from the initial phase. The field of digital investigation is constantly evolving, and it is important to emphasise the need for continuous revision and updating of the framework presented. Another aspect is the actual content in the different boxes. They are based on what *could* be relevant for different core skills, and are not meant to be exhaustive.

The framework does not contain recommended theoretical education. As stated earlier, this falls outside the scope of this thesis. The core skills *analysis of data* and *presentation of data* are also left blank, as they are to be determined on a later stage.

TABLE 46. FIRST RESPONDER SKILLS AND COMPETENCY FRAMEWORK

No	Core skills	Core skills description	Awareness/ Remembering (1)	Knowledge/ Understanding (2)	Skill/Applying (3)	Recommended theoretical education	Recommended practical training
1	**Formulate hypotheses**	Utilise hypotheses in an investigation to improve the overall quality	Familiar with the purpose of hypotheses in an investigaiton	Explain why hypotheses are important in an investigation	Formulate hypotheses, both from known and unknown information	Recommended, but not specified to what extent	E.g. paper exercises, discussion groups and other approaches
2a	**Identify, locate and handle data sources - at a crime scene**	Identify and handle digital devices using best practice grounded on theory	Investigative procedures at crime scene	Understand impact on volatile and non-volatile evidence	Identify network diagram and access controls mechanisms to understand dependencies	Recommended, but not specified to what extent	Real life scenarios under supervision of qualified instructor, discussion groups and other approaches
2b	**Identify and locate data sources - when receiving a complaint**	Properly identify and locate data sources that might be relevant for the criminal case	Familiar with basic data source locations, common social media platforms	Explain how the data sources can be relevant for a criminal case	Use the awareness and knowledge to ask sufficient follow-up questions to uncover relevant data sources	Recommended, but not specified to what extent	Scenario-based cases, discussion groups and other approaches
3a	**Acquisition of data - physical devices (at a crime scene)**	Aquire data from physical devices at a crime scene using appropriate methods and tools. Ability to conduct live forensics.	Describe the best method for acquisition to preserve maximum data related to the criminal case	Explain the acquisition process, understand pros and cons with various methods which can be applied	Acquire data based on Order of Volatility if needed, document evidence that cannot be acquired due to various constraints	Recommended, but not specified to what extent	Scenario-based cases, on-the-job training under supervision of qualified instructor and other approaches
3b	**Acquisition of data - physical devices (in lab)**	Aquire data from physical devices in a lab environment using appropriate methods and tools. Ability to conduct live forensics.	Describe the best method for acquisition to preserve maximum data related to the criminal case	Explain the acquisition process, understand pros and cons with various methods which can be applied	Acquire data based on Order of Volatility if needed, document evidence that cannot be acquired due to various constraints	Recommended, but not specified to what extent	Scenario-based cases, on-the-job training under supervision of qualified instructor and other approaches

No	Core skills	Core skills description	Awareness/ Remembering (1)	Knowledge/ Understanding (2)	Skill/Applying (3)	Recommended theoretical education	Recommended practical training
3c	**Acquisition of data - online**	Aquire data from the Internet.	Describe the best method for acquisition to preserve maximum data related to the criminal case	Explain the acquisition process, understand pros and cons with various methods which can be applied	Acquire data based on Order of Volatility if needed, document evidence that cannot be acquired due to various constraints	Recommended, but not specified to what extent	Scenario-based cases, on-the-job training under supervision of qualified instructor and other approaches
4	**Examination/ exploration of data**	Examine data from an acquisition using appropriate tools, ability to produce reports which are approved for court	Identify the best suited approach for examination based on the data material in question	Understand limitations in various tools, and the necessity for peer reviews/dual tool verification	Present findings from an examination, and argue why they are deemed to be relevant (and true)	Recommended, but not specified to what extent	Scenario-based cases, on-the-job training under supervision of qualified instructor and other approaches
5	**Analysis of data**	TBD	TBD	TBD	TBD	TBD	TBD
6	**Presentation of data**	TBD	TBD	TBD	TBD	TBD	TBD
	(1) Awareness/ Remembering:	*Recognise and identify, ask when help needed*					
	(2) Knowledge/ Understanding:	*Formal training, working in team*		*ISO 27037*	*Awareness (1)*	*Knowledge (2)*	*Skill (3)*
	(3) Skill-proven experience/ Application:	*Work unsupervised, apply/ demonstrate, do without help*		*Bloom's taxonomy*	*Remembering*	*Understanding*	*Applying*

5. Summary of Findings and General Discussion

The research problem for this thesis was *How capable are the Norwegian Police to handle the initial phase of a digital investigation?.* This research problem was broken down into five research questions. A summary of the findings for question I - IV will be presented in this chapter, while question V will be covered in chapter 5.2.1.

I. What is the present status of the field of digital investigation in Norway?
II. What kind of digital forensics knowledge are the police student taught at the Norwegian Police University College?
III. Are there any requirements for doing digital forensics and digital investigation? If yes, what are they?
IV. How competent does an investigator feel when met with digital evidence during an investigation?
V. What can be done to further improve the competency level?

The research conducted to answer these questions has included literature review of official reports and academic theses. The curriculum from the Norwegian Police University College has been reviewed and categorised. A survey was designed to let police officers self-assess how competent they perceive themselves when faced with digital evidence. Finally, a practical test has been designed, and tested, to propose a proof of concept for a tool which can be used as part of a certification process for police employees who will work with digital evidence and digital investigation. Based of the research conducted, the following has been identified:

I. *What is the present status of the field of digital investigation in Norway?*

The importance of digital competence has been announced several years ago, but the implementation is slow

The implications that arose when the police started policing to the Internet, including the need for the police districts to plan more work towards digital forensics tasks, was highlighted in Marit Gjerde's master thesis in 2007. Four years later, in 2011, a working group created by POD and the Attorney General wrote a report which was completed in 2012. The working group states that data seizures normally is done by the police generalists, but that *far from all* has the competency to do this correct. Furthermore, they point out that the police generalist has a need for basic competence about technology and the possibilities and challenges which technology has when fighting crime. A new working group who wrote a report in 2017 stated that «*anyone who is going to work with the police's core tasks must therefore have a basic understanding of how computers, computer systems, and computer networks function.*».

When reviewing the thesis and the two reports, it can be concluded that several independent parties, with experienced professionals within the field of digital investigation, have announced that digital competence is important for the police. It can also be concluded that the Norwegian Police are slow to implement measures which could rapidly increase the digital investigation competence level for the police employees.

One reason the Norwegian Police are slow to implement competence improving measures, can be due to the Norwegian Police being an organisation which contains elements of hierarchy and bureaucracy. A organisation that contains these elements can be governed by processes which renders rapid changes impossible. Instead changes must go through several stages of approval, where each stage can take a long time.

II. *What kind of digital forensics knowledge are the police student taught at the Norwegian Police University College?*

The field of digital investigation has had an increasing focus from the Norwegian Police University College

For the students who graduated in 2011 or earlier, the only curriculum which included digital evidence and digital investigation was a specialisation course they could attend in their last bachelor year. This course was limited to 48 students, meaning not every student would be able to attend this course.

For the bachelor students who graduated from the Norwegian Police University College in 2012 and later, there was an increase in focus on digital evidence and digital investigation in the curriculum. In addition to the specialisation course, each student had digital evidence as one of several subjects included in the course «*Investigation*».

The real increase started with the students who started in 2016 and graduated in 2019. They had digital evidence and digital investigation on their curriculum throughout all three years of the bachelor education. These student received a total of ten credits in the courses «*Digital Policing and Investigation».* For the students graduating in 2021 the same amount of credits is included in the curriculum.

III. *Are there any requirements for doing digital forensics and digital investigation? If yes, what are they?*

No requirements for conducting digital investigation

There are no specific requirements related to competence for police generalists who will investigate criminal cases where digital evidence is present. There are no specific competence requirements for a police generalist who will handle digital evidence. POD has stated that these tasks should only be carried out by personnel with «*adequate training*» and «*appropriate competence*», but the meaning of these terms has not been outlined and defined.

A police generalist who graduated before PHS implemented digital evidence in the curriculum can, in the utmost consequence, be tasked to investigate criminal cases which has an abundance of digital evidence without having any digital competence. The generalist can be lead by a chief investigator who also does not have any knowledge about digital evidence, at least not any formal competence.

On one side there are no stated requirements for investigating digital evidence and handling digital evidence, and on the other side it is stated that no personnel should perform these tasks without sufficient training and sufficient competence. This paradox with requiring sufficient training and sufficient competence without defining what the training and competence is actually comprised of, underlines the importance of addressing this issue as soon as possible.

IV. *How competent does an investigator feel when met with digital evidence during an investigation?*

Deficiencies in knowledge and skills towards technology and digital investigation

Faced with various technology and concepts from digital investigation, the results from the survey indicate deficiencies in all technology and concepts presented. Two examples of concepts and technologies where the majority answered they did not have the knowledge or no skills at all is digital currency like Bitcoin and Ransomware. The answers also indicate there are major deficiencies in the competency for live data forensics. With user-friendly encryption tools easily available, initial digital investigation on live evidence might be a task which a police generalist should be able to perform.

Major deficiencies in knowledge when it comes to reviewing digital evidence with forensic tools

The findings from the survey indicate the general knowledge related to reviewing evidence with the forensics tools Griffeye Analyze, Internet Evidence Finder, Cellebrite Physical Analyser/ Reader and XRY reader are low or absent. Only the minority of the respondents assessed they were competent or very competent in using these tools to review digital evidence.

V. Other findings

Based on the findings from this thesis, it emerged additional topics outside the research questions which is worth mentioning. The topics were related to training, verification and the reported number of criminal cases that contains an element of digital evidence.

Shortcomings in how digital investigation training is conducted in the police districts
The survey yielded answers which indicate that training sessions where the delivery method is informal training with a colleague is used. Training where the delivery method is a practical approach with learning by doing, is also used. These forms of delivery method for training, or transfer of competence, can fortify misunderstandings and eventually appear as truths. Therefore they should as a minimum be grounded with a degree of relevant theory to ensure the receiver of the competence has sufficient background knowledge to actually understand what happens when they puts practice into action.

Missing procedures for verification before presenting evidence in court
Over half of the respondents who have testified in court with digital evidence did not verify their findings with someone else before they testified. This can indicate a system weakness in the Norwegian police if digital evidence are not verified to determine the evidential value. The weakness can, in the utmost consequence, lead to miscarriage of justice if digital evidence with low, or even incorrect, evidential value are presented in court without verification.

The number of digital evidence present in criminal cases are potentially significantly higher than in the official reports
The reporting regime used by the Norwegian police might not be sufficient to register how widespread digital evidence is present in criminal cases. The official number of criminal cases with an ICT-related modus was 16.225 (5,1%) cases in 2018. The total number of reported offences in 2018 was 318.556. Findings in the survey can indicate the number of criminal cases which has digital evidence present is potentially significantly higher. 51,5% respondents in the survey answered that in the last three (3) cases they worked on/were involved in, there was at least one potential digital evidence present in all the three cases.

The compulsory annual training omits an important target group
The compulsory annual training (OÅO) has included digital investigation as a topic in 2019, but the target group is only investigators and chief investigators. The police officers who have patrol duty as one of their main tasks are omitted from the annual training. These officers often are the first ones to face digital evidence on a crime scene, and they should have the same competence and understanding as investigators.

Findings from the survey indicates that almost 50% of the respondents has no knowledge of the Order of Volatility (how volatile digital evidence are - in what order should they be acquired). This topic was covered in OÅO spring 2019, before and while the survey was active. On reason can be that the respondents had not yet completed OÅO. Another reason why many respondents did not have any knowledge might be because the learning outcome for the lesson was low. A third reason can be that the respondents were not part of the compulsory annual training, and thus did not have any prerequisites to know what the Order of Volatility is.

5.1 Reflections on own work and method use

The Austrian poet Ernest Fischer once said «*as machines become more and more efficient and perfect, so it will become clear that imperfection is the greatness of man*». No thesis is flawless and this thesis is no exception. While writing and analysing the results from the survey and practical test several areas of improvement were observed.

Both the survey and the practical test should have been further quality assured to detect and remove poor design. One lesson learned the hard way was how the results from the practical test was presented in QuestBack. The results from the question where the participants were

asked to rank in which order they would handle evidence, gave no possibility to see what each participant had answered in what order. If a trial of the analysis had been conducted prior to publishing the test, this should have been observed and another approach could have been used.

In retrospect, long processing time for an approval for conducting a survey on employees in a government agency should have been foreseen. If the application had been sent in August instead of November, there could have been more time to conduct deeper analysis of the results from the survey.

Theory about learning is an area of research which could have been researched even further, as this area is fundamental for both designing and implementing measures to assess and increase competence. Looking back, adding more from this research area is one topic this thesis could have benefited from.

5.1.1 Future work on a personal level

If this thesis is well received, I want to immerse myself in the theory of learning and further use this to be a resource to help increase the digital competence in Norwegian police.

5.2 Implications for the Norwegian police

In this thesis it has been found that digital competence is important for investigating criminal cases where digital evidence is present. The top management of the Norwegian police, POD, should have been aware of this based on the reports produced from the working groups in 2012 and 2017. The working group created in 2011 was tasked to survey how the police worked with ICT-crime, digital evidence and how they policed the Internet. The other working group was tasked to write about the capacity and competence need for the next ten years to come. However, implementation of measures to ensure the digital competence is raised for every police employee seems to be belated. One example on how this is belated is the missing requirements for doing digital investigation set by POD. The national role requirements and descriptions could have been used to establish concrete requirements for employees who would either investigate digital evidence or somehow come in contact with digital evidence.

PHS has taken measures, and have included digital investigation as a separate course for the bachelor students. This is definitely a step in the right direction, but a plan to ensure the police officers that graduated *before* PHS included digital investigation on the curriculum also receives fundamental digital competence seems to be missing. PHS offers various post graduate studies within digital investigation, and in theory every police officer can obtain more competence if they desire it. However, being digital competent as a police officer should maybe not be voluntary in 2019. Perhaps it should be required, and of course facilitated, that every police employee attended a post graduate study adapted to the tasks they can face everyday.

One of the pitfalls with not actively working towards increasing the digital competence in the Norwegian police, is that the investigative quality will suffer. A police officer who is not digital competent will most likely not be able to ask the right question when receiving a complaint and the police report will be of insufficient quality. A police report which lacks vital information lays a poor foundation for further investigation. Furthermore, the lack of competence or competence acquired by informal training by a colleague can lead to digital evidence being interpreted wrong. If no system is set in place for verification of evidence, wrongly interpreted evidence can, in the utmost consequence, lead to miscarriage of justice where innocent

individuals are wrongfully imprisoned. Every police officer is most likely expected to be able to collect fingerprints from a crime scene, as well as collecting traces of DNA. It can now be appropriate to point out that time is ripe to enable the Norwegian police officers to identify potential digital evidence and acquire them.

The short-term goals for the Norwegian police towards 2020 presented in chapter 2.3.5 can be mentioned again.

In 2020, the Norwegian police will:

- investigate and process criminal cases according to standards and expectations, comply with process requirements and have good notoriety
- implement and prioritise the right investigative efforts with competent employees as early as possible (in the initial phase) in criminal cases
- have the necessary capacity, technical and police expertise centrally and locally, for secure storage, sharing and analysis of digital evidence and digital information

To achieve these short-term goals, an increased focus on competence-raising measures is needed. Work on these measures should begin as soon as possible to achieve the goals within 2020. In the next section possible approaches towards reaching the goals is proposed.

5.2.1 Future work at the system level

Based on the research question related to what can be done to further improve the competence level, and the findings in this thesis, there are approaches which can be suggested to be researched further or looked closer at.

Establish a system for registration of how widespread digital evidence is in criminal cases

In order to understand how relevant digital evidence is for the Norwegian police, a system can be established to learn the real extent of digital evidence. If digital evidence is present in almost every criminal case, this could be an incentive to increase the basic competence among those who investigates the criminal cases.

National survey to assess competence

To get an overview of digital competence among the Norwegian police officers, a national survey can be developed and conducted. This survey can be designed to include both theoretical questions, as well as practical tasks related to digital investigation and handling of digital evidence.

Create a framework with defined requirements for employees who will either investigate or come in touch with digital evidence

A framework with defined requirements facilitate efforts to create a program for national learning and training. It can also ensure that only employees who meet the requirements are tasked to investigate criminal cases with digital evidence present. The training competency framework on cybercrime presented in chapter 2.4 could be benefical to include in this framework, as well as elements from the ISO standard presented in chapter 2.5.3.

Development of program(s) for national learning and training with certification(s)
A program for national learning and training can lead to a more equal police service when it comes to investigation of criminal cases that has digital evidence present. A certification ensures that the employees who are certified has a certain degree of digital competence. This can also act as a safeguard to better avoid miscarriage of justice.

Implementation of standard operating procedures (SOP)
The results from the practical test indicates a need for SOP's for both handling of digital evidence and acquisition of forum posts and videos from the Internet. It is recommended that SOP's are developed and implemented for all police employees.

Further development of the practical test
A practical test, as the proof of concept test in this thesis, can be used to allow the investigators to demonstrate their skills and competency. OÅO can be used a delivery method to maintain digital skills and competency on a theoretical level, but it is still recommended that a practical approach is included in the training.

Implementation of a verification system for digital evidence
To ensure that evidence which is presented in court is reliable and have a high evidential value, peer review or a form for verification are needed. Evidence which has only been verified by one person should be avoided. Implementation of measures to require peer review and verification of digital evidence is recommended. One approach could be to require verification from at least one other competent person before digital evidence is allowed to be presented in court.

Develop/purchase application-based solutions for first responders
There are commercial solutions available that provides first responders with a sort of encyclopaedia. One example is Evolve[32] from Blue Lights Digital. The first responders can get updated information about various devices and how they should handle them. They also have a live chat where first responders can inquire specialised personell if they face challenges that are not covered by the application. A working commercial product can be bought and integrated into the standard police equipment, or a similar solution could be designed from scratch.

Collaborate with International actors who address digital competency
The Norwegian Police are most likely not the only organisation that has a need for digital competency among their employees. There are other actors where collaboration might be fruitful, the Netherland Forensic Institute being one of them.

[32] https://bluelightsdigital.com/products/evolve/

Bibliography

1. Andersen, S. (2019) *Technical Report: A preliminary Process Model for Investigation*. Available at: https://doi.org/10.31235/osf.io/z4wma.
2. Årnes, A. (2016) *Digital forensics*. Fall 2016 edn. NTNU, Gjøvik.
3. Cambridge Dictionary *HYPOTHESIS | meaning in the Cambridge English Dictionary*. dictionary.cambridge.org. Available at: https://dictionary.cambridge.org/dictionary/english/hypothesis (Accessed: 30th of May 2019).
4. CEPOL et al. (2018) *Training Competency Framework on Cybercrime*.
5. College of Policing (2017) *Forensics*. Available at: https://www.app.college.police.uk/app-content/investigations/forensics/ (Accessed: 1st of May 2019).
6. Direktoratet for Forvaltning og IKT (2017) *Om lønnssystemet i staten | Arbeidsgiverportalen*. Available at: https://arbeidsgiver.difi.no/lonn-goder-og-reise/om-lonnssystemet-i-staten (Accessed: 29th of April 2019).
7. Furnell, S., Emm, D. and Papadaki, M. (2015) The challenge of measuring cyber-dependent crimes, *Computer Fraud & Security*, 2015(10), pp. 5-12. doi: 10.1016/S1361-3723(15)30093-2.
8. Gjerde, M. (2007) *Victims of success? Knowledge discovery amongst digital forensic investigators in the Norwegian police districts*. Minor thesis, University College Dublin.
9. Gogus, A. (2012) Bloom's Taxonomy of Learning Objectives (pp. 469-473).
10. Grøtan, E. M. (2019) *Fagkontakters rolle innenfor etterforskning av elektroniske spor.* Bachelor, Politihøgskolen.
11. Hondrelis F.N; Ingwersen J.R (2018) *Digitalt politiarbeid: Teoretisk oppgave.* Bachelor, Politihøgskolen.
12. Innst. 306 S (2014-2015) *Endringer i politiloven mv. (trygghet i hverdagen - nærpolitireformen)* Stortinget: Justiskomiteen.
13. International Organization of Standardization (2012) Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence - ISO/IEC 27037.
14. Justis- og beredskapsdepartementet (2018) *Fakta om nærpolitireformen - regjeringen.no*. Available at: https://www.regjeringen.no/no/tema/lov-og-rett/kriminalitet-og-politi/innsikt/narpolitireformen/fakta-om-narpolitireformen/id2398894/ (Accessed: 7th of February 2019).
15. KarriereStart.no *2. gangs utlysning - Vi søker etter politioverbetjent - etterforsker innen datakriminalitet og digitalt politiarbeid ved Felles enhet for etterretning og etterforskning.* Available at: https://karrierestart.no/ledig-stilling/1112845 (Accessed: 22nd of April 2019).
16. Leedy, P. D. and Ormrod, J. E. (2015) *Practical research : planning and design.* 11th ed. edn. Boston: Pearson.
17. Lystad et al. (2017) *Politi- og lensmannsetatens kapasitets- og kompetansebehov de kommende ti-årene*. Oslo: Politidirektoratet. Available at: https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/bemanning-ressurser-og-dekningsgrad/bemanning-og-dekningsgrad/politi--og-lensmannsetatens-kapasitets--og-kompetansebehov-de-kommende-ti-arene.pdf (Accessed: 21st of April 2019).
18. Politidirektoratet (2016) *Handlingsplan for løft av etterforskningsfeltet*. Available at: https://www.politiet.no/globalassets/05-om-oss/03-strategier-og-planer/handlingsplan-for-loft-av-etterforskningsfeltet.pdf (Accessed: 7th of May 2019).

19. Politidirektoratet (2017) *Politiet mot 2025*. Available at: https://www.politiet.no/globalassets/05-om-oss/03-strategier-og-planer/politiet-mot-2025---politiets-virksomhetsstrategi.pdf (Accessed: 15th of May 2019).
20. Politidirektoratet (2018) *Nasjonale rolledefinisjoner med kompetansekrav - etterforskningsfeltet v0.7*. Available at: https://www.politilederen.no/dokumenter/POD/Nasjonale%20rollebeskrivelser%20med%20kompetansekrav%20v0.7.pdf (Accessed: 29th of April 2019).
21. Politidirektoratet (2019) *Nasjonale rolledefinisjoner med kompetansekrav - etterforskningsfeltet. v1.0 not published. V0.7 can be found at https://www.politilederen.no/dokumenter/POD/Nasjonale%20rollebeskrivelser%20med%20kompetansekrav%20v0.7.pdf. Not published. Available at: V0.7 https://www.politilederen.no/dokumenter/POD/Nasjonale%20rollebeskrivelser%20med%20kompetansekrav%20v0.7.pdf.*
22. Politiet (2018) *STRASAK-rapporten - Anmeldt kriminalitet og politiets straffesaksbehandling 2018*. www.politiet.no: Politiet. Available at: https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/strasak/2018/strasak-2018.pdf (Accessed: 15th of May 2019).
23. Politiet.no (2019) *Politiet.no - Bemanning og dekningsgrad*. Available at: https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/bemanning-ressurser-og-dekningsgrad/bemanning-og-dekningsgrad/arsverk-pr-ar-pr-maned.xlsx (Accessed: 7th of February 2019).
24. Politihøgskolen (2012) *Fagplan for Bachelorstudiet BI Studieåret 2012/2013*. Available at: https://www.phs.no/Documents/5_Studenter/Fagplaner/Fagplan%20B1%202012-2013.pdf (Accessed: 23rd of April 2019).
25. Politihøgskolen (2014) *Fagplan for Bachelorstudiet BIII Studieåret 2014/2015*. Available at: https://www.phs.no/Documents/5_Studenter/Fagplaner/Fagplan%20B3%202014-2015.pdf (Accessed: 23rd of April 2019).
26. Politihøgskolen (2016) *Fagplan Bachelor - Politiudanning 2016-2019*. Available at: https://www.phs.no/Documents/5_Studenter/Fagplaner/Fagplan%202016-2019.pdf (Accessed: 23rd of April 2019).
27. Politihøgskolen (2017) *Studieplan videreutdanning i etterforskning*. Available at: https://www.phs.no/Documents/2_Studietilbud/3_EVU/Studieplan%20Videreutdanning%20i%20etterforskning%20VEF.pdf?epslanguage=no (Accessed: 29th of April 2019).
28. Politihøgskolen (2018) *Fagplan Bachelor - Politiutdanning 2018-2021*. Available at: https://www.phs.no/Documents/5_Studenter/Fagplaner/Fagplan%202018-2021.pdf (Accessed: 23rd of April 2019).
29. Politiregisterloven (2010) *Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)*. www.lovdata.no: Justis- og beredskapsdepartementet. Available at: https://lovdata.no/dokument/NL/lov/2010-05-28-16?q=politiregisterloven (Accessed: 6th of May 2019).
30. Rachlew, A. (2009) *Justisfeil ved politiets etterforskning - noen eksempler og forskningsbaserte mottiltak*, Universitetet i Oslo. Available at: https://www.duo.uio.no/bitstream/handle/10852/22587/Rachlew_avhandling.pdf?sequence (Accessed: 29th of April 2019).
31. Romerikes Blad (2018) *Romerikes Blad - Mann i 20 årene tiltalt for overgrep mot over 300 mindreårige gutter*. Available at: https://www.rb.no/nyheter/nedre-romerike-tingrett/overgrep/mann-i-20-arene-tiltalt-for-overgrep-mot-over-300-mindrearige-gutter/s/5-43-920691 (Accessed: 1st of May 2019).

32. Schlösser, T. *et al.* (2013) How unaware are the unskilled? Empirical tests of the "signal extraction" counterexplanation for the Dunning-Kruger effect in self-evaluation of performance, *Journal of Economic Psychology*, 39, pp. 85.
33. Storruste et al. (2012) *Politiet i det digitale samfunnet: en arbeidsgrupperapport om elektroniske spor, IKT-kriminalitet og politiarbeid på internett*. Oslo: Politidirektoratet. Available at: https://medlem.ntl.no/Content/103500/cache=20122109105334/Politiet%20i%20det%20digitale%20samfunn%20juli%2012.pdf (Accessed: 21st of April 2019).
34. Straffeprosessloven - strpl (1981, last changed 2018) *Lov om rettergangsmåten i straffesaker (Straffeprosessloven)*. www.lovdata.no: Justis- og beredskapsdepartementet. Available at: https://lovdata.no/dokument/NL/lov/1981-05-22-25?q=straffeprosessloven (Accessed: 10th of February 2019).
35. Sunde, N. (2017) *Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation*, Politihøgskolen / NTNU.
36. TechTerms *Digital Footprint Definition*. Available at: https://techterms.com/definition/digital_footprint (Accessed: 10th of February 2019).
37. Verizon (2019) *2019 Data Breach Investigations Report*. Available at: https://enterprise.verizon.com/resources/reports/dbir/ (Accessed: 18th of May 2019).

Appendices

Appendix 1: List of figures and tables

Appendix 2: Terminology

5WH
To fulfil the requirements of the Criminal Procedure Act §226 it is common to seek answers to the basic questions known as 5WH defined by (Stelfox, 2013) referred to by Årnes (Årnes, 2016, p. 19). 5WH defines the objectives of an investigation as determining *Who* was involved, *Where* did it happen, *What* happened, *When* did it happen, *Why* did it happen and *How* did it happen. Answer to these questions can be imperative to conduct a proper investigation.

Chain of Custody
The documentation of evidence acquisition, control, analysis and disposition of physical and electronic evidence (Årnes, 2016). Serves as a way to insure that evidence has not been tampered with or altered.

Competence
Andersen (2019) defines competence as «*knowledge to understand a certain subject and the skills to perform a particular action*». Digital competence uses the same definition, but is used to emphasise that the competence is related to the digital sphere.

Computer Crime Units (CCUs)
Each police district has dedicated personnel working full-time with digital forensics. Depending on the size of the CCU they may investigate own cases and/or focus primarily on giving technical support to other units. After the Norwegian police went through a reform, «*Nærpolitireformen*», which started 1st of January 2016 (Justis- og beredskapsdepartementet, 2018), there are now twelve local CCUs in Norway.

Digital evidence
Årnes (2016) defines digital evidence as «*any digital data that contains reliable information which can support or refute a hypothesis of an incident or crime*». This definition is based on a definition by Carrier (2004).

Digital forensics
The NPCC Digital Forensics portfolio board (College of Policing, 2017) has defined digital forensics as «*the application of science to the identification, collection, examination and analysis of electronic data whilst preserving the integrity of the information and maintaining the chain of custody of that data*».

Digital investigation
In this thesis digital investigation is defined as conducting traditional investigation to fulfil the purpose with investigation in accordance with the Criminal Procedure Act, but with electronic data and information (digital evidence).

Evidence integrity
The goal in digital forensics is to preserve the evidence in its original form (Årnes, 2016). Ideally an independent third party should be able to reproduce the exact same result as you have done using another approach and/or setup that you used.

Forensically sound
When methods and approach have followed digital forensics principles and process the result (and process as a whole) will be defined as forensically sound (Årnes, 2016).

Hypothesis
«*An idea or explanation for something that is based on known facts but has not yet been proven*» (Cambridge Dictionary).

ICT-crime
Crime related to Information and Communications technology. An obsolete, or at least a vague, definition about crime that has a various element of digital aspect present. A more updated definition divides into two; cyber-dependent and cyber-enabled crimes (Furnell, Emm and Papadaki, 2015). Cyber-dependent crimes rely on a computer, a computer network or other forms of Information and Communications technology. Examples can be DDoS-attacks and Ransomware. The other crime type is cyber-enabled. This can be conventional crime like fraud, only that the delivery method is on a computer. Cyber-enabled crime has a greater reach when utilising computers, but the crime type itself can also be done in the analogue world.

Initial phase of a digital investigation
In this thesis the initial phase starts with an incident and ends when evidence is acquired. The next phase is examination or exploration of the evidence.

Investigation
The Norwegian Criminal Procedure Act (Straffeprosessloven - strpl) states that the the purpose of an investigation is to gather necessary information to decide the issue of indictment, to serve as a preparation for the court's consideration of the issue of criminal liability and, possibly, the question of the determination of reaction, to avert or stop criminal offences or to execute punishment and other reactions.

Order of Volatility
Order of Volatility can be defined as «*the prioritization of the potential evidence source to be collected according to the volatility of the data*» (Årnes, 2016). RAM is normally more volatile than a traditional hard drive, and if the principle with Order of Volatility is to be followed RAM should be acquired before the hard drive.

Police generalist
Police officers that either has patrol duty or non-specialised investigations as their primary work tasks.

Police specialist
A police officer that has specialised work tasks, for example a computer forensics investigator or a police officer that only works with illegal immigrants.

Appendix 3: E-mail to leaders of Computer Crime Units

Fra: Odin Heitmann
Sendt: 25. oktober 2018 10:18
Til: -
Kopi: -
Emne: Enkel kartlegging DPA ifm masteroppgave

Hei!

Jeg tar en erfaringsbasert master på NTNU/PHS, og nå har tiden kommet for masteroppgaven. Temaet jeg ønsker å belyse er norsk politi sin kompetanse på digital etterforskning. Fokuset vil være hvor kompetente "vanlige" etterforskere er når det kommer til håndtering av digitale spor i sin etterforskning.

Tenker det vil være naturlig å nevne kapasiteten til spesialistene innenfor digitalt politiarbeid for å kunne si noe om spisskompetansen som finnes i distriktene. I den forbindelse håper jeg at dere kan hjelpe meg med svar på følgende spørsmål:

1. Hvor mange ansatte er det ved DPA i ditt distrikt?
2. Hvilken bakgrunn har de ansatte? (Antall sivile/politi)
3. Hvor lenge har de jobbet med digital etterforskning/digitalt politiarbeid?
4. Hvilken formalkompetanse har de ansatte? (NCFI moduler, verktøykurs, sertifiseringer, andre kurs/ utdanninger innenfor fagfeltet)

Det kan godt hende jeg kommer tilbake med flere spørsmål underveis, men foreløpig er det disse fire spørsmålene jeg skulle hatt svar på.

I løpet av 2018/starten av 2019 vil jeg sende ut en spørreundersøkelse til samtlige politiansatte i Norge der jeg prøver å kartlegge opplevd kompetanse på digital etterforskning. Hvis noen av dere har lyst til å se gjennom spørreundersøkelsen før den sendes ut for å gi tilbakemeldinger er det bare å gi lyd!

Jeg vet dere alle har en hektisk hverdag, men jeg håper dere får tatt dere tiden til å svare ut spørsmålene over. Hvis jeg lander oppgaven på en god måte kan den forhåpentligvis bidra til økt fokus på digital kompetanse i politiet, noe som vil komme oss alle til gode.

Innspill mottas med takk!

Odin Heitmann
Politioverbetjent

Appendix 4: Approval from the Norwegian Centre for Research Data for conducting survey

NSD NORSK SENTER FOR FORSKNINGSDATA

NSD sin vurdering

Prosjekttittel

Digital Investigation: How capable are the Norwegian Police to handle technology when investigating criminal cases

Referansenummer

852360

Registrert

28.11.2018 av Odin Heitmann - odinhe@stud.ntnu.no

Behandlingsansvarlig institusjon

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

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Katrin Franke, katrin.franke@ntnu.no, tlf: [redacted]

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Odin Heitmann, odinhe@stud.ntnu.no, tlf: [redacted]

Prosjektperiode

08.11.2018 - 01.06.2019

Status

21.01.2019 - Vurdert

Vurdering (1)

21.01.2019 - Vurdert

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 21.01.2019. Behandlingen kan starte.

MELD ENDRINGER
Dersom behandlingen av personopplysninger endrer seg, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. På våre nettsider informerer vi om hvilke endringer som må meldes. Vent på svar før endringer gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 01.06.2019.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).

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

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

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

Dersom du benytter en databehandler i prosjektet må behandlingen oppfylle kravene til bruk av databehandler, jf. art 28 og 29.

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

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

Lykke til med prosjektet!
Tlf. Personverntjenester: 55 58 21 17 (tast 1)

Appendix 5: Approval from the Norwegian Police Directorate for conducting survey

POLITIET
POLITIDIREKTORATET

Odin Heitmann
[redacted]

NATIONAL POLICE DIRECTORATE

Deres referanse:	Vår referanse:	Sted, Dato
	201805105-11 053	Oslo, 11.04.2019

SØKNAD OM FRITAK FRA TAUSHETSPLIKT - MASTEROPPGAVE - NORSK POLITI OG DIGITAL KOMPETANSE - PHS - ODIN HEITMANN

Politidirektoratet viser til søknad av 28.11.2018 og utfyllende oversendelse samt etterfølgende epostutveksling og telefonisk kontakt. Direktoratet beklager at gjennomsnittlig saksbehandlingstid for enkeltsaker for tiden er 6 måneder.

Det vises til at søker for tiden tar en erfaringsbasert master i informasjonssikkerhet ved PHS/NTNU.

Veileder for forskningsprosjektet er Katrin Franke ved NTNU. Forskervilkåret om førstestillingskompetanse er med dette oppfylt.

Fra søknaden hitsettes:

> *"Temaet for masteroppgaven min er «Digital Forensics Investigation: How capable are the Norwegian Police to handle technology when investigating criminal cases." Det jeg ønsker å undersøke er hvor god digital kompetanse norsk politi har, og jeg ønsker å fokusere på vanlige polititjenestepersoner – ikke de som primært har en rolle som dataetterforsker. Tilnærmingen til kartlegging av kompetansenivået til norsk politi vil være en spørreundersøkelse som sendes til de politiansatte der de blir spurt om hvordan de selv opplever sin kompetanse. I tillegg til spørreundersøkelsen vil jeg kartlegge eventuelle kompetansekrav til digital etterforskning og hva slags digital kompetanse studentene har fått/får på Politihøgskolen."*

Det opplyses at spørreundersøkelsen vil bli meldt til NSD. Det vises i sin helhet til søknaden.

* * *

Politidirektoratet har vurdert saken etter reglene for innsyn i person- og saksopplysninger, jf. politiregisterloven § 23 første ledd samt i forhold til politiets operative virksomhet og organiseringen av dette og sikkerhetsmessige aspektet m.v. i politiregisterloven § 23 andre ledd, jf. § 33.

Politidirektoratet

Post: Postboks 8051 Dep., 0031 Oslo
Besøk: Fridtjof Nansens vei 14/16
Tlf: 23 36 41 00
Faks: 23 36 42 96
E-post: politidirektoratet@politiet.no
Org. nr.: 982 531 950 mva
Giro:
www.politi.no

"§ 23.Omfanget av taushetsplikten
Enhver som er ansatt i eller utfører tjeneste eller arbeid for politiet eller påtalemyndigheten, plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om

1. *noens personlige forhold, eller*
2. *tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den opplysningen angår.*

Taushetsplikten gjelder også for opplysninger som det ut fra hensynet til etterforskningen i den enkelte sak, hensynet til spanings- og etterretningsvirksomheten eller hensynet til politiets operative virksomhet og organiseringen av denne er nødvendig å holde hemmelig. Begrensningene i taushetsplikten i § 22 og §§ 24 til 34 kommer bare til anvendelse så langt de passer.

Taushetsplikten gjelder også etter at vedkommende har avsluttet tjenesten eller arbeidet. Opplysninger som nevnt i paragrafen her kan heller ikke utnyttes i egen virksomhet eller i tjeneste eller arbeid for andre.

Taushetsplikten gjelder også overfor andre i politiet og påtalemyndigheten, med mindre § 21 kommer til anvendelse.
For taushetsplikt i tilknytning til kommunikasjonskontroll gjelder straffeprosessloven kapittel 16a."

"§ 33. Taushetsplikt ved forskning
Når det finnes rimelig og ikke medfører uforholdsmessig ulempe for andre interesser, kan det bestemmes at opplysninger i det enkelte tilfelle gis til bruk for forskning, uten hinder av taushetsplikten i § 23.

I straffesaker treffes beslutning etter første ledd av riksadvokaten og for øvrig av Politidirektoratet, eller av Justisdepartementet for så vidt gjelder opplysninger i saker som behandles av Politiets sikkerhetstjeneste.
Bestemmelsene i forvaltningsloven § 13d annet og tredje ledd og § 13e kommer til anvendelse så langt de passer."

Politidirektoratet viser til at mastergradsstudenten ikke vil samle inn, lagre eller skrive ut personopplysninger, og at slik data dermed heller ikke skal registreres. Videre vises det til at prosjektet forutsettes å være samtykkebasert.

I de saker Politidirektoratet mener det klart kan gjøres unntak fra taushetsplikten er det ikke nødvendig med en rådsbehandling av søknaden, jf. forvaltningsforskriften § 9, 2. ledd. Politidirektoratet anser prosjektet for å ha en samfunnsnytte. Gitt det ovennevnte kan ikke Politidirektoratet se at det foreligger skranker for innsynskravet i forhold til § 23 første ledd.

Når det gjelder taushetsplikten etter § 23 andre ledd vil denne omfatte konkrete faktaopplysninger om samarbeid operativt/taktisk og beredskapsmessig som vil kunne avdekke forebyggende tiltak, planer og operative og taktiske innsatsmekanismer og løsninger. Dette er kritisk sensitiv informasjon som direktoratet ikke fritar fra taushetsplikten. Derimot når det gjelder mer generelle opplysninger om hvordan en samarbeider, planlegger, øver og liknende, hvilke samarbeidsparter som er relevante på hvilke områder osv, vil dette ikke være underlagt taushetsplikten og noe søkeren kan spørre og motta opplysninger om.

En frigivelse av informasjon kan medføre at politiet mister kontroll over informasjon som er av betydning for politiets evne til å løse sine oppdrag. Hvordan informasjon fra prosjektet skal håndteres og brukes helt konkret vil således være av stor betydning for politiet.

Når det gjelder sensitivitet til opplysningene som vil inngå i forskningsprosjektet antas disse ikke å være sikkerhetsgradert etter sikkerhetsloven. Det gis under ingen omstendighet innsyn i sikkerhetsgradert informasjon.

Politidirektoratet er av beredskapsmessige hensyn meget restriktiv med hensyn til å frigi taushetsbelagt informasjon som er taushetsbelagt av politioperative grunner, særlig når det gjelder politiets oppdragsløsning, taktikk mv. Hvor et viktig spørsmål også er om frigivelse av informasjon kan medføre at politiet mister kontroll over informasjon som er av betydning for politiets evne til å løse sine oppdrag. Det gis ikke innsyn i opplysninger som direkte kan skade politiets arbeid. Prosjektet er blitt forelagt KRIPOS v/Nasjonalt Cyberkrimsenter som har uttalt at de opplysningene som kartlegges i seg selv ikke er av en slik karakter at de er nødvendige å holde hemmelige.

Politidirektoratet finner det etter dette politifaglig formålstjenlig å innvilge søknaden. Samtidig som det opparbeides empiri og kunnskap vedrørende problemstillingen er det også grunn til å anta at resultatene kan ha verdi for norsk politi.

* * *

Direktoratet tar forbehold om NSDs vurdering av saken.

Direktoratet vil presisere at søker også selv underveis må vurdere egne funn opp mot bestemmelsen, og kontakte direktoratet dersom det er uklart om noen av opplysningene som blir gitt vil kunne komme i strid med bestemmelsen og/eller tillatelsen. Det bes også om at søker kontakter Politidirektoratet før publisering ved tvil om oppgaven inneholder informasjon som ikke er godkjent utlevert.

Det er Politidirektoratets vurdering at søker etter dette kan gis adgang til å gjennomføre prosjektet på de vilkår som er satt i nærværende brev, jf. ovenfor og nedenfor, samt med de kvantitative og praktiske begrensningene som er foretatt av Politidirektoratet forut for godkjenningen i samarbeid med søker.

Politidirektoratets samtykke er videre betinget av at gjennomføringen av prosjektet skjer uten overlevering av taushetsbelagt persondata til søker og uten nedtegning av personopplysninger fra observasjoner. Videre forutsetter Politidirektoratet at all innsamling, oppbevaring og bruk av opplysninger skjer på en faglig forsvarlig måte, og at det ikke finnes personidentifiserende opplysninger, eller eventuelle sikkerhetsmessige og beredskapsmessige opplysninger, i det publiserte materialet. Søker og andre som får tilgang til opplysningene må undertegne en taushetserklæring. Det vises ellers til reglene om forskeres taushetsplikt, jf. forvaltningsloven § 13 e.

Videre er samtykket betinget av at alle respondentene samt ledere gjøres kjent med det nærværende brev og dets vilkår. Deltakelse i spørreundersøkelsen skjer etter samtykke fra ledelsen i distriktet samt samtykke fra respondentene (frivillighet).

Direktoratet forutsetter at innsynet legges opp på en slik måte at alle involverte er bevisst på skrankene for taushetsplikten ved besvarelse av spørsmålene tilknyttet undersøkelsen.

Til slutt ber direktoratet om å motta en kopi av ferdig produkt.

Med hilsen

Heidi Toward
Seniorrådgiver

Appendix 6: Information letter presented to respondents of survey

Odin Heitmann

Fra: Odin Heitmann
Sendt: 25. april 2019 10:56
Til: [redacted]
Emne: Spørreundersøkelse om digital kompetanse i politiet
Vedlegg: Fritaksbrev taushetsplikt Politidirektoratet.pdf

Vil du delta i forskningsprosjektet

"Digital Investigation: How capable are the Norwegian Police to handle technology when investigating criminal cases"?

Kjære kollega med politiutdanning!

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å kartlegge kompetansen til norsk politi innenfor digital
etterforskning. Dette skal blant annet besvares ved å kartlegge hvordan politiet selv opplever sin kompetanse innenfor digital etterforskning. I
dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Kort om studenten
Jeg heter Odin Heitmann, og til daglig er jeg ansatt i Kripos. Tidligere har jeg jobbet som lensmannsbetjent og som dataetterforsker i Øst
politidistrikt. Jeg tar nå en erfaringsbasert master i informasjonssikkerhet ved Norges teknisk-naturvitenskapelige universitet (NTNU). Dette studiet
er et samarbeid mellom Politihøgskolen og NTNU, og studieretningen jeg går omhandler digital forensics og etterforskning av cybercrime. I
forbindelse med studiet skriver jeg en masteroppgave som i hovedsak baserer seg på dette prosjektet.

Formål
Formålet med prosjektet er som nevnt over å kartlegge kompetansen til norsk politi innenfor digital etterforskning. Prosjektet er en selvstendig
masteroppgave som resulterer i en oppgave som tilsvarer 30 studiepoeng.
Problemstillinger som vil bli forsøkt besvart i oppgaven er blant annet:

- Hvor kompetente er norsk politi når det kommer til digital etterforskning?
- Stilles det krav til grunnleggende kompetanse for å drive med digital etterforskning?
- Hvis ja, hva er kravene?
- Hvilke utfordringer finnes innenfor digital etterforskning og er det mulig å møte disse utfordringene uten å være en spesialist innenfor digital etterforskning?

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

Hvorfor får du spørsmål om å delta?
For å kunne besvare hvordan politiet selv opplever sin kompetanse innenfor digitale etterforskning er jeg avhengig av å få besvarelser fra
personer som har politiutdanning og som jobber i politiet i dag. Utvalget er trukket ved at tre politidistrikter i Norge ble valgt ut basert på størrelse.
Det var ønskelig at det ble brukt et stort, et mellomstort og et lite politidistrikt. Basert på antall årsverk per 30.09.18 ble politidistriktene Øst,
Trøndelag og Møre og Romsdal valgt ut. Samtlige politiansatte i disse distriktene får spørsmål om å delta i prosjektet ved at distribusjonslistene
for e-post for disse politidistriktene blir benyttet for å nå alle ansatte. Totalt vil ca. 2200 få tilbud om å delta. Spørreundersøkelsen er godkjent sendt ut av politimester i ditt distrikt.

Hva innebærer det for deg å delta?
Hvis du velger å delta i prosjektet, innebærer det at du fyller ut et digitalt spørreskjema. Det vil ta deg ca. 10-15 minutter. Spørreskjemaet inneholder blant annet spørsmål om dine digitale vaner og caser der du må ta stilling til hvor kompetent du anser deg selv. Dine svar fra spørreskjemaet blir registrert elektronisk.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Rent praktisk
lukker du den digitale spørreundersøkelsen for å trekke tilbake samtykket. Svarene dine vil ikke bli lagret hvis du avslutter spørreundersøkelsen ved å lukke vinduet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med
personvernregelverket. Det er kun student som vil ha tilgang til datamaterialet.

Undersøkelsen gjennomføres på en slik måte at vi ikke vil få anledning til å se hvem som har svart, så sant du ikke selv skriver identifiserende
informasjon der det er felt for fritekst. Alle besvarelser som ligger hos spørreskjemaleverandør (QuestBack) vil slettes når prosjektet er ferdig.
Resultatene vil samlet sett bli tilgjengelig i masteroppgaven, men uten at det vil være mulig å knytte besvarelser til enkeltpersoner.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Prosjektet skal etter planen avsluttes 1. juni 2019, og alle data slettes innen prosjektslutt.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:
• innsyn i hvilke personopplysninger som er registrert om deg,
• å få rettet personopplysninger om deg,
• få slettet personopplysninger om deg,
• få utlevert en kopi av dine personopplysninger (dataportabilitet), og
• å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke. På oppdrag fra *Norges teknisk-naturvitenskapelige universitet (NTNU)* har
NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:
Norges teknisk-naturvitenskapelige universitet (NTNU) ved *Katrin Franke, på e-post katrin.franke@ntnu.no*.
Vårt personvernombud: *Thomas Helgesen, på e-post thomas.helgesen@ntnu.no*
NSD – Norsk senter for forskningsdata AS, på epost (personvernombudet@nsd.no) eller telefon: 55 58 21 17.

Ved å trykke på linken under samtykker du til å delta i spørreundersøkelsen. Husk at samtykke når som helst kan trekkes tilbake
ved å lukke spørreundersøkelsen.

Merk: Politidirektoratet har gitt fritak fra taushetsplikt. Det er viktig at du leser, og forstår, vedlagt "Fritaksbrev taushetsplikt Politidirektoratet.pdf".

https://response.questback.com/odinheitmann/digitalkompetanse

På forhånd tusen takk!

Med vennlig hilsen,
Odin Heitmann

Appendix 7: Survey design

Note: This is the English version. The respondents were presented a Norwegian version.

Digital forensics skills for police employees

Hello, and thank you for taking time to answer this survey!

The aim for the thesis is to map how competent Norwegian police officers feel they are when investigating criminal cases that have an element of digital evidence in them.

The survey will take approximately 10-15 minutes to complete. The questions vary from questions about your digital habits to scenario-based questions where you must decide how competent you consider yourself.

Again, thank you for taking time to answer this survey!

Your identity will be hidden.

When hidden identity is used in surveys, no identifiable information, such as browser type and version, internet IP address, operating system, or e-mail address, will be stored with the answer. This is to protect the respondent's identity.

How old are you?

Select... Select...

Gender

Select... Select...

When did you graduate from the Norwegian Police University College (PHS)?

Select... Select...

How long have you been employed in the Norwegian Police in total?

Select... Select...

In which police district are you employed?

Select... Select...

The next question is about what role that most identify your daily tasks. Please read through the definitions listed under and choose the role that is most describing.

Definitions of roles:

Investigator, general investigation, (investigation at a police station, burglary, violence cases etc)

Investigator, specialised investigation, (specialised investigation of child abuse, human trafficking, illegal immigrants, organised crime etc)

Crime prevention, (online police patrol, youth crime prevention etc)

Computer Forensics Investigator, (your daily tasks are in a computer crime unit like Digital Police Work)

Patrol duty, (your main task is doing ordinary patrol duty)

Manager, (management of personell conducting investigation or personell on patrol duty)

Operations center, (operational leder, communications operator etc)

Prosecutor, (Police lawyer etc)

Civilian duty, (issue of passports, weapons applications etc)

Which one best describe your current role?

Select... Select...

Next >>

Information technology: The use of computers to store, retrieve, transmit, manipulate and present data and information.

Do you have any earlier education within Information Technology obtained before you started at the Norwegian Police College University or before you started working in the Norwegian Police?

○ Yes ○ No

Next >>

What kind of Information Technology education did you finish starting at the Norwegian Police College University or before your started working in the Norwegian Police?

Please list the education(s) here.

34/4000

Next >>

This section is about your education and/or training within digital forensics investigation

Formal education: Attendance at a college or university that leads to credits (studiepoeng)

Have you completed any formal education within Information Technology or Computer Forensics after you graduated from the Norwegian Police College University or after you started working in the Norwegian Police?

○ Yes ○ No

Next >>

Which formal Information Technology or Computer Forensics education(s) have you completed?

- ☐ PHS: Nordic Computer Forensics Investigator: Module 1 (5 credits)
- ☐ PHS: Nordic Computer Forensics Investigator: Module 2 (25 credits)
- ☐ PHS: Nordic Computer Forensics Investigator: Core (15 credits)
- ☐ PHS: Nordic Computer Forensics Investigator: 2A - Advanced Computer Forensics (10 credits)
- ☐ PHS: Nordic Computer Forensics Investigator: 3A - Forensic Tool Development (10 credits)
- ☐ PHS: Nordic Computer Forensics Investigator: 3B - Linux Artifacts (10 credits)
- ☐ PHS: Nordic Computer Forensics Investigator: 3C - Open Source Forensics (10 credits)
- ☐ PHS: Nordic Computer Forensics Investigator: 3D - Macintosh Computer Forensics (10 credits)
- ☐ PHS: Nordic Computer Forensics Investigator: 3E - Windows Forensics (10 credits)
- ☐ Other

Next >>

Which other Information Technology or Computer Forensics education(s) have you completed after graduating from the Norwegian Police University college or after you started working in the Norwegian Police?

Please list the education(s) here.

34/4000

Next >>

Training: Workshop or internal training that might lead to certificate of competence (kompetanse-/kursbevis), but not necessarily. This also includes informal training from a colleague, e.g. a colleague that shows you how to review acquired evidence in an analysis programme like Griffeye or Internet Evidence Finder/Axiom.

Training in digital forensics can be: How to properly seize digital evidence like cell phones and computers, how to acquire cell phones, acquire social media accounts like Facebook and Instagram, review acquired evidence in an analysis programme etc.

Have you completed any training within digital forensics after you graduated from the Norwegian Police University College or after you started working in the Norwegian Police?

○ Yes ○ No

Next >>

Please select what you have received training for:

- ☐ Acquisition of mobile units using XRY products (from MSAB)
- ☐ Acquisition of mobile units using Cellebrite products
- ☐ Acquisition of hard drives from computers using write-blocker and software like FTK Imager
- ☐ Professional contact for digital police work (fagkontakt)
- ☐ Open Source Intelligence (OSINT)
- ☐ Social media acquisition, e.g. "My Archive" from Facebook
- ☐ Review of evidence using Griffeye
- ☐ Review of evidence using Internet Evidence Finder/Axiom
- ☐ Review of evidence using Cellebrite Reader/Cellebrite Physical Analyser
- ☐ Other

Next >>

What kind of other training within digital forensics have you had after you graduated from the Norwegian Police University College or after you started working in the Norwegian Police?

Please list what kind of training you have received here:

57/4000

Next >>

Theoretical lessons: An organised lecture with one or more instructors with a written agenda, not an instructor answering questions on the go. If you have participated in more than one training session, select the option(s) that cover the sessions you have attended.

What did the training include?

- ☐ Only practical approach (learning by doing)
- ☐ Informal practical training with a colleague
- ☐ Only theoretical lesson(s)
- ☐ Combined theoretical lesson(s) with a practical approach
- ☐ Other

Next >>

Digital habits and skills

This section is about your digital habits and skills.

Do you have an account on a social media?

○ Yes ○ No ○ Prefer not to say

Next >>

Which social media(s) do you have an account on?

- [ ] Facebook
- [ ] Facebook Messenger
- [ ] Google
- [ ] WhatsApp
- [ ] Instagram
- [ ] Twitter
- [ ] Telegram
- [ ] Discord
- [ ] Signal
- [ ] Snapchat
- [ ] Other

Next >>

Which other social media(s) do you have an account on?

Please list other social media(s) here.

39/4000

Next >>

Smart phone definition: A mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded apps.

Do you have a smart phone?

- ◯ Yes
- ◯ No

Next >>

Online activities: Social media like Facebook, news sites like VG and Dagbladet, gaming, market places like FINN.no etc.

How many hours per day on average do you use for online activities?

- ◯ 0
- ◯ 1-2
- ◯ 3-4
- ◯ 5 or more

Next >>

How would you rate your competency when it comes to determining if a link or an attachment in an e-mail is safe to click or not?

- ◯ Very poor
- ◯ Poor
- ◯ Fair
- ◯ Good
- ◯ Very good

Next >>

How much experience do you have with the following?

	No experience	Very little experience	Little experience	Some experience	Much experience	Very much experience
Buy or sell items using Norwegian web sites (e.g. Finn.no)	○	○	○	○	○	○
Buy or sell items using non-Norwegian web sites (e.g. Amazon or eBay)	○	○	○	○	○	○
Buy digital currency like Bitcoin and Ethereum from exchanges, e.g. Kraken and Coinbase	○	○	○	○	○	○
Send or receive digital currency like Bitcoin and Ethereum using a digital wallet	○	○	○	○	○	○
VoIP (Voice over IP) calls like FaceTime, Skype and Messenger	○	○	○	○	○	○
Communicating with other people using applications like Telegram, WhatsApp and Skype etc	○	○	○	○	○	○
Using P2P (Peer to Peer) technology to download files, by using clients like LimeWire and BitTorrent	○	○	○	○	○	○
Create a new e-mail address from a site like Gmail and Yandex etc.	○	○	○	○	○	○

Next >>

Digital evidence: Cell phone, social media, computer, bank records, toll records, CCTV etc.

In the last three (3) criminal cases you worked on/were involved in, how many had at least one potential digital evidence present?

○ 0 ○ 1 ○ 2 ○ 3 ○ Unsure

○ Have not worked three criminal cases

Next >>

What kind of digital evidence was present in the case(s)?

○ Cell phone ○ Computer ○ Storage device ○ Social media

○ E-mail ○ CCTV ○ Other

Next >>

Scenario: Initial investigative steps

In the following scenarios the police report is written, and you are tasked to do, or order, initial digital investigative steps. Initial digital investigative steps can be location and preservation of evidence, send requests to third-party actors like Finn.no and ask for account information/basic subscriber information etc.

Please review the scenario details above. How would you rate your own skills when faced with:

	Not competent at all	Very little competent	Little competent	Competent	Very competent	Will never do, or order, investigative steps
The company that has experienced denial-of-service attacks	○	○	○	○	○	○
The young girl with the nude picture that has been distributed using a mobile app	○	○	○	○	○	○
The man that has his online bank account depleted of money	○	○	○	○	○	○
The elderly man that has been defrauded on FINN.no	○	○	○	○	○	○
The woman whose identity has been stolen	○	○	○	○	○	○
The man that was threatened with distribution of a video where he allegedly is watching pornography	○	○	○	○	○	○

Next >>

Familiarity with technology and digital forensics concepts

You will now be presented with technology and digital forensics concepts.

How would you rate your own skills and knowledge with the following:

	No knowledge/skills at all	Very little knowledge/skills	Little knowledge/skills	Some knowledge/skills	Much knowledge/skills	Very much knowledge/skills
E-mail acquisition	○	○	○	○	○	○
Crypto currencies, e.g. Bitcoin and Ethereum	○	○	○	○	○	○
Order of Volatility (how volatile digital evidence are - in what order should they be acquired)	○	○	○	○	○	○
Logical vs physical acquisition of devices	○	○	○	○	○	○
Finding an Internet Service Provider, e.g. Telenor, based on an IP address	○	○	○	○	○	○
Live data forensics (investigation on an actual evidence)	○	○	○	○	○	○
Computer network functionality	○	○	○	○	○	○
Ransomware	○	○	○	○	○	○
Why time zone settings can be crucial	○	○	○	○	○	○
Write and send a request to a content provider like Google, to get basic subscriber information (BSI)	○	○	○	○	○	○
Malware	○	○	○	○	○	○
Dark web	○	○	○	○	○	○
How the Internet works in theory	○	○	○	○	○	○
VPN (Virtual Private Network)	○	○	○	○	○	○

Next >>

How would you rate your knowledge when it comes to reviewing evidence with the following forensic tools:

	Not competent at all	Very little competent	Little competent	Competent	Very competent	Have never heard of
Griffeye Analyze	○	○	○	○	○	○
Internet Evidence Finder/Axiom	○	○	○	○	○	○
Cellebrite Physical Analyser/Reader	○	○	○	○	○	○
XRY reader	○	○	○	○	○	○

Next >>

Court testimony

This section deals with testimony in court, and your experience(s) when giving testimony.

Digital evidence here means every aspect of seizing and handling of digital units like cell phones or computers, social media, review/content analysis of evidence using tools like Griffeye and IEF/Axiom etc. or evidence given to you from a computer crime unit for review.

Have you in your career ever given testimony in court about digital evidence?

○ Yes

○ No

Next >>

How confident were you when you gave your testimony?

○ Not confident at all ○ Very little confident ○ Little confident

○ Confident ○ Very confident

If you have given more than one testimony, please briefly describe how you felt when you gave your testimonies

0/4000

Next >>

Did someone else verify your findings before you gave your testimony?

○ Yes, a colleague from a computer crime unit

○ Yes, another colleague that does not work at a computer crime unit

○ No

Next >>

Parties in court: Judge, jury, prosecutor and/or defence lawyer

Were your testimony questioned from the parties in court?

○ No questions asked ○ A few questions asked

○ Many questions asked

Next >>

Did you feel competent to answer the questions in a sufficient matter?

○ Yes ○ No

If you have given more than one testimony, and you have been questioned in more than one case, please briefly describe if you were able to answer questions or not.

0/4000

Next >>

Challenges and improvements

This section is about your thoughts about digital evidence and digital investigation.

In your opinion, what are the biggest challenge(s) with digital evidence and digital investigation?

0/4000

What can be done to further improve the competency level in digital investigation in the Norwegian Police?

0/4000

Send

100 % completed

Appendix 8: Information letter to the test group for the practical test

Mon 4/15/2019 10:51 PM

To:
Bcc:

Hei!

Jeg er i disse dager i gang med siste innspurt med masteroppgaven i informasjonssikkerhet ved NTNU/PHS. Temaet for oppgaven omhandler digital kompetanse i norsk politi.
Èn del av oppgaven tar for seg hvor kompetente politiet opplever seg selv i forbindelse med etterforskning av digitale spor. Dette gjøres ved en spørreundersøkelse som sendes ut rett over påske til alle ansatte i tre politidistrikt. En annen del av oppgaven vil foreslå en mulig tilnærming til en prøve eller test som kan brukes for å godkjenne etterforskere og patruljemannskap som skal jobbe med digital etterforskning i mindre eller større grad.

Den praktiske testen jeg har utviklet skal i første omgang testes på 10-15 personer og den **kan** få betydning for hvordan politiet jobber mot digital etterforskning i tiden fremover. Estimert tid på testen er 45 minutter - 1 time. Tid til gjennomføring vil variere stort med bakgrunn i erfaring.

Om deltakelse: Det er helt frivillig å delta, og du kan når som helst trekke deg ved å lukke vinduet som testen foregår i. Svarene dine er anonyme, og jeg vil ikke se hvem som har svart hva. Svarene vil bli oppbevart hos meg til utgangen av 2019, og svarene kan bli brukt til videre forskning enten i regi av PHS eller NTNU ut 2019.

Merk: Denne testen skal ikke spres til andre enn de som er mottakere av denne e-posten uten etter avtale med meg. Dette fordi det er ønskelig med et datagrunnlag som ikke overstiger 10-15 stykker.

Hvis du har lyst til å bidra kan du trykke på linken under:

https://response.questback.com/odinheitmann/practical_test

Ved spørsmål er det bare å ta kontakt!

Med vennlig hilsen,
Odin Heitmann
Masterstudent NTNU/PHS

Appendix 9: Practical test design

Note: This is the English version. The participants were presented a Norwegian version.

Practical test in digital investigation

https://cdn.pixabay.com/photo/2017/07/31/00/28/internet-2556091__480.jpg

Introduction

This practical test is part of a master's thesis at NTNU / PHS, which seeks to map the digital competence of police officers in the Norwegian police. The test has been developed as a proposal for how the police *can* test and approve employees who will investigate digital evidence at a generalist level.

The test contains both theoretical questions and practical tasks in securing digital evidence. It contains three main themes:

1. Hypotheses

2. Identification of digital evidence

3. Acquisition of data

Note: When it comes to securing Internet related evidence such as a Facebook profile, it may present certain challenges if the same profile is attempted to be downloaded several times from different IP addresses. In order for those who carry out the test to have a real opportunity to complete the test if the service offers problems, a Word document will be attached to relevant questions. The Word document contains a zip file with already acquired content. To get a most realistic response, I kindly ask that you:

1) Try to acquire the account according to the information in the assignment before you use the Word document.

2) Are honest and select the option that you do not know how the account is acquired if you do not know it.

The results of this test will be deleted at the end of 2019.

Thank you for taking the time to complete this test!

Kind regards,

Odin Heitmann

Your identity will be hidden.

When hidden identity is used in surveys, no identifiable information, such as browser type and version, internet IP address, operating system, or e-mail address, will be stored with the answer. This is to protect the respondent's identity.

Academia: Please select option "Akademia (NTNU/PHS)"

In which Police district are you employed?

Select... Select...

What year did you graduate from the Norwegian Police University College (PHS)?

Select... Select...

The next question is about what role that most identify your daily tasks. Please read through the definitions listed under and choose the role that is most describing.

Definitions of roles:

Investigator, general investigation, (investigation at a police station, burglary, violence cases etc)

Investigator, specialised investigation, (specialised investigation of child abuse, human trafficking, illegal immigrants, organised crime etc)

Crime prevention, (online police patrol, youth crime prevention etc)

Computer Forensics Investigator, (your daily tasks are in a computer crime unit like Digital Police Work)

Patrol duty, (your main task is doing ordinary patrol duty)

Manager, (management of personell conducting investigation or personell on patrol duty)

Operations center, (operational leder, communications operator etc)

Prosecutor, (Police lawyer etc)

Civilian duty, (issue of passports, weapons applications etc)

Academia, employee or student at a College or University

Which role best describe your current role?

Select... Select...

Are one of your primary work tasks investigating digital evidence?

◯ Yes ◯ No

Next >>

Topic 1: Hypotheses

You will now get three assignments where you will be presented with a scenario that contains some information. Then you will be asked which hypotheses you can make from the information you have. Finally, you will be asked which initial digital investigative steps you want to do and why you want to do these.

Scenario 1.1

https://images.unsplash.com/photo-1510503973075-f00509204da1?ixlib=rb-1.2.1&ixid=eyJhcHBfaWQiOjEyMDd9&auto=format&fit=crop&w=1950&q=80

Background

It is Monday April 1, 2019 and the rain is pouring down. Fortunately you have office duty inside a police station in the vicinity of Oslo. One of your tasks is to receive complaints and write down statements from the members of the public. Around 5:00 pm, 20-year old Linda enters the police station and arrives at the counter where you are sitting. She shows you a picture of a gun she has on her iPhone. Linda explains that she got this picture from her boyfriend Ronny around 14:00 the same day. The picture was sent without preamble and she says she hasn't talked to Ronny in a month. She believes Ronny sent the picture because they will meet in court next week in an ongoing child custody case. Now Linda is afraid of her life and she wants to report Ronny to have threatened her.

1.1 What hypothesis/theses can you make from the information above? Max 10.

Case 1.1 - Hypotheses 1	
Case 1.1 - Hypotheses 2	
Case 1.1 - Hypotheses 3	
Case 1.1 - Hypotheses 4	
Case 1.1 - Hypotheses 5	
Case 1.1 - Hypotheses 6	
Case 1.1 - Hypotheses 7	
Case 1.1 - Hypotheses 8	
Case 1.1 - Hypotheses 9	
Case 1.1 - Hypotheses 10	

Scenario 1.1 - Initial digital investigative steps

Limitations: Your job is complete when the police report is written and you have conducted initial digital investigative steps. For example, a digital investigative step can be to seize a harddrive or an e-mail account.

1.1 Which initial digital investigative steps would you like to conduct, and why?

Case 1.1 - 1. Investigative step	
Case 1.1 - 1. Purpose/reason	
Case 1.1 - 2. Investigative step	
Case 1.1 - 2. Purpose/reason	
Case 1.1 - 3. Investigative step	
Case 1.1 - 3. Purpose/reason	
Case 1.1 - 4. Investigative step	
Case 1.1 - 4. Purpose/reason	
Case 1.1 - 5. Investigative step	
Case 1.1 - 5. Purpose/reason	
Case 1.1 - 6. Investigative step	
Case 1.1 - 6. Purpose/reason	

Next >>

Scenario 1.2

https://cdn.pixabay.com/photo/2018/02/28/14/19/fraud-prevention-3188092_1280.jpg

Background

You're out on patrol. Together with your colleague you drive through Oslo city center on a Friday night. A man is frantically waving and it is clear that he wants you to stop. You go out of the car and the man says he was scammed when he was buying a MacBook Pro. He also says that he came in contact with the seller of the computer at Finn.no. They agreed that he would transfer NOK 10,000 in advance via bank transfer. The actual handover of the computer would happen at a McDonalds restaurant at 8pm tonight, but the seller never met. Now the man wants to report the fraud.

1.2 What hypothesis/theses can you make from the information above? Max 10.

Case 1.2 - Hypotheses 1	
Case 1.2 - Hypotheses 2	
Case 1.2 - Hypotheses 3	
Case 1.2 - Hypotheses 4	
Case 1.2 - Hypotheses 5	
Case 1.2 - Hypotheses 6	
Case 1.2 - Hypotheses 7	
Case 1.2 - Hypotheses 8	
Case 1.2 - Hypotheses 9	
Case 1.2 - Hypotheses 10	

Scenario 1.2 - Initial digital investigative steps

Prerequisites: You contact the operations center, and as there are plenty of patrols at work, you are instructed to carry out initial digital investigation steps.

1.2 Which initial digital investigative steps would you like to conduct, and why?

Case 1.2 - 1. Investigative step	
Case 1.2 - 1. Purpose/reason	
Case 1.2 - 2. Investigative step	
Case 1.2 - 2. Purpose/reason	
Case 1.2 - 3. Investigative step	
Case 1.2 - 3. Purpose/reason	
Case 1.2 - 4. Investigative step	
Case 1.2 - 4. Purpose/reason	
Case 1.2 - 5. Investigative step	
Case 1.2 - 5. Purpose/reason	
Case 1.2 - 6. Investigative step	
Case 1.2 - 6. Purpose/reason	

Next >>

Scenario 1.3

https://www.banenor.no/globalassets/documents/1-mapper-for-bildekarusell/1-stasjonsoversikt/hovedbanen/oslo-s/oslo-s6.jpg?preset=sixCol

Background

Oslo Central Station (Oslo S) is a busy area with thousands of travelers every day. Lately, there have been challenges with a criminal gang, consisting of young men, who are staying at Oslo S. The gang is known to rob people either inside Oslo S or in the immediate vicinity.

You work at the police station at Oslo S. It is Saturday around 13:00 and like always Oslo S is crowded with people. A young girl comes to the police station and tells you that a few minutes ago she saw that an elderly man was robbed by several young men in the main terminal, right by the information board.

When you arrive, you immediately see an elderly man standing alone and he appears confused. He repeatedly shouts "my iphone, it's gone .. it's gone".

1.3 What hypothesis/theses can you make from the information above? Max 10.

Case 1.3 - Hypothesis 1	
Case 1.3 - Hypothesis 2	
Case 1.3 - Hypothesis 3	
Case 1.3 - Hypothesis 4	
Case 1.3 - Hypothesis 5	
Case 1.3 - Hypothesis 6	
Case 1.3 - Hypothesis 7	
Case 1.3 - Hypothesis 8	
Case 1.3 - Hypothesis 9	
Case 1.3 - Hypothesis 10	

Scenario 1.3 - Initial digital investigative steps

Prerequisites: You contact the operations center, and they ask you to see what kind of digital evidence can be acquired. They also inform you that they will send a patrol to question any witnesses, but that you have full opportunity to ask witnesses for help / information if you need it.

1.1 Which initial digital investigative steps would you like to conduct, and why?

Case 1.3 - 1. Investigative step	
Case 1.3 - 1. Purpose/reason	
Case 1.3 - 2. Investigative step	
Case 1.3 - 2. Purpose/reason	
Case 1.3 - 3. Investigative step	
Case 1.3 - 3. Purpose/reason	
Case 1.3 - 4. Investigative step	
Case 1.3 - 4. Purpose/reason	
Case 1.3 - 5. Investigative step	
Case 1.3 - 5. Purpose/reason	
Case 1.3 - 6. Investigative step	
Case 1.3 - 6. Purpose/reason	

Tema 2: Identification of digital evidence

In this part of the test you will get theoretical questions that vary between multiple choice and free text.

What is the purpose of hypothesis thinking in an investigation?

0/4000

Next >>

ISP: Internet Service Provider. Company or Organization that provides Internet access, e.g. Telenor og Get.

What is the maximum number of days it is possible to identify who has used an IP address in Norway?

☐ 7 days ☐ 21 days ☐ 30 days ☐ Six months

☐ Varies from ISP to ISP

Next >>

Briefly describe what an IP address is and why it is important for you as a police employee to have knowledge of this.

0/4000

Next >>

Below is a list of various items. Select the items that you think might contain potential digital evidence and move them over to the empty square.

Select the items that you think might contain potential digital evidence.

- Notepad
- Car
- Mobile phone
- Hard drive
- Camera lens
- News paper
- Plant
- Cuddle toy
- Drugs
- Analog watch
- Playstation 4
- Water bottle
- Clothes
- Headphones
- SIM-card
- Power cable

Next >>

Scenario 2.1

https://cdn.pixabay.com/photo/2017/05/12/15/22/car-accident-2307383_1280.png

Background

A brand new Tesla model S has hit a pedestrian, and the pedestrian died after the collision. The driver of the Tesla has explained that the pedestrian jumped into the road. The only witness to what happened was explaining that the pedestrian walked normally on the road shoulder when he was hit.

If you find more than six potential digital evidence, answer with the six you think is most important.

What potential digital evidence can be found here, and what information can be extracted from the digital evidence?

2.1 - Digital evidence nr. 1	
2.1 - Potential information 1	
2.1 - Digital evidence nr. 2	
2.1 - Potential information 2	
2.1 - Digital evidence nr. 3	
2.1 - Potential information 3	
2.1 - Digital evidence nr. 4	
2.1 - Potential information 4	
2.1 - Digital evidence nr. 5	
2.1 - Potential information 5	
2.1 - Digital evidence nr. 6	
2.1 - Potential information 6	

Next >>

Topic 3: Acquisiton of digital evidence

https://cdn.pixabay.com/photo/2017/12/18/14/10/fbi-3026206_1280.jpg

In this topic you will get theoretical questions about acquiring digital evidence, as well as practical tasks in handling digital seizures and acquisition of different Internet accounts.

Name three different methods of acquiring data from the Internet, such as data accessed through a browser such as Firefox and Internet Explorer

Acquisition of data from the Internet: Method 1

Acquisition of data from the Internet: Method 2

Acquisition of data from the Internet: Method 3

Describe what "Order of Volatility" is when it comes to digital evidence

0/4000

List pros and cons with activating flight mode on a phone after it is seized

0/4000

List pros and cons with doing live forensics on a computer before it is acquired

0/4000

Next >>

Practical handling of digital evidence

In the next questions you will be presented with a physical device, for example an iPhone X mobile phone. Your task is to rank in which order you want to handle the evidence.

The option you put at the top is the first thing you want to do with the evidence, alternative two is what you want to do next and so on.

Note: All alternatives are not necessarily correct.

https://cdn.pixabay.com/photo/2018/06/29/10/37/iphone-3505728_1280.jpg

3.1 Evidence: Apple iPhone X where you know the lock code

- Take a picture of the phone
- Turn the phone off
- Check time settings on the phone
- Enable flight mode
- Manual review of the phones content
- Forward messages to your service telephone
- Forward e-mails to an e-mail that you control
- Screenshots of content using the built in functions on the seized phone
- Write down serial number/IMEI number
- Acquire the phone using tools like Cellebrite/XRY
- Bag and tag the phone and hand over to competent personell for acquisition

3.1 Why did you choose to handle the evidence in the order you did?

0/4000

Next >>

https://cdn.pixabay.com/photo/2015/06/04/21/13/samsung-797870_1280.jpg

The option you put at the top is the first thing you want to do with the evidence, alternative two is what you want to do next and so on.

Note: All alternatives are not necessarily correct.

3.2 Evidence: Samsung Galaxy S6 where you do not know the lock code, the phone is locked

- Take a picture of the phone
- Turn the phone off
- Check time settings on the phone
- Enable flight mode
- Manual review of the phones content
- Forward messages to your service telephone
- Forward e-mails to a phone that you control
- Screenshots of content using the built in functions on the seized phone
- Write down serial number/IMEI number
- Acquire the phone with tools like Cellebrite/XRY
- Bag and tag the phone and hand over to competent personell for acquisition

3.2 Why did you choose to handle the evidence in the order you did?

0/4000

Next >>

https://cdn.pixabay.com/photo/2015/01/08/18/27/startup-593342_1280.jpg

The option you put at the top is the first thing you want to do with the evidence, alternative two is what you want to do next and so on.

Note: All alternatives are not necessarily correct.

3.3 Evidence: An older Apple MacBook Pro without screen saver, you have username and password to an admin account

- Turn the device off
- Remove the battery
- Check for active encryption
- Copy relevant files to external hard drive
- Send relevant files from the laptop using e-mail
- Check time settings
- Acquire RAM
- Call a colleague from a computer crime unit (DPA) for assistance
- Consider your own competence
- Turn off encryption if present
- Bag and tag the computer and hand over to competent personell for acquisition
- Document the evidence with photo, active windows etc.

3.3 Why did you choose to handle the evidence in the order you did?

0/4000

Next >>

https://images.pexels.com/photos/777001/pexels-photo-777001.jpeg

The option you put at the top is the first thing you want to do with the evidence, alternative two is what you want to do next and so on.

Note: All alternatives are not necessarily correct.

3.4 Evidence: Hewlett Packard stationary PC with Windows 10 Pro without screensaver, you have username and password for an admin account

- Turn off the device normally
- Check for active encryption
- Copy relevant files to external hard drive
- Send relevant files from the computer using e-mail
- Check time settings
- Acquire RAM
- Call a colleague from the computer crime unit (DPA) for assistance
- Consider your own competence
- Turn off any encryption
- Turn off the device by removing the power cable
- Bag and tag the computer and hand over to competent personell for acquisition
- Document the evidence with photo, active windows etc.

3.4 Why did you choose to handle the evidence in the order you did?

0/4000

Next >>

https://cdn.pixabay.com/photo/2016/08/12/05/06/technology-1587673_1280.jpg

The option you put at the top is the first thing you want to do with the evidence, alternative two is what you want to do next and so on.

Note: All alternatives are not necessarily correct.

3.5 Evidence: Dell server with Windows 2012 without screensaver, you have username and password to an admin account

- Turn the device off normally
- Check for active encryption
- Copy relevant files to an external hard drive
- Send relevant files from the device using e-mail
- Document the evidence with photo, active windows etc.
- Check time settings
- Acquire RAM
- Call a colleague from the computer crime unit (DPA) for assistance
- Consider your own competence
- Turn off any encryption
- Turn off the device by removing the power cable
- Bag and tag the server and hand over to competent personell for acquisition

3.5 Why did you choose to handle the evidence in the order you did?

0/4000

Next >>

https://cdn.pixabay.com/photo/2016/09/18/23/38/social-media-1679307_1280.jpg

4.1 Gmail

In an ordinary criminal case, you have been given permission to acquire the following email:

Username: "odihei399@gmail.com"

Password: "Julekake123!"

Assignment

Acquire the email by taking a Google Takeout.

Note: If you experience technical problems due to logins from several places in the country, use the attached Word document. Inside the document you will find a zip file that contains already acquired content.

Download Google Takeout.docx

4.1 Were you able to acquire the Google account?

◯ Yes ◯ No, I don't know how to do it

◯ No, I encountered technical difficulties and had to use the attached Word document

https://cdn.pixabay.com/photo/2016/09/18/23/01/social-media-1679230_1280.jpg

4.2 Facebook

As you may have figured out, the user of the Google account has sent the password of a Facebook account to himself by email. You speak with a prosecutor and get permission to acquire this account as well.

Assignment

Acquire the Facebook account.

Username: "odihei399@gmail.com"

Password: "Julekake456?"

Note: If you experience technical problems due to logins from several places in the country, use the attached Word document. Inside the document you will find a zip file that contains already acquired content.

Download Facebook archive.docx

4.2 Were you able to acquire the Facebook account?

◯ Yes ◯ No, I don't know how to do it

◯ No, I encountered technical difficulties and had to use the attached Word document

Next >>

https://cdn.pixabay.com/photo/2016/10/10/01/09/social-media-1727458_1280.jpg

4.3 Instagram

From the acquired Facebook account, you might find that there is an Instagram account associated with it. You ask the suspect in the case about Instagram and you are provided with the following credentials:

Username: "lindahansen999"

Password: "Pepperkake41"

Assignment

Acquire the Instagram account.

Note: If you experience technical problems due to logins from several places in the country, use the attached Word document. Inside the document you will find a zip file that contains already acquired content.

Download Instagram.docx

4.3 Were you able to acquire the Instagram account?

- ○ Yes
- ○ No, I don't know how to do it
- ○ No, I encountered technical difficulties and had to use the attached Word document

Next >>

https://www.youtube.com/yts/img/yt_1200-vfl4C3T0K.png

4.4 YouTube

The lead investigator on the case asks you to acquire the following YouTube video:

https://www.youtube.com/watch?v=dQw4w9WgXcQ

4.4 How would you acquire this video? Briefly explain your approach

0/4000

Next >>

4.5 Forum

The intelligence leader comes into your office and shows you the post above which he has come across in a forum. He asks you to acquire only the post in the picture above.

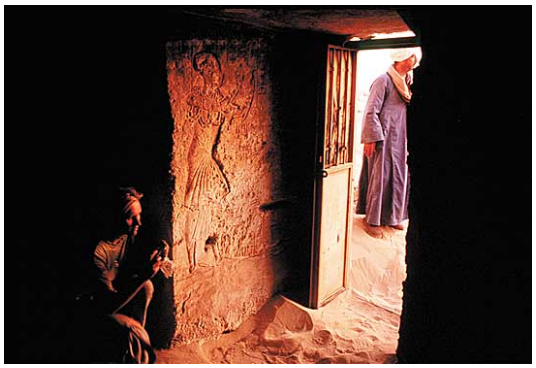
The original thread can be found in the link below.

https://forum.kvinneguiden.no/topic/1266744-hjeelp-wifi-funker-ikke-etter-jeg-slo-av-routeren/

4.5 How would you like to acquire this post so you can use it in a police report? Describe briefly.

0/4000

Next >>



http://www.opanda.com/en/pe/images/sample_001.jpg

4.6 EXIF-data

Images can contain a lot of information. Using tools and procedures of your own choosing, see if you are able to answer the questions below. All the questions are related to the picture above.

4.6.1 What is the "Image Description" for this picture?

4.6.2 Which camera brand is used to capture the image?

4.6.3 Which tool/method did you use?

Next >>

4.7 E-mail

Imagine that you are investigating a case, and the e-mail ola.nordmann123411@gmail.com is relevant in the case.

4.7.1 Which step(s) would you take to find out who the owner of the gmail account is?

0/4000

Next >>

You end up sending a request to Google to get basic subscriber information (BSI) for the e-mail. After a few days you get an answer from Google with an IP address that you find out belong to the ISP Canal Digital.

4.7.2 What would you do next?

0/4000

Next >>

You send a request to Canal Digital to find out who used the IP address in that particular time.

The answer from Canal Digital is that the following person had the IP address at this time:

Nicolay Pettersen, Sorgenfrigata 1, 0010 Oslo

In Sorgenfrigata 1, four people are registered: Nicolay Pettersen, his cohabitant Kari Nilsen and two adult children (Ronny and Truls Pettersen-Nilsen).

The lead investigator asks you to clarify whether there is basis to suspect and apprehend Nicolay. The IP address is the only evidence you have in the case.

4.7.3 What assessment(s) should you make before you possibly suspect and arrest Nicolay?

0/4000

Next >>

Final Question

As mentioned, this is a proposal for a practical test that can serve as an approval test for those who are going to work with digital research.

If there are topics or practical tasks you would like to see in a test you can write this under.

Input to topics or suggestions for practical tasks

0/4000

Send