Live Data Forensics

A quantitative study of the Norwegian Police University College students LDF examinations during their year of practice

Leif Erik Andreassen and Geir Andresen

A minor thesis submitted in part fulfilment of the degree of MSc. in Forensic Computing and Cyber Crime Investigation with the supervision of Dr. Nhien-An Le-Khac.

School of Computer Science and Informatics

University College Dublin

19 December 2019

Acknowledgments

We would like to thank the Norwegian Police University College and our leaders; Head of Department/Professor Per-Ludvik Kjendlie and Program Coordinator/Police Inspector Beathe Rødsand for giving us the opportunity for further education within the increasingly important field of Digital Forensics and Cyber Crime Investigation.

We would like to thank the University College Dublin for an engaging study with important topics, and our supervisor Dr. Nhien-An Le-Khac for valuable inputs and thoughts.

We would like to thank all colleagues who have assisted us with constructive inputs and good reflections. Special thanks to Associate Professor Asle M. Sandvik for positive inputs and invaluable assistance in SPSS!

To our families: We are finally back in your lives! Thank you for always being positive and driving us forward!

Abstract

Traditionally, the computer specialist in the Norwegian police has performed most of the tasks dealing with electronic evidence. The technology development has put this way of working and thinking under pressure. Today, it is often a limited window of opportunity to obtain digital evidence. If this opportunity is not used, the evidence may be inaccessible or lost forever. Those who are in active service, the First Responders, will most likely be the ones who first come into contact with digital devices that contain electronic evidence.

The investigation of a live (on/running) electronic device, Live Data Forensics (LDF) is a clear deviation from the established methodology we strive to follow in all processing of potential electronic evidence. At the same time, it is absolutely necessary in many criminal cases. Despite the fact that the Norwegian Police University College (NPUC) students in their practical year (B2) lack sufficient LDF competence, we had the impression that they performed LDF. In this thesis we investigate to what extent they performed LDF and how the execution was carried out.

The discussion will include, among other topics, if there is a need to move the boundary between what should be considered First Responder (generalist) and specialist tasks. The analysis of data from the conducted survey shows that more than half of the students performed LDF during their year of practice. LDF on mobile phones is prevalent. The analysis also shows that many LDF examinations are not conducted according to methodology/principles. These types of deviations can cause digital evidence not to be detected, not secured, that they are altered, destroyed, degraded and subsequently leading to not being possible to use in a court of law. In the end, this can lead to errors of justice and weakening society's trust in the police.

Based on the findings in the study, we have some recommendations. Guidelines should be drawn up on how to conduct LDF on mobile phones. The First Responder in the Norwegian police must be able to perform LDF satisfactorily. The NPUC should adjust the education accordingly. The police districts must ensure that the First Responders have sufficient competence, and that LDF is carried out according to both Norwegian and other ratified legal framework.

Keywords

Digital Forensics, Investigation, Competence, PHS, Norwegian Police University College students, Digital Evidence, Method, Digital Forensic Process, Live Data Forensics, LDF, NPUC

Sammendrag

Tradisjonelt sett har dataspesialisten i norsk politi utført de fleste oppgaver som omhandler elektroniske bevis. Teknologiutviklingen har satt denne måten å jobbe og tenke på under press. I dag er det ofte et begrenset handlingsvindu til å få sikret digitale bevis. Dersom man ikke benytter denne muligheten, kan bevisene bli utilgjengelige eller gå tapt for alltid. De som er ute i aktiv tjeneste, First Respondere, er de som sannsynligvis først kommer i kontakt med påslåtte digitale enheter som inneholder elektroniske bevis.

Undersøkelsen av en påslått enhet, Live Data Forensics (LDF) er et klart avvik fra den etablerte metodikken vi i all behandling av potensielle elektroniske bevis tilstreber å følge. Det er samtidig helt nødvendig i mange straffesaker. Til tross for at Politihøgskolestudenter i sitt andre studieår (B2) ikke har tilstrekkelig LDF kompetanse, hadde vi et inntrykk av at de utførte LDF. I denne oppgaven undersøker vi i hvilken utstrekning de utførte LDF og hvordan utførelsen ble gjennomført.

Diskusjonen vil blant annet dreie seg om det er behov for å forskyve grensen mellom hva som skal regnes som First Responder (generalist) og spesialistoppgaver.
Analysen av data fra gjennomført spørreundersøkelse viser at over halvparten av studentene utførte LDF i løpet av praksisåret. LDF på mobiltelefoner er spesielt utbredt. Analysen viser også at mange LDF undersøkelser ikke utføres i henhold til metodikk/prinsipper. Denne typen avvik kan føre til at digitale bevis ikke blir oppdaget, ikke sikret, at de endres, ødelegges, degraderes og ikke kan bli brukt i retten. Dette kan igjen føre til justisfeil og til at samfunnets tillit til politiet svekkes.
Basert på funnene i studien kommer vi med noen anbefalinger. Det bør utarbeides retningslinjer for hvordan LDF skal utføres på mobiltelefoner. First Responder i det norske politiet må kunne utføre dette tilfredsstillende. Politihøgskolen bør justere utdanningen i tråd med dette. Politidistriktene må forsikre at First Respondere har tilstrekkelig kompetanse, og at LDF utføres i henhold til både norske lover og annet ratifisert regelverk.

Nøkkelord

Digital Forensics, etterforskning, kompetanse, PHS, Politihøgskolestudenter, digitale bevis, metode, digital forensic process, Live Data Forensics, LDF, NPUC

Table of content

List of Abbreviations

5WH	What, When, Why, Who, Where and How
ACPO	Association of Chief Police Officers
B1	First Academic year at NPUC
B2	Second Academic year (Year of practice) at NPUC
B3	Third Academic year at NPUC
CCU	Computer Crime Units
CD	Criminal Detective
CFD	Criminal Forensics Detective
DF	Digital Forensics
DFD	Digital Forensic Detective (specialist)
DFP	Digital Forensic Process
DPI	Digital Policing and Investigation (a subject within NPUC)
DFWRS	Digital Forensics Research Workshop
ECHR	European Convention on Human Rights
FCCI	Forensic Computing and Cybercrime Investigation (study program at UCD)
FR	First Responder (usually a generalist within the Norwegian Police)
ICCPR	International Covenant on Civil and Political Rights
ISO	International Organization for Standardization
KRIPOS	Norwegian Criminal Investigation Service (NCIS)
LDF	Live Data Forensics
LF	Live Forensics
LR	Live Response
NFAM	Need for assistance model
NPUC	Norwegian Police University College (PHS)
NSD	Norsk Samfunnsvitenskapelig Datatjeneste - Norwegian Social Science Data Service
PHS	Politihøgskolen (NPUC)
POD	Politidirektoratet - The Norwegian National Police Directorate
UCD	University College Dublin

List of figures and tables

Figures

Tables

1. INTRODUCTION

Electronic evidence plays a vital part in most criminal investigations today. Police officers working as generalists/First Responders (FR), will most likely be the first who come in contact with live digital devices that contain electronic evidence. It is of utmost importance that they are competent to handle these devices according to established guidelines and methodology. Our focus has been to gain a deeper insight into the extent of Live Data Forensics (LDF) and how these examinations are performed.

NPUC educates the generalist in Norwegian police. For further understanding of this thesis we have included a quote from NPUC's website which briefly describes the education model and desired competence for the generalist:

"*The Bachelor's Degree in Police Studies is a three-year course run by the Norwegian Police University College. The training is professionally orientated and is intended to provide a broad theoretical and practical foundation for police work. The training is based on the principle that all newly qualified policemen/women must be generalists. A generalist is a policeman/woman who possesses basic knowledge and skills pertaining to the police's preventative, crime prevention and civil order work. In solving assignments, generalists shall be able to perform basic police duties, make overall assessments of situations, view their work in a broader social context and engage relevant specialist expertise and partners as required. Generalists shall acquire a basis for continued learning and development through the execution of their profession"*[1].

1.1 Audience

This primary audience for this thesis is those within an executive level at the NPUC and the Norwegian police. It will also be important for educators within all subjects that involves digital forensics at NPUC, and leaders of Computer Crime Units (CCU). Digital Forensics Detectives (DFD) working with digital evidence as their primary task and police officers working as First Responders (FR) will also benefit from this study. Feedback from all groups are important to develop the right competence so that the Norwegian police can do a satisfactory job within the complex field of digital forensics.

[1] https://www.phs.no/en/studies/bachelor-police-studies/

1.2 Motivation

Both authors have a genuine interest in technology and grew up in a time when technical problems in software or hardware were solved by endless hours of trial and error. Besides many nights with lack of sleep, the result was often that we were able to solve the problems ourselves. This was the start of a growing interest in how technology works and how it is used. In the years we worked in active service in the police districts, we experienced how technology was increasingly used by criminals, and a growing challenge for the police.

When we were given the opportunity to start working for NPUC as teachers in the subject *Digital Policing and Investigation* (DPI), we were able to combine self-interests and experiences with the opportunity to influence what kind of knowledge students should possess when they graduate as future police officers.

In 2017 we got the opportunity to study an experience-based master's in Forensic Computing & Cybercrime Investigation at the University College Dublin. Our competence was formalized and the motivation to develop the subject further strengthened. Our desire has always been, and will always be, to educate our students to become a police generalist/FR who is competent to handle tasks within electronic evidence they encounter within their line of work.

1.3 Research problem

The research problem for this thesis is:

LDF is performed by NPUC students despite their lack of competence.

1.4 Research questions

In order to be able to answer the research problem, it was necessary to define research questions. With these questions we were able to keep focus and stick to the scope of the thesis.

These are the research questions:

1. To what extent do NPUC students perform LDF during their year of practice?
2. Do they perform LDF according to basic principles and current methodology?
3. Which electronic devices are the subject of LDF investigations?

1.5 Scope and limitations

The scope of this thesis is primarily NPUC students and their LDF-experiences while in practice in one of Norway's police districts, working with tasks that are natural for the generalist/First Responder (FR). Education, competence and LDF examinations are central.

It is important for us to emphasize that our findings in this thesis cannot be generalized to the Norwegian police force, but rather be an indication.

2. STATE OF THE ART

2.1 Background and terminology

As a democratic nation and a member of the United Nations, Norway has several obligations and principles that must be complied with to ensure that the population has economic, social and cultural rights and can enjoy civil and political freedom.

The International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR) are important agreements that Norway is committed to. The Norwegian Constitution (Grunnloven) § 96, 1st and 2nd section states that: "*no one can be judged or punished unless it is defined by law*" and "*everyone has the right to be presumed not guilty until guilt is proven by law*" (Grunnloven, 1814, § 96).
Article 14 in ICCPR states that: "*in the determination of any criminal charge against him, or of his rights and obligations in a suit at law, everyone shall be entitled to a fair and public*

hearing by a competent, independent and impartial tribunal established by law" (ICCPR, 1966).
Article 6 in ECHR has a similar description of an individual's rights when accused of a criminal act. The article has the heading: "*Right to a fair trial*" and describes several rights of the accused. One important right is the notion that the accused is presumed innocent until proved guilty according to law (ECHR, 1950).
If one or more of these rights are deprived, one cannot say that the accused has received a fair trial.

The Norwegian Penal Code (Straffeloven) is based on the Norwegian Constitution and on the human rights as stated in the UN Declaration of Human Rights[2] and the EHCR. When a citizen is accused of a criminal act, the general principle is that the prosecutors must prove that the accused in fact is guilty. Translated from Norwegian, this is referred to as "the burden of proof" (Grunnloven, 1814, § 96).

Section 3 in ECHR lists several minimum rights of the accused. It is especially letter (b) "*to have adequate time and facilities for the preparation of his defence*" and letter (d) "*to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him*" (ECHR, 1950, p. 29) that require a deeper explanation.
By following letter b, an accused should be given adequate time to prepare his or her own defence. This will mean that the case, interrogations and evidence must be presented to the accused within a timeframe that gives him/her enough time to properly review and be able to give his/her own explanations of what has been presented. Letter (d) specifies that the accused must have the same opportunities as any other party in the case to have witnesses speaking for him/her to be questioned. When these witnesses are being questioned, it is to be under similar conditions as witnesses speaking against the accused.

Law enforcement is required to comply with Norwegian law and obligations as stated in ICCR and ECHR. This must form the basis for standards and guidelines so that the individual rights belonging to all citizens are safeguarded. This thesis will not go into further detail on

[2] https://www.un.org/en/universal-declaration-human-rights/

general investigation and review of interrogations, but it will be the *digital evidence*, and the process from collection to presentation as evidence, that will be dealt with in more detail.

There are several definitions of what digital evidence is. It is crucial to have a definition of the term to be able to describe a process that shows how this type of evidence "travels" from a crime scene or incident to the court. In an investigation, digital evidence does not differ much from other types of evidence. The main difference is that they in fact are digital.
Eoghan Casey defines digital evidence as "*any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi*" (Casey, 2011, p. 7). Anders O. Flaglien defines it as "*any digital data that contains reliable information that can support or refute a hypothesis of an incident or crime*" (Flaglien, 2018, p. 7). These two definitions have essentially the same content and meaning. They have the similar expression s*upport or refute*, referring to an offense or incident, but Casey uses the expression *any data* while Flaglien uses *any digital data*.

The United Nations Office on Drugs and Crime defines evidence as *"the means which facts relevant to the guilt or innocence of an individual at trial are established"*. Electronic evidence is defined as *"all such material that exists in electronic or digital form"* (UNODC, 2013, p. 157).

By summarizing these definitions one can say that any digital data that supports or refutes a theory or hypothesis of an offense or incident is digital evidence. The amount of this type of evidence can be huge in many cases. In most cases, the potential digital evidences will be at a scale that forces the FR to prioritize what to secure and seize according to what can support or refute a hypothesis in a criminal case and the volatility of the digital evidence. In light of Norway's obligations to ECHR, ICCR and § 96, 2nd section of the Norwegian Constitution, it is necessary to have a process that makes sure that these requirements are met. There are several Digital Forensic Models developed to ensure such process. Choice of model(s) can be difficult, and the supporting grounds may vary based on e.g. needs, equipment and competence of those using the model.

This Thesis is mainly focusing on Live Data Forensics which is a deviation from basic traditional Digital Forensic principles. To be able to understand what Live Data Forensic is, it

is necessary to explain more in-depth what Digital Forensic is. Section 2.2 will describe the Digital Forensic model that are currently used by the NPUC and a few other models more superficially.

2.2 Digital Forensic

The field of Digital Forensics (DF) is vast, with a wealth of research, literature, expressions and definitions. Wikipedia may not be considered as the best academic reference, but it gives a rather good overview over what many people mean and refer to when talking about Forensics and Forensic Science. Searching for "Forensic" or "Forensics" redirects to an article about "Forensic Science". This article states that the word *Forensic* originates from the Latin term *forensics*, meaning "*of or before the forum".* The article further describes that in Roman times, the different parties in a criminal case would give speeches to a forum based on their side of the story, and in the end of the case, the forum would decide in favor of the party that gave the best argumentation and delivery.
"In modern use, the term forensics in the place of forensic science can be considered correct, as the term forensic is effectively a synonym for legal or related to courts. However, the term is now so closely associated with the scientific field that many dictionaries include the meaning that equates the word forensics with forensic science" (Wikipedia, 2019). According to Årnes "*Forensic Science was established as a separate scientific domain during the 1800s and early 1900s*", further on he describes the story from Mathieu Orfila and forensic toxicology in 1814 to Edmund Locard who established a police laboratory in Lyon in 1910 (Årnes, 2018, p. 2).

2.2.1 Forensic Science

In the Norwegian language, there is no word for what in English is called "Forensic". One of the reasons for this could possibly be that the Norwegian language is a "poor" language in the number of words compared to English (approx. 300 000 vs. 500 000 words), but another and more probable reason may be that "Forensic" – especially in the context of "digital" is a rather young expression and probably has its origin from countries where English is the native language. English is also the main language worldwide within the field of computers and technology.
Årnes is basing his definition of Forensic Science on Saferstein´s definition which states: *"Forensic science in its broadest definition is the application of science to law"* (Årnes, 2018,

p. 2 after Saferstein, 2007). Årnes is taking the definition a little bit further: *"Forensic Science: The application of scientific method to establish factual answers to legal problems"* (Årnes, 2018, p. 2).
Eoghan Casey has a similar definition: *"Strictly speaking, Forensic Science is the application of Science to law and is ultimately tested by use in court"* (Casey, 2011, p. 15). Casey also states: *"The systematic study of digital data becomes a forensic discipline when it relates to the investigation and prosecution of a crime"* (Casey, 2011, p. 15).
According to Årnes "*Digital forensics refers to forensic science applied to digital information"* (Årnes, 2018, p. 4). He is also using the Digital Forensics Research Workshop (DFRWS) definition of Digital Forensics, which they created in their first workshop in 2001 (Årnes, 2018, p. 4):

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

Based on the definitions and the literature studied it is reasonable to say that Digital Forensics is considered as part of the Forensic Science.
Science can be defined as: *"The intellectual and practical activity encompassing the systematic study of the structure and behavior of the physical and natural world through observation and experiment"* (Lexico, 2019).

2.2.2 Digital Forensics Internationally

According to Eoghan Casey (Casey, 2011) the history of the DF is quite young and arose as a result of the rapid technological development and distribution of this technology, especially in the form of computers and mobile phones that occurred from the 1980-90. Digital devices soon became available for an increasing proportion of the population. Until 2001, *"when the primary source of digital evidence was computers, the field was logical called computer forensics, forensic computer analysis, or forensic computing"* (Casey, 2011, p. 37). In 2001, during the first annual DFRWS conference, a revision of terminology was proposed. *Digital*

Forensic science was proposed to describe the field as one. In 2008 the American Academy of Forensic sciences (AAFS)[3] proposed the title *Digital and multimedia science* for the new section regarding analysis of computer systems as well as digital images, audio, and videos (ibid).

For the criminals, the new technology soon became new tools for old crimes. Digital devices containing digital evidence became more and more important in investigations. Today, digital evidence is relevant in virtually all criminal cases.
"Digital evidence has undergone a rapid maturation process. The discipline did not start in forensic laboratories. Instead, computers taken as evidence were studied by police officers and detectives who's had some interest and expertise in computers. Over the past 10 years, this process had become more routine and subject to the rigors and expectations of other fields of forensic science" (Casey, 2011, p. 11-12).
In other words, it gradually became a need for a process and a methodology for dealing with digital evidence. It could no longer be a condition that relied on individuals to have an interest in technology to work with electronic evidence.
Casey describes three challenges that arose from the start of the Digital forensic field. They were still unresolved challenges when he wrote his book in 2011, and we believe that they still are unresolved.
The three challenges (Casey, 2011, p. 12):

1. *The forensic community does not have an agreed certification program or list of qualifications for digital forensic examiners*

2. *Some agencies still treat the examination of digital evidence as an investigative rather than a forensic activity*

3. *There is wide variability in and uncertainty about the education, experience, and training of those practicing this discipline*

There has been a rapid development within the field of DF over the past decades. It seems as the pace of development is steadily increasing. This appears in the form of quantities of academic literature, articles, publications, both commercial and non-commercial programs

[3] https://www.aafs.org/

and tools, law-enforcement and civil educations, legislation and guidelines.

The International Organization for Standardization (ISO)[4] has been, and is, an important contributor in Digital forensics. The organization has 164 member countries working on relevant International Standards that support innovation and provide solutions to global challenges. ISO has published 22877 International Standards covering almost every industry, including technology. ISO standard 27037 (ISO/IEC 27037:2012) includes guidelines for identification, collection, acquisition and preservation of potential digital evidence.
ISO 27037 "*It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions"* (ISO, 2012)
Among several other topics, the document covers recommended core skills and competency descriptions for the Digital Evidence First Responder.

Request for comments (RFC) 3227[5] by The Internet Engineering Task Force (IETF). "*The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet"*[6]. They release RFCs. *"An RFC is authored by engineers and computer scientists in the form of a memorandum describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems. It is submitted either for peer review or to convey new concepts, information, or occasionally engineering humor"*[7].
The content of RFC 3227 describes principles during evidence collection, collection procedures and archiving procedures. Important well established principles like chain of custody and order of volatility are also described (RFC 3227, 2002).

Cooperation internationally and across different agencies and organizations is also widespread. The Europol/Interpol is an example of this. Another example of collaboration is the Digital Forensic Research Workshop (DFRWS)[8]. According to Casey "*The DFWRS has*

[4] Homepage: https://www.iso.org/home.html)
[5] Webpage: https://www.rfc-editor.org/info/rfc3227)
[6] https://ietf.org/about/who/
[7] https://en.wikipedia.org/wiki/Request_for_Comments
[8] https://dfrws.org/dfrws-vision

contributed more than any other organization to the advancement of research and development in the field of digital forensics" (Casey, 2011, p. 32). Among vital contributions is the mentioned terminology. The FCCI (Forensic Computing and Cybercrime Investigation) master's education at UCD, is an example of international education for law enforcement.

The Electronic Evidence Guide is a document of importance regarding the handling of electronic evidence for Law Enforcement. The guide was developed by the Council of Europe due to the increasing need for handling electronic evidence within the EU. The purpose was to provide guidance and support in identification, handling and examination of electronic evidence. The guide is an important document for law enforcement. It is a restricted document and will not be described further.

It seems like that the development of DF internationally is influenced by many individuals, groups, organizations and nations. There does not seem to be any common and uniform direction or understanding of how the development of DF should be. This a plausible reason to why it seems to be difficult to find agreed standards and methods that are absolute and universal. DF is a large area that requires expertise in a number of specific fields. These specific fields often require their own methods and guidelines that may not equally apply to other fields. The development in this area is almost explosive and the number of electronic devices with potential electronic evidence is increasing day by day. In our opinion, this description is applicable to the current situation in Norway as well. It is not the scope of this Thesis to describe all contributors to the development of DF in detail, but we have listed the most important as we see it.

2.2.3 Digital Forensics in Norway

Both authors of this thesis have broad experience as First responders (FR) in and from the Norwegian police. We worked in the same police district, which is a medium to large police district in a central part of Norway. We both started as teachers at NPUC in 2012. In the years in active duty, we both experienced that there was a small, or rather an absent focus on DF and the associated methodology for FR in Norwegian police. In the unlikely event that it existed an overall strategy/methodology at that time, it was certainly not known to us as FR. Other police officers have the same impression and experience. This is confirmed through

conversations with many colleagues with broad experience, who have worked elsewhere in Norway in the same period of time as we did.

During our years in active service we were aware that there were a few Digital Forensic Detectives (DFD) in the police district we were employed in. We didn't know the details of how they worked. It happened quite often that we took e.g. computers and mobile phones in search & seizures. These were in some cases delivered to the specialists for examination, and if evidence was found on the devices, we were (sometimes) contacted. In some cases, mobile phones and computers where examined out on the crime scene, without having any idea of what LDF was at that time. There were no established and known routines about what to do or how to go forward in such type of cases. It was just as Casey describes, up to the individual interest of the involved FR which decided what happened with the digital devices. The absence of known and established approach to digital evidence in the Norwegian police, a kind of "vacuum condition", we believe lead to a need for focus on DF.

Marit Gjerde described the historical background for DF in Norway in her Master´s thesis (2007). The first Computer Crime Unit (CCU) was established in 1995 and the first educational courses in 1996. These courses were a collaboration between NPUC and the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim). The participants were largely police officers who were particularly interested in computers but lacked education and training. In 2004, the first DF academic course was approved. Those attending this course had to have basic computer knowledge approved by the Norwegian Network University[9] (NNU), now closed down. NPUC paid the technical training at NNU. In the next course (2006), the police districts had to pay the technical training themselves. This led to the number of applicants falling from 75 to 25. In 2007, the study had 15 participants. In august 2006 the total number of Digital Forensics investigators in Norway were 45 (Gjerde, 2007)

In 2011 Politidirektoratet (POD)[10] established a working group to: "survey police work on ICT crime, electronic evidence and online police duties and assess how to work with these areas in the future" (Politidirektoratet, 2012). This work culminated in a report that was

[9] https://www.ntnu.no/iie/
[10] The Norwegian National Police Directorate - the agency responsible for professional management, allocation of resources, follow-up of results and development of police in Norway.

released on July 10, 2012. According to this report: *"The Working Group accounts for the status of police districts and the special services and gives recommendations on how the police can work with electronic evidence, ICT crimes and online police duties"* (ibid). The most interesting findings in the report are included, as they describe the state of Norwegian police anno 2012. The report describes who are conducting data-technical investigations in the police (our translation, throughout the description of this report) (Politidirektoratet, 2012, p. 13):

Digital Forensic Detectives in the police are either civilian engineers or police-educated personnel with additional education and/or expertise acquired through practice. There are different practices regarding who is doing evidence preservation and analysis. The seizure itself is most often carried out by investigators Criminal Detectives (CD) with general investigative competence. The subsequent mirror copy, facilitation and the analysis are normally performed by a Digital Forensic Detective (DFD). Police districts have from none to three Digital Forensic Detectives, except for the largest district of the survey (Oslo Police district) that currently has 14 and plans to expand to 20.

There is usually a CD who has the case responsibility for the investigation. The bulk of the computer equipment seized in police districts is secured and analyzed by a DFD. Some police districts have CDs who have been trained to secure the contents of mobile phones.
Both the Norwegian Criminal Investigation Service (KRIPOS) and the police districts point out that the need for digital forensics increases, while the Digital Forensic Investigations become more difficult and time consuming. A special challenge is that the various manufacturers of computers, mobile phones and other electronic devices use different solutions to protect their data. This means that different methods of securing and analysis must be used. In addition, the functionality of the computer equipment changes so quickly that one must constantly develop new methods and/or improve the existing.

The report does not mention any requirement for those who are in first-line service, the First Responders. This condition is further described in section 3.2.4 in the same report:
How do the police work with electronic evidence?
Seized electronic evidence comes to the police in various ways. In the case of planned actions where one expects to find computer equipment that may contain evidence, DFDs are sometimes taken into planning the action. CDs and DFDs discuss and determine what data

seizures to do and how they should be carried out from what is to be proved. Sometimes the DFD is included in the action Phase itself. In this way, the quality of the work is ensured. With few DFDs available, it is not possible to do this routinely. Actions can also take place in the evenings and weekends. The DFD is sometimes summoned in such situations, although police districts have not established any formal routine for this.
Some CDs know how to handle the equipment, so that no evidence is lost or altered as a result of police handling. Others do not have this competency. Therefore, it happens that data is deleted or changed, so the evidence value decreases or falls away (Politidirektoratet, 2012).

Thus, a condition is described where the police apparently are entirely dependent on specialist competence to solve the missions in a good way. The report, and other studies, including Marit Gjerde (Gjerde, 2007), show that there have been some significant differences in how high the individual police district in Norway has prioritized the DF-field, especially in terms of the number of DFD employed in the district.

In the years after 2012, a major initiative has been undertaken in the field of DF in Norway. In 2014, a separate subject was established at the NPUC, Digital Policing and Investigation (DPI), described in chapter 4 - Education.

In June 2015, the Norwegian Parliament decided to implement a reform in the Norwegian police, "Nærpolitireformen" [11] ("near-police reform" - our translation).
The aim of this reform is according to the Norwegian Parliament *"to ensure the presence of a competent and effective local law enforcement, where the population resides, and at the same time develop good units that are equipped to meet today's and tomorrow's crime challenges"*.
The reform has led to extensive restructuring of Norwegian police. The number of police districts decreased from 27 to 12, and the number of service locations from 340 to 217.
The same year Oslo Police District was tasked with establishing a pilot project, from the Ministry of Justice and Public Security, on how the police can develop their tasks in a wide range when it comes to investigating and preventing ICT[12] crime that does not fall under a national center (Justis- og beredskapsdepartementet, 2015). As a result of this work, it was recommended to establish a *professional contact*-function (in Norwegian *fagkontakt*). The

[11] Regjergningen.no: https://www.regjeringen.no/no/tema/lov-og-rett/kriminalitet-og-politi/innsikt/narpolitireformen/id2398914/
[12] Information and Communications Technologyhttps://www.apple.com/shop/product/MD821AM/A/lightning-to-usb-camera-adapter?fnode=97&fs=f%3Dlightning%26fh%3D458e%252B3068

professional contact will have traditional police work as their primary task but have extra digital expertise. The recommended competence requirements were the NPUC post graduate study Nordic Computer Forensic Investigators (NCFI) module 1. This is a 15 credits course with the aim of ensuring that computer forensic investigation is at a high level (Politihøgskolen (PHS), 2017a).

In 2016, POD issued a document with guidelines and detailed descriptions on how the new police districts were to be organized (Politidirektoratet, 2016). The document contains several guidelines for the "Digital policing" field. The document clearly describes that a Digital policing unit (function) must be established in all (new) police districts. This is also referred to as Computer Crime Units (CCUs). The structure of these units, personnel and purpose is described in the report. *"The function of digital policing shall ensure a broad, efficient and appropriate use of digital information and electronic evidence in police work, including intelligence, operational policing, prevention, investigation and commissioning. Through the utilization of technology and electronic evidence, the feature will ensure that more criminal cases can be investigated quickly, and with good quality in evidence collection, analysis and method use"* (ibid, p. 98).
Further on, the document describes the unit's main tasks, organization of the work, interaction, roles and responsibility.
From the First Responders view, the specification and implementation of the mentioned professional contact is important in this report.
According to the document, the professional contact shall:

- Be an advisor to his/her own unit regarding digital evidence
- Be a professional contact link between own unit and the unit for digital policing
- Be contact link/ambassador and an intermediary of new method and new knowledge within electronic evidence

As of 2019, after our knowledge, all police districts in Norway has established the Digital policing units and implemented the professional contact-function. The document is clearly a systemization and commitment in the field of Digital policing (Digital Forensics) from the top management of the police in Norway.

January 25, 2019, the National Cybercrime Centre (NC3) was established in Norway. The NC3 is part of the NCIS (KRIPOS)[13]. Among other tasks, it provides assistance to the police districts in Norway and develops the police´s expertise and methods.

POD has developed national role descriptions with associated competence requirements for various roles within the police. The purpose of these role definitions is to ensure equal responsibility for authority, content and competence in equal roles across districts and special agencies. (Politidirektoratet, 2019). Relevant descriptions of competence requirements are:

Police generalist (usually a First Responder):
"*Graduated from the Norwegian National Police University College or other relevant education at a bachelor level"*

Digital Forensics Detective (DFD - primary tasks are Digital Forensics):
"*Graduated from the Norwegian National Police University College or other relevant education at a bachelor level. The post graduate study Nordic Computer Forensic Investigators (NCFI) module 1 or equivalent must be passed".*

Even though the professional contact- function already is established in most police districts, this function is not mentioned in this document. According to an article on Parat.com[14], which is a politically independent workers' organization with members in most professions and industries, this is strange. The article is written by Nina Sunde and Ulf Bergum, both police superintendents, working with the NPUC´s department for Post Graduate education and Doctoral Research Fellows. They question that the competence that was recommended to the professional contact is set as competence requirements for the DFD. According to them, the competence requirement for DFD should be Nordic Computer Forensic Investigators (NCFI) module 2 (Sunde & Bergum, 2019). NCFI module 2[15] has 15 credits and is more advanced than module 1.

In his thesis Odin Heitmann wrote that even though there are many signs of increased commitment in the DF field, there are still no formal competence requirements for the

[13] https://www.politiet.no/en/om/organisasjonen/specialist-agencies/kripos/key-roles-of-ncis/national-cybercrime-centre/
[14] Link to article: https://www.parat.com/norges-politilederlag-5410-406272/aktuelt/dataetterforskning-en-ungdom-med-voksesmerter
[15] https://www.phs.no/studietilbud/etter--og-videreutdanning/utdanninger/etterforskning-og-kriminalteknikk/

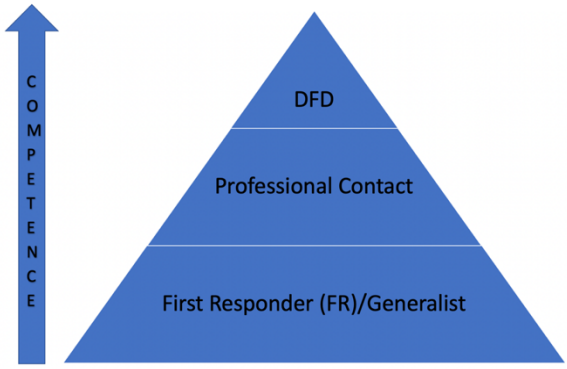
generalist (FR) in the Norwegian police (Heitmann, 2019). In summary, some of his findings are (ibid, p. 86-89):

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

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.

Heitmann's findings match our view of the current state of DF in Norway. The mentioned three challenges Casey described in 2011 are probably still the same today, but probably to a lesser extent. The Norwegian police has come a long way in some areas and the developments are on the right track, in many ways. The national role descriptions with associated competence requirements issued by POD is an important step, but there is still disagreement about the content regarding competence requirements. The results from our survey indicates that the examination of digital evidence on mobile phones in many cases often is treated as an investigative rather than a forensic activity (further described and discussed in chapter 5 – Analysis and results, and in chapter 6 – Discussion). The opinions about what education and competence requirements should be for those who are going to practice within the field of DF are largely influenced by different points of view, and there is still no common perception accepted by all.

Figure 1: A graphical representation of Digital Forensic competence within the Norwegian police

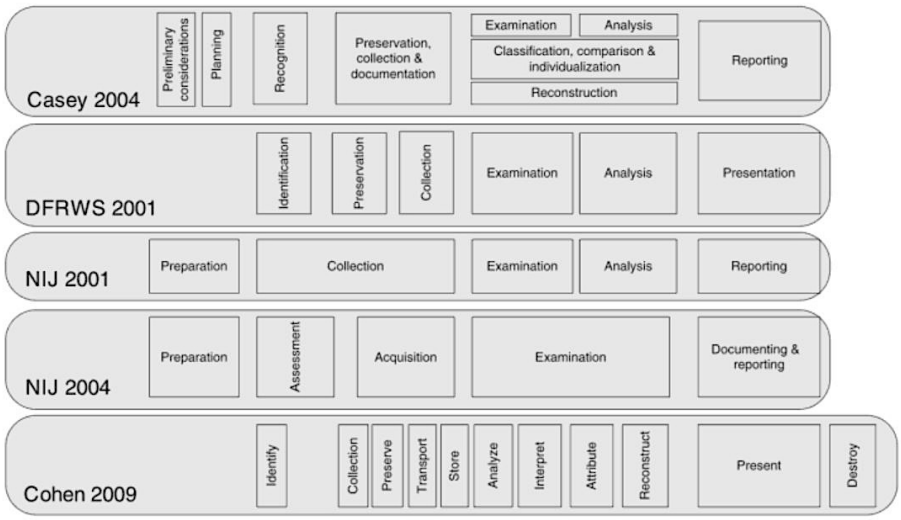


2.2.4 The Digital Forensic Process (DFP)

According to Casey (Casey, 2011, p. 187) the goal of any investigation is to uncover and present the truth. To be able to do this in a sound and proper manner, in accordance with international and national legislation, we need a methodology or process. "To seek to use trusted methodologies and techniques to ensure that the analysis, interpretation, and reporting are reliable, objective and transparent" (ibid). The reason for this is, of course, that the consequences are severe for those who are under suspicion or prosecution if evidence is presented as truth, and it turns out not to be. A Digital forensic process should serve the investigation and it should not be too rigid or dictating. An established model also helps to provide good training and reflection on working methods. It ensures proper evidence handling and reduces the chance of different "pitfalls" in the investigation – such as preconceived theories.

"*Process models have their origin in the early theories of computer forensics which defined the field in terms of a linear process*" (Casey, 2011, p. 188). Many different models describe the digital investigation process. Some models have many Phases/steps, other fewer. This can also be called different granularity. Fortunately, all models have many similarities and the Phases are similar, overall. "*In general, the differences between these process models may be explained by the way they dissect the investigative process. Some models use broad categories, whereas others divide the process into more discrete steps*" (Casey, 2011, p. 190).

Figure 2: Different DFP models as illustrated in Casey, 2011, p. 189



Even internally on NPUC, models with variations are used. One plausible reason for the use of different models on NPUC, is that there are different target groups for education. The Bachelor's department educates the Police generalists and has chosen a model based on what expectations are set for this type of personnel. The department for Post Graduate studies further educates the generalist to become e.g. a DFD. They use a model that is adapted to this education. Currently they use a 6-step model containing the following steps:
Localization – Preservation – Acquistion – Processing – Analyzing - Report/Presentation.

After much consideration, the NPUC bachelor's department have chosen the DFP model described by Anders O. Flaglien in the book "Digital Forensics" edited by Andre Årnes (2018). For the NPUC Bachelor´s department, it is important to teach a model that is universal and relatively easy to understand. Starting this year (2019) this book's chapter 2, "The Digital Forensic Process" (DFP) is curriculum for the bachelor students of the NPUC. We will refer to this model further in this thesis.
The model describes what we in the education at NPUC refer to as the “main methodology” or “main rule”, what we should strive for in every investigation involving electronic evidence. Deviation from the process is sometimes necessary, but the students must understand why there is a need for deviation, and what they could and should do to minimize the forensic challenges that arise when one deviate from the methodology. These challenges will be addressed in-depth in section 2.3 LDF.

The described DFP is universal in the sense that it can be used for investigations of any kind of crime or incident involving digital devices, such as computer forensics, mobile forensics, internet forensics as well as future technologies. It defines a structured investigation from any device capable of storing or processing data in a digital form (Flaglien, 2018).
The DFP is simply explained a series of steps on how digital evidence should be handled. If these steps are performed correctly and in the correct order, then the evidence is valid and can be presented in court. In addition, the process must be performed in compliance with several important basic principles, what we can call a foundation for the process. The principles, the model and its individual steps will be described in detail.

2.2.4.1 Principles of DFP:

In his description of principles of the DFP, Flaglien highlights two principles which is necessary to consider a process or method to be *forensically sound*. Forensically sound is an overlaying principle and means that the process must adhere to established principles, standard, and processes (Årnes, 2018).

Evidence integrity - the preservation of the evidence in its original form. "*This is a requirement that is equally valid both for the original evidence when it is collected, as well as the copy of the evidence that is used for the analysis and then referred to when evidence is presented in court"* (Flaglien 2018, p. 15). The content and understanding of this definition are also described by Casey (Casey, 2011) and Hamremoen (Hamremoen, 2016

Chain of custody – "The ability to document all actions done to the evidence in order to prove its authenticity and integrity" (Flaglien, 2018 p.15) Also described by Casey (Casey, 2011, p. 21) and Kruse & Heiser (Kruse & Heiser.

In addition to the two principles mentioned above, Flaglien also describes the principle of repeatability or reproducibility, which means that a *"skilled third party, should in principle, be able to reproduce the findings"* (Flaglien, 2018, p. 46).

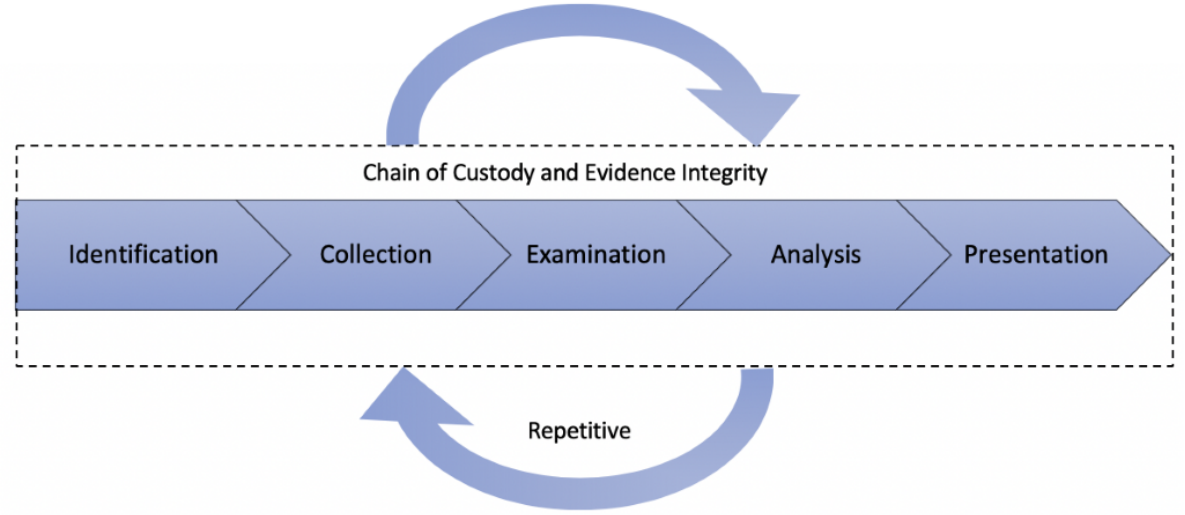
2.2.4.2 Flaglien's Digital Forensic Process model

According to Flaglien, research into developing a standard has been ongoing since the 1980s. He describes that his model is based on the most well-known processes, which then has been analyzed in order to identify their common characteristics and pphases. He has chosen to focus on the most common pphases, and he then describes the essence of each pphase. The model describes a normative approach of conducting digital forensic investigations
The model consists of five pphases. These are: *Identification, collection, examination, analysis* and *presentation*. The process is described as a step-by-step process from start to end, but there can and will be multiple iterations of several phases. A simple overview of the model is given by Flaglien (Flaglien, 2018, p. 16):

"The first Phase is the Identification of potential evidence sources from digital devices. Then, we collect digital raw data by copying the source in a forensically sound manner. Next, we examine the raw data, giving it structure so it is easier to process and understand. Then we conduct the analysis, where we seek to gain a better understanding and to identify digital objects that would ideally be the evidence that is, finally, presented to a court of law"

Traditionally, and in many cases today, the FR is involved in only the first phase; Identification. However, it is a goal to raise the competence for the police generalist (FR) in Norway. The reasons for this are many and will be discussed further in chapter 6.

Figure 3: Digital Forensic Process Model by Flaglien, reproduced/modified by us. (Flaglien, 2018, p.16)

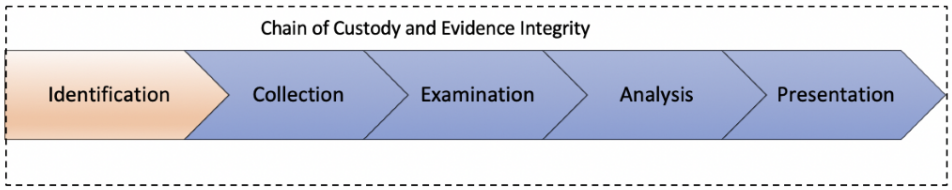


Chain of custody and evidence Integrity is "surrounding" the phases, the principles are the foundation of the process and is valid throughout all phases – from start to end. The arrows represent that the phases are iterative (repetitive).

We will use an example case during the description of some of the phases. A third-year student at the NPUC told us (the authors) the details of this case. The student had experienced the case during the second/practical year at NPUC. Some details are left out to safeguard the privacy and integrity of the individuals involved in the case. The student and his supervisor were working a night shift at a police station. In the evening, they got a mission/assignment from the operations center. They were ordered to do a search and seizure in an apartment, a person was under suspicion in an ongoing child sexual exploitation case. They tried to get a DFD to ride along to the scene, but due to the late hour no DFD was available. They could not even get in contact with a DFD by phone to ask for any tips/hints. Further on in this chapter, we will describe additional information from this case where we see fit.

2.2.4.2.1 The Identification Phase:

Figure 4: DFP - The Identification Phase. This and all models in this chapter are made after inspiration from Flaglien.



The Identification Phase is: *"The task of detecting, recognizing, and determining the incident or crime to investigate"* (Flaglien, 2018, p. 18 after Reith et al., 2002). The main task in this phase is identifying digital devices and systems that can contain electronic evidence. Compared to other DFP models, Flaglien´s model is wider and includes more investigative steps in each phase.

According to Flaglien, evidence can be relevant in two ways, the ontological way – as something we can observe and describe. The second way is evidence by recognition, what the evidence can tell us about a case. The Identification Phase should always raise the 5WH questions "*5WH defines the objectives of an investigation as who, where, what, when, why and how*" (Årnes, 2018, p. 3 after Stelfox, 2013; Tilstone et al., 2013). These questions can help establish hypothesis about the crime based on the information triggering the incident. The 5WH is fundament for all procedural steps in several investigative models. In Norway the 5WH are implemented in the "Investigative Cycle" (Sunde, 2017 after Fahsing, 2016).

In our example case, the student told us that as soon as they got the order, they started planning the search and seizure. They had few details about the grounds for suspicion at the time, the particular search & seizure was a part of a bigger synchronized operation. On the way to the crime scene, they talked about what they could meet, different hypotheses about the crime, what kind of evidence they should be looking for first – and where. They discussed different scenarios (it was a 20+ minute drive). "What do we do if the suspect is home?", "What if not?", "What should we say when we knock on the door?", "If we say we are the police, will the suspect be destroying evidence?", "Should we place the suspect under arrest immediately and should we question him on site?". According to the student, the discussion helped them to be relatively mentally ready and prepared for what met them.

When they arrived, they knocked on the door. They announced that it was the police and that they had a search Warrant. They heard plenty of "rummaging" noises from inside, and the suspect used a long time to answer the door. When they got into the apartment, the first thing they saw was a running stationary computer with a live Skype session. The video feed showed a situation involving sexual exploitation of a child. The suspect was immediately placed under arrest.

At this point the student felt that the situation was going from what he thought was a very challenging case, to be far more complicated than he and his colleague could handle alone. They tried to get additional police personnel to what now was a crime scene, but they had no luck with that. However, they got another police patrol to transport the suspect from the crime scene to police custody. The only aid they had was the operation manager in the Operations center, but when they asked questions on e.g. what to do with the live Skype session, the answers they got did not make them feel assured. The two officers felt that they did not have the competence to investigate the running computer with the live Skype session. They decided to document the session with their service phone (iPhone) and recorded a video of parts of the live session. After this, they pulled the plug on the computer. At the time they did not know how to proceed with the running computer, but they felt like they had to do something. Pulling the plug on the machine felt like a relief. With the computer powered off they could focus on all the other tasks at the scene.

Preservation is a part of Flaglien's Identification Phase. *"The processing of potential evidence normally starts during the Identification Phase, and it is crucial to preserve the chain of custody and evidence integrity from the very start. This includes activities to isolate, secure and document the physical and digital devices at hand"* (Flaglien, 2018, p. 22).

Since the two officers had no special DF-competence and could not consult with a DFD during the search and seizure, they did things as good as they were able to.

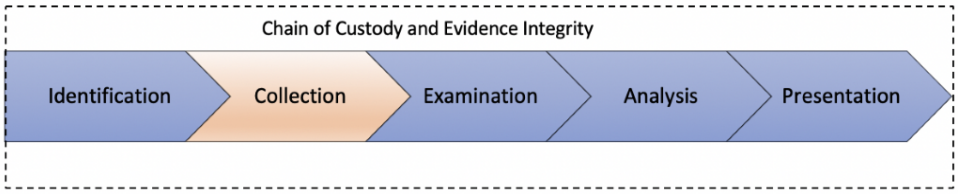
Preservation is also about documentation, and by documenting, we can enable reproducibility of results – and traceability from the evidences origin to the final step in the DFP, the presentation of the evidence.

After pulling the plug on the machine, the officers started a thorough search after other sources of potential digital evidence (and other evidence). They identified several USB "Thumb-Drives", one 3,5" S-ATA Hard Drive (in the gutter on the balcony of the apartment), a mobile phone and some handwritten notes containing username and passwords (to different e-mail accounts and so on).

All the seized items were photographed before they were removed. The mobile phone was off, so it remained off. All items were transported to the police station for further analysis by a DFD.

2.2.4.2.2 The Collection Phase:

Figure 5: DFP - The Collection Phase.



The Collection Phase is: "*Collection of data from digital devices to make a digital copy using forensically sound methods and techniques"* (Flaglien, 2018, p. 25).

It seems like most of the literature that discusses DFP models, uses either *collection, acquisition* or *extraction* about the same process – coping of the data.
While the Identification Phase includes the collection of physical evidence (which of course can contain electronic evidence) out on a crime scene, or more correctly – at the Scene of the Incident, the Collection Phase refers to the acquisition or copying of data. Traditionally, this is done by a DFD and is considered a specialist task, at least in Norway. As we will describe in section 2.3, this can also be done as a part of an LDF process, but anyway this is a deviation from the established methodology of what we at NPUC refer to as "the main rule".

The raw data is copied to a separate media, and the DFD continues the further steps in the DFP on a copy. The terms *duplication*, *cloning* and *bit-by-bit* copying is synonyms for the same process, the copying of the raw data (Flaglien, 2018). The principle is that no data should be changed in the process of copying. The DFD ensure this by using special forensic software with either a hardware or software-based write blocker. A write blocker means that no data can be written to the source where the original data resides.
It is important to underline that even if write blockers are used, we can never guarantee that changes did not occur. Using a hardware write blocker on a hard drive alters the original state of the drive. Such alteration can according to Casey include making a hidden area of the hard drive accessible or updating the S.M.A.R.T (Self-Monitoring, Analysis, and Reporting

Technology) on the drive (Casey, 2011). Due to this fact, it is not wise to set an absolute standard that dictates "preserve everything but change nothing". It is inconsistent with other forensic disciplines, and dangerous in a legal context, (Casey, 2011, p. 19-20). We must compensate for this by minimizing the changes to the original evidence to as little as possible, and document everything we do.

After copying, the DFD generates a digital signature of the data/image by using a cryptographic hash algorithm function. This is often referred to as "digital fingerprinting". The website 2brightsparks.com has an explanation of hashing that reflects what we consider to be accurate.

"Hashing is an algorithm that calculates a fixed-size bit string value from a file. A file basically contains blocks of data. Hashing transforms this data into a far shorter fixed-length value or key which represents the original string. The hash value can be considered the distilled summary of everything within that file.
A good hashing algorithm would exhibit a property called the avalanche effect, where the resulting hash output would change significantly or entirely even when a single bit or byte of data within a file is changed.
A hash is usually a hexadecimal string of several characters. Hashing is also a unidirectional process so you can never work backwards to get back the original data. Hashing is also used to verify the integrity of a file after it has been transferred from one place to another" (2BrightSparks, 2019)[16].

Examples of different algorithm are MD5 and SHA-2 (often 256 bits). The output from the algorithms (the hash value) is regarded more unique than DNA from a human being. It is mathematically infeasible that two different files can have the same hash value.
So, by hashing both the original data and the copy, we can compare the hash values to verify the integrity of the file/data. If the value is identical, we can prove evidence integrity and chain of custody throughout the DFP.

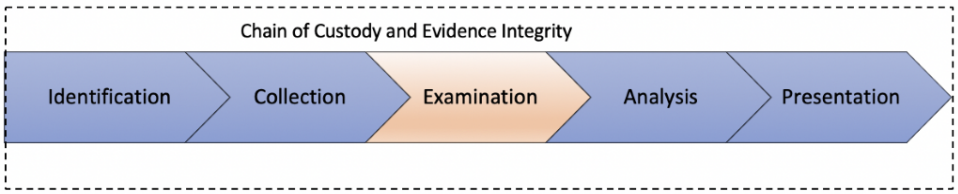
[16] Hashing explained: https://www.2brightsparks.com/resources/articles/introduction-to-hashing-and-its-uses.html

We always work on the copy (more often a copy of the copy), and we can always refer to the original data/source. If we make a mistake, the original data is always intact – and we can repeat the process without corrupting or changing the original data.

The order of Volatility is also a principle which must be considered closely in the collection Phase:
"Prioritization of the potential evidence source to be collected according to the volatility of the data" (Flaglien, 2018, p. 30). For the FR, this is a very important principle, in our example case for instance, the FR had to handle and secure evidence from the running/live machine before going on with the search for other evidence. By ignoring this principle, important evidence (of the live abuse) could have been lost. A further discussion on this principle would be given in chapter 2.3 LDF.

2.2.4.2.3 The Examination Phase:

Figure 6: DFP - The Examination Phase



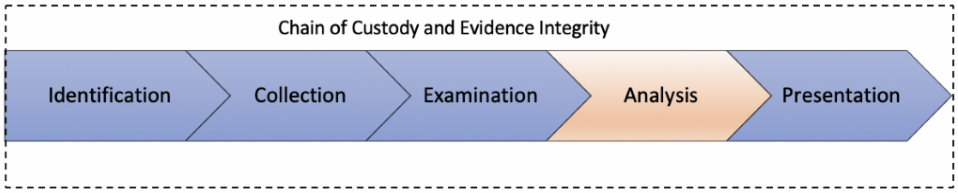
The Examination Phase is: *"Preparation and extraction of potential digital evidence from collected data sources"* (Flaglien, 2018, p. 34).

In this phase, all data collected must be examined and prepared for later analysis. Restructuring and preprocessing is necessary to make the raw data understandable for a human, both in form of a DFD or/and the Criminal Detective (CD) in charge of the case. The data in its raw form can be often be overwhelming, both in size and form/representation. It is common to use special forensic software, tools and techniques to make it more structured and readable. Since cases today often involves huge amounts of data, it is necessary, from both a digital forensic and investigative perspective to identify the most relevant data as quickly as possible. The forensic software and tools can automate many of these tasks, for instance by using scripts that run specific tasks. It is for instance possible to specify what kind of information the software should "look" for in the raw data, specific file types, specific hash

values (known files, hash databases), keywords, most changed files and so on. Anyhow, the value of human examination, based on experience and intuition should not be underestimated. The cooperation between DFD and the CD in charge of the case is very important. Otherwise, it can be difficult, or at worst, impossible for the DFD to know what information (digital evidence) is relevant to the case and decide what information that should be extracted. Another important aspect in this phase is data recovery. Forensic software can, from most file systems, recover deleted files if they are not overwritten. "*A copy of a data source can be considered a "black box" of unstructured, binary data"* (Flaglien, 2018, p. 34). The collected data image can contain broken files, deleted files, and fragmented data elements that stem from many years of using a computer (Flaglien, 2018). To interpret and structure this data manually can be a very time-consuming task. To help the DFD in this process, there are several different tools which can do what is referred to as parsing and carving. "*Carving is a method that looks for data that fits into known file structures or other data structures and interprets the data in light of the structures"* (Sandvik, 2018, p. 250). By using these tools, it is possible to recover deleted and/or parts of files, e.g. e-mails, video- and image files. Manual work cannot be overlooked when handling proprietary files and objects, the DFD must often do this manually to examine the information within the files and present them in a format readable. The forensic software can in most cases also process compressed, encrypted and obfuscated files.

2.2.4.2.4 The Analysis Phase:

Figure 7: DFP – The Analysis Phase



The Analysis Phase: "*The processing of information that addresses the objective of the investigation with the purpose of determining the facts about an event, the significance of the evidence, and the person(s) responsible"* (Flaglien, 2018, p. 40).

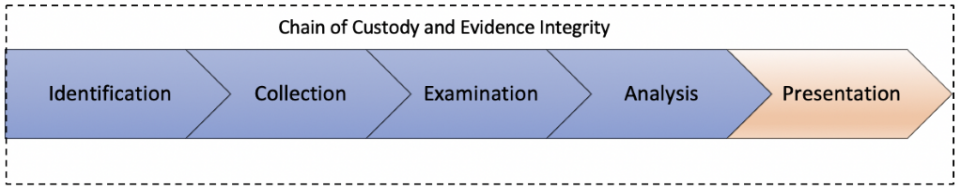
The DFD must determine which digital objects to be used as digital evidence. The evidence will then help to support or refute a hypothesis of a crime or incident. Methods used in this phase can include statistical methods, manual analysis, techniques for understanding protocols

and data formats, linking of multiple data objects and timelining (Flaglien, 2018). DFP is, as mentioned, an iterative model. The analysis phase is an iterative process in itself. It often happens that one forms new hypotheses about the case while performing analysis, which generate new needs for collection of additional data. This process continues until the result is sufficient to support or refuse the hypothesis.
"Any case will have its own evidence, depending on the type of crime." (Flaglien, 2018, p. 40). In our example case, evidence that could tie the suspect to the electronic device (evidence source) would be of utmost importance.

Objectivity is a cornerstone of forensic analysis (Casey, 2011). *"The interpretation and presentation should be free from bias to provide decision makers with the clearest possible view of the facts"* (Casey, 2011, p. 24).

2.2.4.2.5 The Presentation Phase:

Figure 8: DFP - The Presentation Phase



The Presentation Phase is: *"The process by which the examiner shares results from the analysis phase in form of reports to the interested party or parties"* (Flaglien, 2018, p. 45).

This phase is about the documentation and presentation of the DFP to the "interested parties". For the Norwegian police - this is mainly to the court of law. In Norway a police prosecutor and/or the management will in most cases review the documentation/report before it goes to proceedings in the court. The presentation should be based on objective findings from the analysis of the digital evidence. It is important that the findings are summarized and that all actions performed during the investigation are accounted for and described in a fashion that is understandable by the audience. (Flaglien, 2018).
To insure and prove that the principles of chain of custody and evidence integrity are considered throughout all steps of the investigation, the final report should include thorough documentation of all steps taken – from the start to the end of the process. Eventual errors or mistakes which has occurred during the investigation, must be documented in the report. The degree of uncertainty about i.e. a method, tool or program must also be documented.

Uncertainty first becomes a problem when the police don´t express (the grade of) the uncertainty, or in the worst case the opposite and proceed as if it is a certainty. This latter is a certain way to compromise or weaken the value of the digital evidence – and of course the DFDs credibility.

Flaglien lists up some typical information which is required in the final report:

- Roles and tasks assigned for the investigation
- Executive summary of all information sources and evidence
- The forensic acquisition and analysis, which reflects chain of custody and evidence integrity
- Visualizations and diagrams
- Images and screenshots
- Information that supports the repeatability or reproducibility of the analysis
- Tools used
- Findings

The forensic tools used by the police often have reporting functionality. The output (report) from these digital forensic tools are not enough, the investigator must prepare this information so that is understandable for a third party. Often, the reader lacks the technical insight and competence the DFD has. The purpose of the investigation is after all, to present the findings in a clear and understandable manner (Flaglien, 2018). The use of visualization techniques can be useful to fulfill this goal. Diagrams, graphics and timelines are examples of this. In the Norwegian police, there are no general approved template for report writing in a case involving electronic evidence. It is not described in the subject "Investigation and report writing" at the NPUC either.

"The documented chain of custody is the glue that holds the forensic process together and supports the final evidence integrity so that it can be presented as trustworthy evidence in court" (Flaglien, 2018, p. 47). Documentation on all activities is crucial to avoid that the court (and the defense) can claim that a critical task did not occur. All the work done throughout the DFP, however good it is executed, could be a waste of time if one lacks proper documentation.

2.3 Live Data Forensics

LDF is in this thesis used as a terminology that describes a process for acquiring and analysis of digital evidence that deviates from the DFP. LDF requires that the person(s) performing this has adequate competence and understanding of the consequences of investigating a live system. Briefly the difference is that while the DFP, within law enforcement in Norway, describes the acquisition and analysis of digital data from a "post-mortem" (dead) system, LDF describes the same process on a live (running) system.
Conducting a search for information about LDF on the internet gives results where Live Data Forensics often is combined with other terminology like "Live Response" and "Live Forensics". If we combine the three terminologies there are quite a lot of articles and education addressing these terms, but there seems to be a shortage of literature that goes in depth on either one of them.

The terminology "Live Data Forensics" is relatively new in the Norwegian police and within the NPUC educational program. For the Bachelor´s program education it was first taken into use in the fall of 2014 as a result of implementing the FiRST tool into the education. Our personal view and experience in the field is that there is a variety of definitions and not one universal definition adapted by all. An example of this variety may be that e.g. two different articles describes the same processes about how to e.g. secure data from "live" systems but use different terminology.

The Symantec connect official Blog[17] describes Live Response *as the same as traditional forensics in the way that they both are looking for similar artifacts. The difference is that this examination is done on live system while conducting live response.*

The Electronic Evidence Guide from the Council of Europe (COE)[18] has a similar definition of LDF: "*how to acquire, process, analyze and present data from a computer system that is turned on"*. COE´s cybercrime department[19] (restricted, law enforcement only) facilitates a variety of courses where LDF is one of the topics. Some of them are in cooperation with the University College Dublin (UCD). UCD work closely with the Norwegian Police University

[17] Viewed 27.11.19 https://www.symantec.com/connect/blogs/live-response-vs-traditional-forensics-0
[18] https://www.coe.int/en/web/portal/home
[19] https://www.coe.int/en/web/cybercrime/home

College (NPUC) and has published multiple research articles regarding digital forensics and their teachers are from different parts of the world.

Our LDF study at UCD has been a major inspiration and contributor to the current LDF education at NPUC. In the NPUC Bachelor program education we have chosen to define LDF in the same way as UCD. Further description of the LDF methodology will be related to the 2018 UCD Live Data Forensics curriculum unless otherwise stated.

Live Data Forensics definition:
Live Data Forensics (LDF) is *"the forensic acquisition and/or analysis of the data from a running (Live) digital system for use in a court of law".*

As described the terminology can appear confusing but the meaning of the different terminology has similarities. It´s important to clarify that for our definition of, and education in LDF, "Live Response" is included as a vital part of this.

Live Response definition:
Live Response (LR) is "*the investigation of the suspect system while the system is powered on (live)".*

The difference between LDF and LR can be described as while LDF is the forensic acquisition and/or analysis of the data from a live system, LR is the process of examining the system while it is on.

LR can also be described as an initial process to see if LDF is needed, or in cases where information is more important than data preservation. Examples of these types of cases can be terror cases, or other cases where there is danger to life and health. A practical example is instead of acquiring the content of a folder or a disk using software or hardware that ensures this is done in a forensically sound way according to the LDF process, LR will, in short, mean that the folder or disk is examined before it is copied. Rather than acquiring data from the system, we extract information from it.

In the education of our students in the field of LDF, we use the terminology LDF for both LDF and LR. In our experience the subject Digital Policing and Investigation is one of the

most demanding and difficult subjects the students participate in during their education. This is based on student feedback since 2014. Due to limited educational time and that we educate the generalist/FR and not a DFD we have chosen not to split the LDF process up into several parts.

2.3.1 LDF Methodology

When to perform LDF depends on several factors. Each case is distinctive and consists of different types and amount of potential electronic evidence that must be secured and analyzed. Type of case, timeframe, the suspect, environment and type of electronic devices are all factors that influence the decision on if, and how, LDF is to be performed.

When searching for a specific LDF methodology in literature, articles, education and online, we struggled to find a methodology exclusively for LDF. As earlier mentioned, there are a variety of models describing the DFP. Several of the descriptions of these models also describe securing electronic evidence from a live system. Flaglien states: "*special caution must be taken before any action, regardless of whether the system is live or dead"* (Flaglien, 2018, p. 25). This indicates that the process is intended for both types of investigation.

As previously described, it may seem that there is no established definition internationally of what LDF is. It may look like the terms "Live Forensics", "Live Response", and "Live Data Forensics" are used interchangeably, but the method and the process they describe have many similarities. Both Casey (Casey, 2011, p. 249) and Flaglien (Flaglien, 2017, p. 22) describes the handling and challenges regarding acquisition and preservation of data on live systems. Furthermore, they acknowledge an emerging need to do so, as technological developments have led to potential electronic evidence being lost by turning off the electronic device or disconnecting it from the network to which it is connected.
Rapid technological development can be one of the challenges of establishing a methodology that becomes a common established standard. The technological arena has a number of different areas that are complex and very different from each other. A common standard that covers all areas with its characteristics we believe is almost impossible. One plausible question one might ask is whether this could be one of the reasons why it seem to exist

several different terms like LDF, LR & LF, referring to a process or method described quite similarly, and not an established international definition.

To illustrate the complexity, we have the following example:

Imagine that there has been developed a method for network isolation of a mobile phone using Android OS which includes that this is possible to do when the mobile phone is on and locked

This method worked until the next Android OS update made this impossible from a locked phone. The consequence of this is that a new method must be developed as quickly as possible. Meanwhile, the First Responder (FR) has the opportunity to use the old method in cases where the user has not yet updated to the latest version of the operating system. The "window of opportunity" will decrease by the hour and it also has the effect that the FR must have competence in two methods for network isolation on an Android mobile phone. This is just one of many examples of real case challenges regarding LDF.

A possible consequence of these challenges and rapid evolution in technology may be that instead of leading to international and standardized methods, the experience of specialists, researchers and other experts has led to the development of best practice guides in specific fields, and ground rules that apply to different areas of DF. An example of this is the ACPO guidelines (ACPO, 2012) which is a "best practice guide for digital evidence" developed by the Association of Chief Police Officers of England, Wales & Northern Ireland. The benefits of this guide are that it is not only for LDF, but it is applicable for all potential digital evidence and process models. The ACPO guidelines will be described in more detail later in this section.

There are various types of tools and software applications designed to, according to the developer, ensure that potential electronic evidence is acquired in such a way that they are altered as little as possible. Private companies, researchers, scientists and law enforcement all develop methods, tools and software applications. Compared to private companies, Law enforcement tend to develop tools and software application at a slow pace. The reason(s) for this is beyond the scope of this thesis, but the result is that law enforcement often is dependent on using programs developed by private companies (Flaglien, 2018).

To be able to trust the technology and the presented information, especially from private companies, law enforcement must test the tools and software in a controlled environment to check if the result is correct. In cases where there is uncertainty about the results, a "Dual Tool Verification" can be applied to detect errors (Flaglien, 2018). This involves using two different software applications/tools to perform the same task. If they present the same result, the probability that the result is correct is significantly higher. Due to the rapid technological development, there can often be a gap between the need for tools for a particular task and the development and access to the tool.

In our research we found that even if there are many different tools, approaches, terminologies and methodologies, there are some basic principles and common challenges that are similar. One of the main challenges with performing LDF is the inevitable change of data while examining the system. This change of data can be explained through "Locard´s Exchange Principle" (Årnes, 2018, p. 3 after Saferstein, 2007):

"Whenever two objects come into contact with one another, there is an exchange of materials between them"

This means that when a Police officer, or any other person, interacts with an electronic device there will be changes to the system. This is in itself a contradiction to the principle about forensically soundness (Årnes, 2018).

One of the two fundamental principles regarding forensically soundness is e*vidence Integrity* (ibid). Based on Locard's Exchange principle, this is not possible to achieve when performing LDF.

Some practitioners of digital forensic believe that the only way to follow a forensically sound manner is by not altering the digital evidence in any way. According to Casey, this is not true (Casey, 2011). He compares digital forensics with traditional forensics disciplines such as DNA to prove that to measure forensically soundness the original material does not need to be left unaltered. In many cases the DNA test are destructive. Nevertheless, it is rare that DNA is not accepted as evidence.

The other fundamental principle Flaglien describes is the "Chain of Custody" . Chain of Custody is defined as (Årnes, 2018, p. 6):

"Chain of Custody refers to the documentation of acquisition, control, analysis, and disposition of physical and electronic evidence"

Since 2014 the general approach for students graduated from NPUC is that digital forensics (in general), is a task for the DFD. Simplified, they have been educated in the following "main rule":

Every electronic device that is turned off (dead) shall remain off, and electronic devices that are on (live) shall remain on.

If the device is to be transported from the crime scene, and needs to be powered off, this should be done by "pulling the plug".

If this is not possible due to e.g. non-removable battery, the device, depending on the case, is to be network isolated. Especially for mobile phones; a switched-on device should remain switched-on, but, depending on the case, it should be network isolated. Every student graduated from NPUC since 2014 are educated with the same main rule. Therefore, the same main rule will apply to the generalist/FR if they have not received additional training in the Police district they work.

In order to uphold this main rule and at the same time the two fundamental principles of forensically soundness, the ACPO guidelines is implemented as a general forensic principle and as a general LDF guideline by the NPUC. The ACPO guidelines has the purpose of being a best practice guide not only to law enforcement, but also for all that assists in investigating cyber security incidents and crime (Association of Chief Police Officers (ACPO), 2012). It is emphasized that personnel that have not received appropriate training and are unable to comply with the principles, should not carry out this category of activity. The guidelines states in section 2.2 that all digital evidence is subject to the same rules and laws that apply to documentary evidence and that the doctrine of the documentary is to show the court that the evidence produced is no more and no less now than when it was first taken into the possession

of law enforcement (ACPO, 2012, 2.2.1, 2.2.2). This is a very important statement for law enforcement in Norway and in the education at NPUC.

The guidelines consist of four guiding principles for digital forensics that attempts to encompass the diversity of the digital world. Even though the principles were formed in 2012 they still hold today.

The principles of digital evidence (ACPO)

Principle 1

"*No action taken by law enforcement agencies or their agent´s should change data held on a computer or storage media which may subsequently be relied upon in court."*

Principle 2

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

Principle 3

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

Principle 4

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

It is in particular principle 2 and 3 of the ACPO guidelines that ensure that an investigation is conducted in compliance with the two fundamental principles of forensically soundness; evidence integrity and chain of custody. The central principle, however, is principle 1, which states that law enforcement must *not do anything that changes data on a computer or storage media which may subsequently be relied upon in court*. This is a vital principle which applies to all education and training in digital evidence at the NPUC Bachelor department.

2.3.2 Performing LDF

Further description of how LDF is performed will be related to the current education at the NPUC Bachelor department. This will also reflect the execution to a great extent after graduation, i.e. how it is performed by the generalist/FR in active duty without further education than graduating from NPUC. The education of the students is mainly based on our own education at the UCD. Therefore, many of the steps in the LDF process will be similar to the process taught by UCD. Where it is natural, the LDF process will be compared to the ordinary process for digital forensics. An example of this is ACPO guidelines principle 2 which states that "*when it is necessary to access original data, that person must be competent to do so and to be able to give evidence explaining the relevance and the implications of their actions".* This principle is equally applicable to both the LDF and a post mortem examination.

The first thing to consider is whether to perform LDF or to follow the "traditional" digital forensic process and "pull the plug".

It is important to emphasize that it is the individual case that determines whether LDF is needed. What is the case, who is the suspect, what do we want to prove, what is the environment (home or office), which device(s) to examine and how much time we have are all relevant issues we need to elucidate before making a decision (UCD, 2018).

Being able to make this decision is a major challenge for many FRs. Feedback from the students since we started the subject Digital Policing and Investigation at the NPUC, FRs in active duty, results from our survey and our own experience shows that this is an important, but difficult decision. Incorrect decision can cause important electronic evidence to be lost forever. This is the reason for the implementation of a software tool in the education at NPUC in 2014. This tool makes this decision easier for the FR. The tool is restricted and for law enforcement only, so the description will be brief and include what we consider to be widely known. The First Responder Scan Tool (FiRST) is a software-based tool developed to be a decision aiding tool for FRs, without the need for advanced training. The program is developed by law enforcement in cooperation with UCD as a part of the "FREETOOL project"[20] that aims to develop free reliable tools for investigating cybercrime. The purpose of

[20] UCD.ie: https://www.ucd.ie/cci/projects/current_projects/freetool2.html

the program is to aid the FR in taking a qualified decision whether it is safe to power the machine off, or if LDF is necessary to prevent loss of vital data.

FiRST is designed to make minimal changes to the suspect´s system, but it is important for the FR to know that all programs will lead to changes on that system. By connecting e.g. an USB memory stick, there will be created USB-related registry keys, and by starting a program it will change memory while loading and executing the program. It may also add/update a file in the prefetch folder and add/update User Assist data value (UCD, 2018)

The LDF course at UCD describes three rules for when not to perform Live Data Forensics:

1. When critical data or information can be gained in any other way
2. When the required data or information has been acquired
3. With every new action justify the need to continue with LDF

Rules 1 and 2 are particularly important in the Identification Phase. Rule 3 is especially important if the principle of *"evidence integrity"* is to be followed. To be able to cancel further LDF examination when sufficient potential electronic evidence is acquired and/or extracted will be an important skill for the FR.

Similarly, there are rules for when LDF should be executed (UCD, 2018)

1. When switching the computer off is likely to make evidence inaccessible
2. Disk encryption is used, and no recovery key is available
3. Online disk storage is used, and access would be lost once the computer is switched off
4. When switching the computer off is impractical:
    a. Production servers in large organizations
        i. Amazon, E-bay
        ii. May put human lives at risk
        iii. Large monetary losses
        iv. If shutting off the system causes the system to crash – may result in lawsuit against the conducting law enforcement agency

5. When crucial data is likely to reside only in RAM (Random Access Memory)
    a. Instant messenger conversations
    b. Traces of computer intrusions/malware
    c. Passwords typed by the user
    d. Decrypted files or text
    e. Clipboard contents

6. When "post-mortem" techniques are not applicable due to the lack of resources or equipment:
    a. Evidence is contained on rare or custom-made storage
    b. Need to identify a small number of relevant systems among a large number or potentials with little time and/or resources

7. When intelligence information is needed quickly
    a. Kidnapping cases when the primary aim is to locate the victim whose life is in danger (incident response)
    b. Need to identify a location for a bomb treat on the suspect´s computer.
    c. Missing persons/persons wanting to commit suicide

When the decision to conduct LDF is made, it is, with every device, important to perform the least invasive action first.

- Take a photograph of the screen before doing LDF
- Suppose that we know that a certain tool is going to modify the registry, it makes sense to collect a copy of the registry first before it is modified by the tool.

When this is done make sure to collect the most volatile data first. UCD defines volatile data as "changeable, fleeting or transient". This is data that has the possibility to change and is often lost upon powering down the computer (UCD, 2018).

The "Order of volatility" is an important mindset in digital forensics. The term is based on the fact that investigations rarely involve just one single digital device, but that the potential

evidence may be present across multiple devices. If the Heisenberg principle of uncertainty[21] is applied to digital forensics then this will mean that it is impossible to gather all the information from a computer system without changing its state (Flaglien, 2018).

By following the order of volatility, the FR will prioritize which evidence source to be collected first according to the volatility of the data. This means that the most volatile data according to its value and relevance to the case should be acquired first.

Figure 9: Order of Volatility - examples (Flaglien, 2018, p. 31, table 2.1)

Type of storage media and data	**Typical storage lifespan and longevity (dependent on usage)**
System registers, peripheral memory, and cache	Nanoseconds
RAM	Ten nanoseconds
Network state	Milliseconds
Running system processes	Seconds
Data on disk (cache)	Minutes
Cloud storage	Months to years
HDD data storage	Years
Floppies, and other magnetic tape-based media	Years to decades
CD-ROM´s, DVD´s, print-outs,	Decades
Read-only memory; flash and SSD data storage	Decades to centuries

When collecting the different electronic evidence, using different tools, it is vital that the FR have knowledge of the tools used and their impact on the system. Some tools and actions may crash the live system, causing further LDF examination impossible.

Document everything: chain of custody is one of the two fundamental principles regarding forensically soundness (Flaglien, 2018). If this principle is to be followed, it is imperative to document all steps taken from the evidence was discovered until it was fully investigated.

[21] German physicist Werner Karl Heisenberg presented the uncertainty principle in 1927 which states that the position and the velocity of an object cannot be measured exactly, at the same time, even in theory.

At a minimum the following should be covered (Flaglien, 2018, p. 24 after Laliberte & Gupta, 2004):

- The person handling the evidence,
- Processes and procedures performed;
- The time and date of evidence acquisition;
- Original location of the evidence collected
- Method of collection, examination, and analysis; and
- The reason for collecting the evidence

The aim is to show the court that the digital evidence presented is no more and no less than when it was first taken into possession of law enforcement (ACPO, 2012). In cases where the evidence is changed as a consequence of our actions and thereby does not comply with the principle of *evidence integrity*, this becomes especially important. To support the chain of custody the process can be documented by various kind of data, for example:

- Photographs,
- Reports,
- Laboratory information management systems,
- Notebooks,
- Checklists,
- Log files, and
- Videos and screen capture

Detailed notes of everything the investigator has done to the system may help determine the impact of the investigator´s action on the system at a later date (UCD, 2018). Responding countries to UNODC reports that a variety of techniques are used to ensure the integrity of electronic evidence collected. Documentation is one of these techniques (UNODC, 2013).

It is important to emphasize that this section describes what the student should be able to do when they graduate. The knowledge of those who participated in the survey is far less. This is described in detail in Chapter 4 - Education.

Digital forensics and LDF is a large, complex, and in a historical perspective, a relatively new field. The field requires expertise in a number of specific areas. Standardization of models, terminology and methodology still seems to be challenging, both internationally and nationally. Yet, there are signs of the field moving in the direction of unified standards and definitions. In Norway national developed role descriptions with associated competence requirements for various roles within the police by POD is an example of this.
In our research we have not found previous studies describing how LDF is practically performed by NPUC students in Norway.

3. METHODOLOGY

In this chapter, we will address and describe the methodological choices and the procedures we have used in this thesis. We will describe our thoughts and justifications for the selection of respondents, ethical challenges related to our role as researchers and teachers, the design of questions and analysis of data.

The practice or techniques used to answer or illuminate research questions and scientific challenges can be defined as research methodology (Ringdal, 2007).

The purpose of research is to produce valid and credible knowledge of reality. To achieve this, the researcher must have a strategy for how he or she should proceed. This strategy is the method (Jacobsen, 2015). The method is about approaching and trying to uncover reality. In practice, this will be how we can collect empiricism about reality in the best possible way. The collected empiricism must be reliable and able to answer the questions the researcher wishes to elucidate (Jacobsen, 2015).

3.1 Choice of Method

Which method to use is an important and difficult decision to make for the researcher. When conducting any form of research, the method must be chosen based on the research question, e.g. what do we want to find out, what problem do we want to solve or what field of knowledge do we want a deeper insight in?

Social science is about the study of people. People have opinions and beliefs about both themselves and others. These beliefs and opinions are not static but constantly changing. The social science researcher is a participant in society and can not only be a spectator to what is being studied (Johannessen et.al., 2010 after Skjervheim, 1957/1976).

Natural science on the other hand relates to phenomena without language and the ability to understand themselves and their surroundings. It will not be possible to ask these study objects whether they are animals, cells, atoms, genes or a computer program (Johannessen et. al, 2010).

We wanted to find out how people, in our case NPUC students have performed certain tasks, and how they have considered themselves and others in relation to these performed tasks. It was therefore natural for us to use the social science method to get as good picture of reality as possible.

Our research is empirical in which the theory and hypotheses are supported by data. If a theory t is not supported by data, it becomes speculation (Svartdal, 2009). Our approach to this is by using the *deductive method*. The deductive method means that you have a theory where data is used to support or refute the theory you had on beforehand. So, you go from the very general (hypotheses) to the concrete using collected data (ibid). We had a hypothesis that students performed LDF while they were in practice despite their lack of competence.

In social science, a question is quickly raised in the choice of method between qualitative and quantitative methods (Johannessen et.al, 2010).

3.1.1 Qualitative Method

Qualitative methods will be more concerned with content than frequency. "*Qualitative method is about characterizing*" (our translation) (Repstad, 2007, p. 16). While the quantitative method, simply put, will revolve about numbers, the qualitative method is characterized by observation, fieldwork, interviews and text analysis. This is work that focuses on characteristics and traits, and that will be less suited to quantify (Repstad, 2007).

Qualitative method is not equally suitable if you want to investigate the prevalence of something within many people. It is more suitable for examining nuances in a smaller group (ibid).

3.1.2 Quantitative Method

Quantitative method can, simplified, be described as a method of counting e.g. how many people are using Windows 10 OS in Norway. One wants to find out to what extent something is widespread or how often it is used (Repstad, 2007). The approach will fetch many of its procedures from the natural scientific method. At the same time, it will adapt to the human phenomena and that it is people that are being studied (Johannessen et.al., 2010). The actual numerical material will be central, and it will involve a comparison of this (ibid).

The quantitative methods are, in many cases, called *extensive methods,* as they address several units, but the information collected is relatively closed as the information is pre-defined by the researcher in advance (Jacobsen, 2015).

The advantage of this method is that its capabilities to capture the prevalence of something among many. The survey is the most widely used method of collecting data as it is very effective and many can respond in a short time (Svartdal, 2009).

A challenge with the quantitative methodology is that it relies largely on the analysis of data collected. Data is not actual reality, but more or less successful representations of reality. Even the most accurate observation will not be able to capture the authentic reality. Reality will be too complex (Johannessen et. al., 2010).

The choice of method does not mean that one must chose only one or the other. The methods can also be combined (Repstad, 2007). As a researcher, you want to illuminate the research problem in such a timely and valid manner as possible. According to Repstad, a combination of methods will give “a broader data base and a safer basis for interpretation” (our translation) (Repstad, 2007, p. 29).

The different methods will have different challenges related to the actual method as such, and to what considerations the researcher must take to the assessment of outcomes and to ethical issues around their own role.

The scope of this thesis was to find out how many of the students had performed LDF during their practical year. Did they perform LDF according to basic principles and current methodology? Which electronic devices are the subject of LDF examinations? We wanted to collect data material so we could get knowledge about how many of the students had experiences related to our questions, whether these were local experiences, or was applicable to students from all the police districts in Norway.

In quantitative surveys, those being examined are called *units* and what is examined *variables* (Johannessen et. al., 2010). As teachers in the subject Digital Policing and Investigation at the NPUC, we were in a particularly favourable position with the opportunity to use the students who had had practice within all the police districts in Norway as units. By choosing survey, we would be able to get a large number of units, and at the same time ensure that the response rate would be high. We or another teacher could be present when the Survey was conducted. According to Svartdal, the presence of the researcher will lead to the answering of this more conscientiously (Svartdal, 2009).

The quantitative method and survey as a data collection method was chosen as we believe that this would give us the best answers to our research questions within our timeframe.

Based on the above reasoning, qualitative method and survey as a data collection method were chosen. In our opinion, these are best suited to illuminate the research questions and the research problem in the best possible way.

3.2 Population and Variety

In social science, population may refer to objects, but most often this refers to the people or entities to which a problem relates (Johannessen et.al., 2010). In this thesis, population will refer to students in the class of 2017-2020 at the NPUC while they attended their practical year (2018-2019) in one of Norway's twelve police districts.

When a survey is conducted, those who are asked to participate are called *population*. Our study includes the entire population. If one had to make a selection within the population, it would be problematic to decide how to make such a choice and to the degree which the selection matched the ones one optimally wanted to study (ibid).

All students were informed about the survey and asked if they wanted to participate. Neither we nor other teachers became aware of students who would not participate in the survey. It is not possible for us to find out if this was actually the case as the response rate is not 100 percent. The chance of achieving that all who receive e.g. a survey will respond is small. There will always, for several reasons, be respondents that does not answer a survey. This is a source of error it is important that the researcher is aware of (Johannessen et.al., 2010).

3.3 Data collection

According to Svartdal (Svartdal, 2009), surveys are both effective and the most widely used method in psychology and social sciences. Surveys with closed response options for collection of primary data is most used in quantitative methods (Jacobsen, 2015). Closed questions are questions that the researcher has pre-defined and that forces the respondent into established response categories such as: yes, no, do not know etc. (ibid.).
By using this method, information from multiple devices can easily be systematized and analysed in a standardized form by a computer (Jacobsen, 2015).

According to Johannessen, standardization such as fixed question and answer-alternatives will allow the researcher to look at the similarities and variations that respondents respond to (Johannessen et. al., 2010).

Three elements will be central when planning data collection by survey; what we want to measure must be *concretized* (operationalized) and the questions must be *designed* in such a way that undesirable results are not created based on imprecise question design. The researcher must *decide* how he/she would like to conduct the survey itself, e.g. mail, personal interview, via internet/mobile phone etc. (Jacobsen, 2015).

3.3.1 Survey - General Information

All employees and students at NPUC have license and access to the Microsoft Office 365 software Package. We chose to use Microsoft Forms, which is part of this package to conduct our survey. Microsoft gives the following description of this program/app:

"*Microsoft Forms is a simple, lightweight app that lets you easily create surveys, quizzes, and*

polls. In educational institutions, it can be used to create quizzes, collect feedback from teachers and parents, or plan class and staff activities. In business organizations, it can be used to collect customer feedback, measure employee satisfaction, improve your product or business, or organize company events"[22].

There are many advantages when using such an easy to use and simple application. The major advantage for us was the fast and efficient data collection. It is also very easy to use for respondents. The survey could be conducted on PC/mobile and all known Operating Systems. We shared a link on the learning platform "Canvas"[23]. The students accessed the survey via this link and completed the survey. Most students used less than 10 minutes to complete. We chose that the survey would be anonymous and that it could only be completed once for each respondent. In the aftermath, we as administrators of the survey could see the answers and details presented in the form of various diagrams internally in the program. The results could then be exported as a Microsoft Excel file. We chose to conduct the survey in Norwegian, the student's native language. We did this to avoid unnecessary error sources and misunderstandings. In the appendix, the survey is translated into English.

3.3.2 The design of the survey

A questionnaire/survey must be designed to provide answers to the research problem/questions, or to illuminate this in the best way possible. The questions should be as specific as possible, making it easier to answer, and easier to interpret the data afterwards (Johannessen et al., 2010). Often, researchers use questions and/or the design from other researchers' completed surveys. This is considered a good practice. In this way, one can compare one's own results with those of others (if questions and answer options are identical). However, we did not find surveys from others on the same topic, so we had to design the survey from scratch. To compensate for this fact, we were well assisted by several highly competent professionals at NPUC who have conducted extensive researches themselves.

In qualitative methods, such as when using an interview, the researcher can adjust data collection along the way. This is not a possibility when using a survey. This means that you

[22] Microsoft forms webpage:https://support.office.com/en-us/article/frequently-asked-questions-about-microsoft-forms-495c4242-6102-40a0-add8-df05ed6af61c
[23] https://www.instructure.com/canvas/

must have done thorough research before completing the survey (Johannessen et al., 2010). To comply with this, we conducted the survey on all teachers in the subject Digital Policing and Investigation at NPUC.

A survey can be very structured, i.e. with a set of standardized questions with a fixed scheme, but it may also contain open questions where respondents can write down their own answers. The former is defined as pre-coded or pre-structured surveys (Johannessen et al., 2010). You can use a combination of open and pre-coded responses, and then the questionnaire is referred to as semi-structured (ibid). Our survey is semi-structured, as we have some open questions in the last section.

We chose to divide the survey into different sections. These are:

1. Introduction
2. Background questions
3. Knowledge questions
4. Experience questions
5. Open questions

Comments on Section 1:
In order for students of the various campuses to have as similar prerequisite and basis as possible, we agreed with teachers who were responsible for conducting the survey that they should not teach or provide other information in the subject before the survey was initiated and completed. The introduction in the survey was designed to make sure that everyone had sufficient information prior to answering the survey questions. As described in chapter 4 - Education, the students had limited education in LDF during the first year of study. Therefore, there was a need to refresh the term LDF. This is done in the survey's introduction. There is also information that the survey is anonymous and voluntary.

Comments on section 2, 3 and 4:
These sections of the survey have pre-coded answers, and in some of the questions we use a five-part scale, which is graded in range from "very low" to "very high" (1-5), with as many options on either side of the middle value (3). By designing the grading in this way, the respondent can answer "neutral" in questions they have no particular opinion about. This

scaling/grading is recommended by Johannessen (Johannesen et al., 2010, p. 266 after Haraldsen, 1999).
Questions 18, 19 and 22 have response options in the range from 1 to more than 6. The reason for this is a limitation in Microsoft Forms. This has the consequence that in these questions the results will be a minimum number as we do not know how many “more than 6” is.

Comments on section 5:
In the final section of the survey, we chose to include three open questions. According to Repstad a combination of methods such as elements of open questions, provide a broader data base and a more secure basis for interpretation (Repstad, 2007). The downside may be that it provides an unmanageable amount of data, and that it is more time-consuming to analyse. The disadvantage of pre-coded responses is that it can be perceived as limiting for the respondent, and that one can miss important responses/data that fall outside the pre-coded options (Johannessen et al., 2010).
The three open questions we chose to include in the survey gives the respondent the opportunity to share their own considerations. Further, this would give us an answer to whether the survey lacked any questions or had formulations that did not cover the student’s experiences during their practical year.

3.3.3 Conducting the survey

The survey was conducted on Monday 26.08.19 in Bodø and Stavern, and 27-28.08.19 in Oslo. We chose to conduct the survey at this specific time for several reasons. On all three campuses, the survey was conducted in conjunction with the start-up hours of the subject Digital Policing and Investigation. The main reason was that at this point, the third academic year (B3) had recently started. The impressions from the practical year were likely to be "fresh in memory" and not influenced by further education in LDF and/or the Digital Forensic Process. The survey progressed without technical problems, except for one “round” in Oslo, where they had problems with the wireless network. Half of Oslo's class, approx. 200 students could not perform the survey during the planned time. These were given access to the survey after class, so they could respond to the survey later the same day. The response rate from these students was low.

3.4 Data Analysis

To analyse the data collected, we have used two programs; Microsoft Forms own analytics tool and IBM SPSS Statistics (Statistical Package for the Social Sciences) ver. 26, 64-bit edition. According to Svartdal this is a very good statistical program (Svartdal, 2009).

Results based on how the units are distributed on a property or one variable e.g. how many students have responded from each police district is called *univariate analysis* (Johannessen et.al., 2010). Microsoft Forms presents results based on the *univariate analysis*. SPSS was used both for mentioned *univariate analysis* and to analyse the correlation between variables. An examination of the connection between two variables is called a *bivariate analysis* (Johannessen et.al., 2010). In our survey an example of such analysis is e.g. the relationship between the perceived competence within LDF and the actual competence (Table 8).

3.5. Response rate and dropouts

At the Norwegian Police University College there are a total of 710 students in the class of 2017-2020. Everyone had the opportunity to participate in the survey. 552 of 710 students responded to the survey. This is a response rate of 77.75% and a 22.25% dropout.

The number of student's is distributed as follows at the College's three campuses:

Bodø: 133 Students of 145 have responded, which corresponds to a response rate of 91.72%.
Oslo: 265 Students of 406 have responded, which corresponds to a response rate of 65.27%.
Stavern: 154 Students of 159 have responded, which corresponds to a response rate of 96.85%.

There is a big difference between the response rate of the three campuses. Oslo has a significantly lower response rate than the two others. The technical problems as mentioned earlier is likely to be the most probable cause for the high dropout-rate in Oslo. This is backed up when analysing the answers/results against time/date, where it is clear that there are few answers from the group that had technical problems when conducting the survey.
Some students, at all three campuses, have for unknown reasons chosen not to respond to the Survey.

Three of the questions in the survey were open. One of these had corresponding response rate as the rest of the survey (552) while two of the questions had a very low response rate.

Question 31: *Did you experience anything in the practical year regarding the use of LDF that is not covered by the survey questions and that you would like to share?*

This question was answered by 172 students, which corresponds to a response rate of 24.37%.

Question 32: *Is there something specific we should have focused more or less on in the subject "Digital Policing and Investigation" in order for you to be better prepared for your practical year?*

This question was answered by 254 students, which corresponds to a response rate of 35.78%.

Research on non-responses shows that, it is often, not accidental that some groups dropout and that there are specifically three groups this applies to (Jacobsen, 2015).

Dropout groups are:

- Those who are not interested in the issue
- Those who have no knowledge about the questions they are asked
- Those who do not want to pronounce themselves

What the reason for the dropout of these questions from our respondents is uncertain. All types of dropout will affect the ability to generalize from sample to population (ibid)

Question 31 was made part of the survey to provide us with information regarding whether the questions of the survey covered the experiences students had during their practical year. Question 32 were aimed at the actual teaching in the subject to see if the education prior to the student's practical year was sufficient.

In retrospect, we see that these questions have less value for the research questions as such.

3.6 Quality assurance

3.6.1 Validity

If a claim is supported by research, we can say that it is durable. If inferences, theories and concepts can be documented, it is in this context durable (Svartdal, 2009).

In quantitative studies, validity can be divided into two types; *internal* and *external validity*. *Internal validity* will be related to whether the measuring device itself (usually surveys) measures what we want to measure. This means that what we question in the survey actually measures what we want to measure. The questions we have used in our survey are reviewed by several researchers, and by teachers in the subject. The terms we have used are both explained in the survey and known from previous teaching for the respondents.

In the Introduction to this thesis we have explained what our education and personal experiences in this field are. In the choice of data collection method we have put focus on the fact that our role as teachers in this subject may have had an impact on how students responded to the Survey.

In some questions the respondents are asked to evaluate their own competence. We are aware of that there is a possibility that respondents with low competence may evaluate their competence higher than it is due to the "Dunning-Kruger effect" (Kruger & Dunning, 1999). To measure if this effect had an impact on the results, the respondent's self-evaluation was compared with questions that measure their actual competence. We did not see any significant signs of the Dunning-Kruger effect in the results.

When people are being observed, a change in behaviour may occur as a response of being observed, this is known as the "Hawthorne effect" (Leedy & Ormrod, 2014). This may lead to self-bias were the respondents answer what they believe the researcher wants them to. To the extent to which this was relevant for our respondents is unknown, but the probability for this is considered when results are discussed.

Our intention and desire for this thesis has been to focus on to what extent, and how LDF is performed by students in practice. The intention has been to illuminate this in the best

possible way by using adapted methodology and Survey as data collection method. We have no personal agenda attached to this and thus should show that we are not biased.

The *external validity* is related to whether the selection we made of respondents can be generalizable from the sample to the total population (Jacobsen, 2015). For us, this was not a real issue as we examined the entire population. Our overall population response rate is 77.75%. According to other researchers and an article published by Ottar Hellevik (Hellevik, 2016) a response rate of 50-60% would be good. In the same article, it is referred to the American book "Approaches to Social Research" stating that a response rate of 85 % is one should preferably have (Hellevik, 2016 after Singleton et.al., 2005 . Based on this we can say that our survey has a good response rate and thereby a hypothetical external validity. hypothetical external validity.

We are aware that in a research context, our survey has a high response rate. This may be interpreted by some as a sign that respondents have been pressured to participate. A survey conducted in a hierarchical organization like the police can reinforce this view. It is important for us to emphasize that we feel that our students are genuinely interested in contributing to the positive development of the police as such and to the development of the field of Digital Policing and Investigation. In our experience the students are eager to share experiences they have gained while in practice with each other. This is in line with the goal of the Norwegian police; to be knowledge-based and a learning and development-oriented police.

3.6.2 Reliability

Reliability is about the credibility and consistency of the results. If the same survey is performed several times and has the same result one can say that it has credibility (Svartdal, 2009). Our study has been conducted on students at the Norwegian Police University College`s three campuses. The results show that there are small, or no differences in responses based on the different campuses. The survey is further tested on selected qualified people (as mentioned in 3.3.2), showing the same similarities.

3.6.2 Ethics and the role of researchers

Social science surveys have consequences, both for the respondents and the society. The researcher is obliged to consider ethical issues, of which there are often no clear answers to (Jacobsen, 2015). According to Jacobsen, there are three basic requirements which needs to be taken into consideration in the relationship between the researcher and the respondents; informed consent, privacy and correct presentation of data.

Informed consent, i.e. the respondent voluntarily participates in the research. We believe that we have covered this requirement with both oral information in advance of conducting the survey, and that it is mentioned explicitly in the introduction part of the survey.

Regarding *privacy*, the researcher must assess several moments. How sensitive is the data? Is it possible to identify individuals through data collected? How serious is the consequences of being identified? These factors took a lot of time to consider when designing the survey. With our design of the survey, we believe that one will not be able to track/associate data with specific individuals. The answers are anonymous. Only we have access to the full dataset. Anonymization of data has been carried out where needed. Since we are students at UCD, but collect data in Norway, we encountered some issues. In Norway, it is "Norsk senter for forskningsdata" (NSD)[24] which assesses whether the research is subject to notification or is subject to a license. We had a dialogue with NSD before designing the survey. NSD concluded that UCD is the data controller, and that we did not need further dialogue with the NSD in Norway. Our supervisor at UCD consulted with UCD Office of Research Ethics, and we received feedback that our survey was a "Low risk/exemption" not to be considered for further applications within UCD. We have also taken NPUC's own ethical guidelines[25] for research into account. We discussed with our department head, Professor Per-Ludvik Kjendlie and cleared that we could conduct the survey at NPUC.

The last requirement is the requirement for the *correct presentation of data*. This means that, as far as possible, the researcher should try to reproduce results completely and in the right context. This will be something one should strive for, but that will often be impossible to

[24] https://nsd.no/

[25] https://www.phs.no/Documents/4_Forskning/Forskningsetisk%20veileder%20PHS.pdf?epslanguage=no

achieve (Jacobsen, 2015). Transparency about what one has done is an important principle. *"Only when the choices are explicit one can criticize, and only then can one assess how good the research has been"* (our translation) (Jacobsen, 2015, p. 52-53).

We have (after the survey has been completed), come to the realization that we have included some questions in the survey that we would not have included if we were to do it again. We have probably gone into some of the classic pitfalls inexperienced researchers tend to do. Among other things, we have fallen for the temptation to collect more data than was strictly necessary to elucidate the research problem.

4. EDUCATION

4.1 General information about the education:

In this thesis, we have focused on the students who are attending NPUC 2017-2020, in total 710 students spread across three campuses. To give the reader an impression about the student's knowledge and competence, it is necessary to give a general overview of the Bachelor program content, before describing the subject Digital Policing and Investigation.

"*The Norwegian Police University College is an education institution for the police service and county administrative officials in Norway, with its own board as its highest authority. Administratively, PHS resides under the Norwegian Police Directorate, and its purpose is to provide fundamental training for service in the police service or county administration, as well as post graduate studies for employees of the police service. PHS also carries out research and development and handles work-related communication within its professional areas. PHS have three college locations: Oslo, Bodø and Stavern*"[26].

The first year of the study is theoretical, on campus. The second year is the practical year, where the student is out in service in a police district, either at a police station or in a sheriff's office. The last year is theoretical, back on campus.
There are 60 credits for each year, a total of 180 credits for the entire education. The education program consists of 5 main education areas that are consistent through the 3 years.

[26] https://www.phs.no/en/about-phs/

Figure 10: First academic year (B1) (Digital Policing and Investigation outlined in red)

First Year		
Main Area	**Subject**	**Credits**
Police and Society	Sociology	4
	Police Science	5
	Administrative Law and Civil Law Topics	2
	Work Ethics	2
Methodology	**Digital Policing and Investigation**	4
	Scientific theory and Research Methods	2
Order and Emergency Response	Uniformed Police Service	5
	Physical Fitness Training	2
	Communication and Conflict Management	2
	Psychology	4
	Road Traffic Law	3
	Apprehension Techniques	2
Crime Prevention	Crime preventing Police Work	3
Investigation	Criminal Law and Criminal Procedures	10
	Report Writing and Criminal Investigation	6
	Forensic Science	4

Figure 11: Second academic year (B2) (Digital Policing and Investigation outlined in red)

Second Year		
Main Area	**Subject**	**Credits**
Police and Society	Police Science	2
	Administrative Law and Civil Law Topics	2
	Work Ethics	3
Methodology	**Digital Policing and Investigation**	2
Order and Emergency Response	Uniformed Police Service	24
	Physical Fitness Training	
	Communication and Conflict Management	
	Apprehension Techniques	
	Training for Emergency Response Personell	4
	Traffic Patrol Duty	3
	Emergency Response Driving	3
Crime Prevention	Crime preventive Police Work	7
Investigation	Investigation	10

Figure 12: Third academic year (B3) (Digital Policing and Investigation outlined in red)

Third Year		
Main Area	**Subject**	**Credits**
Police and Society	Criminology	4
	Work Ethics	3
Methodology	**Digital Policing and Investigation**	4
	Bachelor Disseration (and Scientific theory and Research Methods)	10
Order and Emergency Response	Uniformed Police Service	5
	Training for Emergency Response Personell	4
	Communication and Conflict Management	4
	Apprehension Techniques	2
Crime Prevention	Crime preventive Police Work	10
Investigation	Investigation	14

4.2 An overview of the content in the subject Digital Policing and Investigation:

As shown in the figures above, the students attend the subject Digital Policing and Investigation (DPI) throughout all three academic years. The subject belongs in the main area Methodology and is 10 credits in total.

4.2.1 The first year (B1)

Description of Methodology from the NPUC curriculum 2017-2020 (our translation) (Politihøgskolen (PHS), 2017b):
Method is an interdisciplinary main area that is consistent for the entire Bachelor's program. Topics of Science Theory, Research and Digital Policing and Investigation constitute the academic contributions in this main area of the first year of study.
Norwegian police shall work knowledge based. It involves a scientific approach by systematizing their own experiences and by using different sources of knowledge. To work knowledge based in modern Norwegian society further implies that the police have to deal with the potential of digital information to affect all policing through collection, registration and analysis.

Method involves systematic procedures that ensure valid knowledge. The purpose of the main area is that the student will be able to conduct knowledge-based policing and make reflected choices between the police work's many sources of knowledge. Moreover, he/she will acquire knowledge of the most important methods of research and Digital Policing and Investigation principles.

General competence:
The student can after the first year of study:

- Understand the importance of and contributing in reflection on knowledge-based policing

The subject Digital Policing and Investigation has the following description and learning objectives in the first year (ibid):
Digital Policing and Investigation is a subject that aims to put the student into relevant digital dimensions of police work. The police rely on various computer systems to solve their tasks. In a modern society, a lot of communication and socialization takes place in the digital world. Modern police must have knowledge of social media and how different groups act on them. Police staff must have high awareness of issues related to data security. The police should have an ethical awareness of how to manage information from different registers, and professional insight into how digital information will be applied in various police tasks. The contents of the digital police work must be seen in the context of other policing topics such as Order and Emergency Response, Forensic Science, Crime Preventive Police work and Investigation.
In the first academic year, the subject focuses on providing the student with an introduction to information technology that lays the foundation for further work on the subject. Moreover, after the first year of study, students will have a practical understanding of how to handle digital devices
The learning objectives are divided into three areas: Knowledge, skills and general Competence.

Knowledge:
The student has after finishing the subject knowledge of:

- How Internet and networking, including mobile communication networks works

- Information gathering from the Internet
- How electronic devices (computers, mobile phones, etc.) hardware and software works
- The importance of documentation when examining digital devices
- Computer Security
- Prevention of unwanted behavior on the internet
- How various electronic traces are generated and how to secure dem
- Key elements in the "Electronic Communications Act" (a Norwegian law regulating providers of electronic communication services - ISP/mobile operators etc.)

Skills:

The student can after finishing the course:

- Use the Police Case management tool for criminal cases (BL – Basis Solution, a computer program) to prepare reports
- Apply relevant search techniques on the Internet
- Identify storage media that may contain evidence
- Identify providers of Internet and phone services and obtain subscription information

General competence:

The student can after finishing the course:

- The potential proof value a digital device may have in a criminal case
- Follow the police code of Ethics and privacy with the use of police Computer systems
- Acting critically and reflected in the digital space

Organizing and working methods:

It is expected that the student works approx. 120 hours with the subject. In this, participation in teaching, individual work, teamwork and literary studies are included.

The instruction relating to the Police Case management tool for criminal cases (BL) is seen in the context of the subject of Report Writing and Criminal Investigation.

Work requirements that must be approved before the student is given the exam:

- Compulsory participation
- Conducting online courses in the Police Registry Act

- Written work assignments to be presented

Assessment:
Individual written exam assessed to pass/no pass.

4.2.1.1 Digital Policing and Investigation, the content of the education in the subject during the first year:

A total 30 hours of teaching in the subject during the first year. The topics were:

- Hardware, central components and which may contain potential digital evidence.
- Operating systems and file systems
- Network
- Internet (IP Protocol, TCP/UDP, DHCP, Internet Governance, DNS, search and search techniques)
- Computer security (different threats, malware)
- Mobile communication and network
- Mobile phones (SIM cards, devices, rules and regulations)
- Digital evidence (Methodology, ACPO guidelines, LDF)
- Digital Investigation
- Exercise, practical

First year education and LDF:
The education in the subject has been on a basic level. Regarding LDF, we have had focus on the “main rule” in the DFP. Briefly the methodology suggests that the police generalist (FR) is supposed to identify and secure the digital devices, and then deliver them to a DFD for further examination. The student should be able to clearly distinguish between the task the FR should do, and what the DFD should handle. This is further described in chapter 2 - State of the art. The students should understand that devices that are turned on should remain on (depending on the case, network isolate them) and that devices that are off should remain off. We have had some small “portions” on LDF, and we have focused on LDF as an deviation from the methodology and the “main rule”. There should be a good reason to perform LDF. The reasons may vary from life and health to the risk of losing potential evidence. We have

repeated this message several times during the first year, in theoretical sessions and in two practical exercises. The students did not receive training in performing actual LDF. This is due to limitations in total education time and the need to cover many other different topics in the subject.

Exam - first year:
The exam had a duration of 3 hours. The students were in a controlled environment (classroom) with an online exam solution called “Inspera”. This program makes sure that the students can’t access internet or open document etc. while they have the exam. The exam contained different categories of questions; multiple choice, short answer and two exercises (cases) in which the candidate had to put themselves on i.e. a crime scene performing search and seizure. The latter required a longer answer. Maximum score was 100 points, and 65 points was needed to pass the exam. There were two questions related to LDF. Both were about “pulling the plug” on a desktop computer.

4.2.2 The second year (B2)

During the second and practical year, the students have several learning goals in the subject DPI. Mostly this is the different work-related Police computer programs the students encounter. These goals are not related to the scope of this thesis and will not be included. A short description of the content of the second year will be given, so that the reader could get an impression on what the second academic year contains.
The second academic year is a practical study and is conducted in a police district. The students participate in various parts of the police work and receive training and guidance. Students are assigned limited police authority during this year.
Students will solve assignments under supervision. At the beginning of the academic year, students will learn to a large degree through observation, but eventually they will also perform work tasks on an independent basis.
The practical year is essentially based on experience learning. In this learning form, a great emphasis is placed on guidance. The guidance, which is mainly conducted by the Supervisor, is intended to help make the students familiar with the practice field and with their own prerequisites for working as a law enforcement person.

The Supervisor is responsible for the guidance of the student in daily service. In addition, planned guidance conversations between student and practice guides will be conducted in the academic year. Practice supervisor and student share responsibility for the guidance talks. The students will take participate in different areas within the police, among others; Patrol duty, Investigation and Crime prevention.

4.2.3 The third year (B3)

The third year consists of more advanced teaching and benefits on the experiences and knowledge the students have from the practical year. The investigative role is more central, and the focus on investigation is clearer.
The main area of methodology has the same description as in the first year, but the learning goal is a little bit different:

General competence:
The student can after the third year of study:

- Assess various sources of knowledge critically and contribute to knowledge-based police work

Digital Policing and Investigation will put the student into relevant digital dimensions of police work. The police rely on various computer systems to solve their tasks. In a modern society, much communication and socialization take place in the digital world. Cybercrime is a growing social problem and the police must be able to prevent and investigate cybercrime. Today, it is almost a rule that electronic evidence contributes as evidence in a criminal case, and police must be able to employ a wide range of digital sources of information to illuminate the events they investigate. The contents of the Digital Policing and Investigation must be seen in the context of other subjects such as Uniformed Police Service, Forensic Science, Crime Prevention and Investigation.
In the third academic year, students will be trained in online investigations and how they can secure and analyze electronic evidence and how they can use electronic evidence in an investigation. Students will also have a focus on writing reports in connection with securing and analyzing digital evidence.
Learning objectives:

Knowledge:

The student has after finishing the course knowledge of

- The polices work and presence online
- Rules, principles and methodologies related to information gathering from open sources
- Principles for handling and examination of digital devices

Skills:

The student can after finishing the subject

- Identify and secure evidence on the Internet
- Use data tools for electronic evidence processing and analysis
- Handle digital devices according to current methodology so that data is in a least possible way is affected, altered or lost
- Search, secure and group information from open sources to prevent and predict crime

General competence:

The student can after finishing the subject

- Document and present investigation of electronic evidence
- Show understanding which evidence value electronic evidence can represent in the Investigation
- Use a methodical procedure when investigating electronic evidence
- Distinguish between generalist and specialist tasks related to electronic evidence

Organizing and working methods:

It is expected that the student works approx. 120 hours with the subject. In this lies teaching, individual work, group work, exercises and literature studies.

Parts of the instruction as well as work requirements and examinations will take place in the main area investigation.

Work requirements that must be approved before the student is given the exam:

- Compulsory participation
- Conducting training in the program FIRST
- Tasks related to selected topics within the subject

Assessment:
Digital Policing and Investigation is part of the examination of the subject of investigation. Individual oral exam.

4.3.1.1 Digital Policing and Investigation, the content of the education in the subject during the third year:

There is approximately 30 hours of education in the third year. Starting this year, DPI is also delivering 12 hours of OSINT education in the topic Crime Preventive Police Tasks, so the total education will be around 42 hours. The topics were:

- The Digital Forensic Process – methodology
- Internet Investigation in general – IP addresses, domain name searches
- Internet investigation – social media
- Blockchain and Crypto Currency
- Analysis – cell phone traffic, legislation and practical analysis, timelines (3 sessions in total 6 hours)
- Forensic file copying
- Online abuse (internet)
- LDF – first responder
- FIRST - theory and practical use
- Exercise (LDF theme)
- OSINT (6 sessions, in total 12 hours). Methodology, image searches, reverse image search, EXIF/metadata, maps and geolocation, case work, analysis, report and presentation

Third year education and LDF:
The education in the subject has overall been on a more advanced level compared to the first year. Regarding LDF, we still focus on the main methodology (main rule), but in the third year we have more topics in LDF and triage. We have a separate lesson in First Responder, and later teach the students in the practical use of the program “FiRST” (with permission from the developers). This year, the students were given three different cases involving LDF.

One session with the use of FiRST on a Windows laptop, one session with LDF on an Android mobile phone and one session with a theory assignment about LDF in general.

Exam - third year:
The exam in the subject "Investigation", which DPI takes part in, is an oral exam where each student is given a case and have to give an oral presentation containing many different "investigate steps". When DPI are present in the commissions, the students have to show that they have knowledge in different scenarios containing electronic evidence. In some of the scenarios, LDF is relevant. The exam is graded.

Note:
This year, 2019-2020 DPI is merged with Forensic Science for students in the first academic year (B1). From the academic year 2020-2021, the subject will be moved from main area Method to main area Investigation. The aim of this is to merge the subject closely with Investigation. Furthermore, the subject has been given additional hours in connection with education within OSINT. OSINT has increased in size and has been moved to the subject Preventive Police Work.
As a consequence of these structural changes the subject DPI has an overall increase in size with approximately 40%.

5. ANALYSIS AND RESULTS

5.1 Analysis

This section will describe the results and our analytic approach in the same order as they are presented in the Survey. A selection of results has been done and will be presented in this chapter.

A descriptive method[27] is used as the results describes how a condition was experienced or performed by the respondents. In this section the possible reasons for the results will not be addressed. This will be discussed in chapter 6 – Discussion.

[27] https://snl.no/deskriptiv

A *univariate analysis* has been used as the primary method except for a few results which are based on a *bivariate analysis*. These results will be described in more detail.
By using Microsoft Forms as platform, the results have limitations. Questions with answers ranging from 1 – 6+ makes it impossible for respondents to answer 7, 8, 9, 10 etc. This limitation leads to all questions with this range will be displayed with a minimum number.

Data from the survey has been processed in IBM SPSS Statistics and Microsoft Excel for an easier view and understanding. Pearson's product-moment correlation was also used to examine the relationships between the respondent's theoretical knowledge, respondent's practical execution, subjective rating of own knowledge and subjective rating of supervisor's knowledge. The results will be presented in tables and/or figures with further explanations below when needed.

5.2 Results

Table 1: General information about respondents

Gender	Frequency	Percent	Valid Percent
Female	256	46,4	46,4
Male	296	53,6	53,6
Total	552	100,0	100,0

Age	Minimum	Maximum	Mean
	21	39	24,40

Campus	Frequency	Percent	Valid Percent
PHS Bodø	133	24,1	24,1
PHS Oslo	265	48,0	48,0
PHS Stavern	154	27,9	27,9
Total	552	100,0	100,0

**Total population 710*

There is a small preponderance of males in the respondents. The youngest respondent is 21 years and the oldest 39 years. 24.4 years is the students mean age.

Table 2: Respondents split by police districts

District	Frequency	Percent	Valid Percent	Cumulative Percent
Agder	36	6,5	6,5	6,5
Finmark	20	3,6	3,6	10,1
Innlandet	38	6,9	6,9	17,0
Møre og Romsdal	35	6,3	6,3	23,4
Nordland	40	7,2	7,2	30,6
Oslo	59	10,7	10,7	41,3
Øst	61	11,1	11,1	52,4
Sør-Øst	80	14,5	14,5	66,8
Sør-Vest	59	10,7	10,7	77,5
Troms	20	3,6	3,6	81,2
Trøndelag	47	8,5	8,5	89,7
Vest	57	10,3	10,3	100,0
Total	552	100,0	100,0	

**All districts in Norway represented. Sør-Øst district has the highest percentage*

Table 3: Respondents use of private technology

Mobile phone

	Frequency	Percent	Valid Percent	Cumulative Percent
Android;	136	24,6	24,6	24,6
Android & Other	1	0,2	0,2	24,8
Other	4	0,7	0,7	25,5
iPhone	409	74,1	74,1	99,6
iPhone & Android	2	0,4	0,4	100,0
Total	552	100,0	100,0	

Private hardware/OS

	Frequency	Percent	Valid Percent	Cumulative Percent
Other	1	0,2	0,2	0,2
Mac	305	55,3	55,3	55,4
Mac & Windows	23	4,2	4,2	59,6
Windows	221	40,0	40,0	99,6
Windows & Other	1	0,2	0,2	99,8
Windows & Linux	1	0,2	0,2	100,0
Total	552	100,0	100,0	

The respondent's use of private technology deviates from the Norwegian market share. They use Apple products to a greater extent than the Norwegian population (iOS 54,18%, OS X 16,02%)[28].

[28] Statcounter: https://gs.statcounter.com/os-market-share/all/norway#monthly-201910-201910-bar

Table 4: Respondents conducting LDF during their practical year

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	296	53,6	53,6	53,6
No	256	46,4	46,4	100,0
Total	552	100,0	100,0	

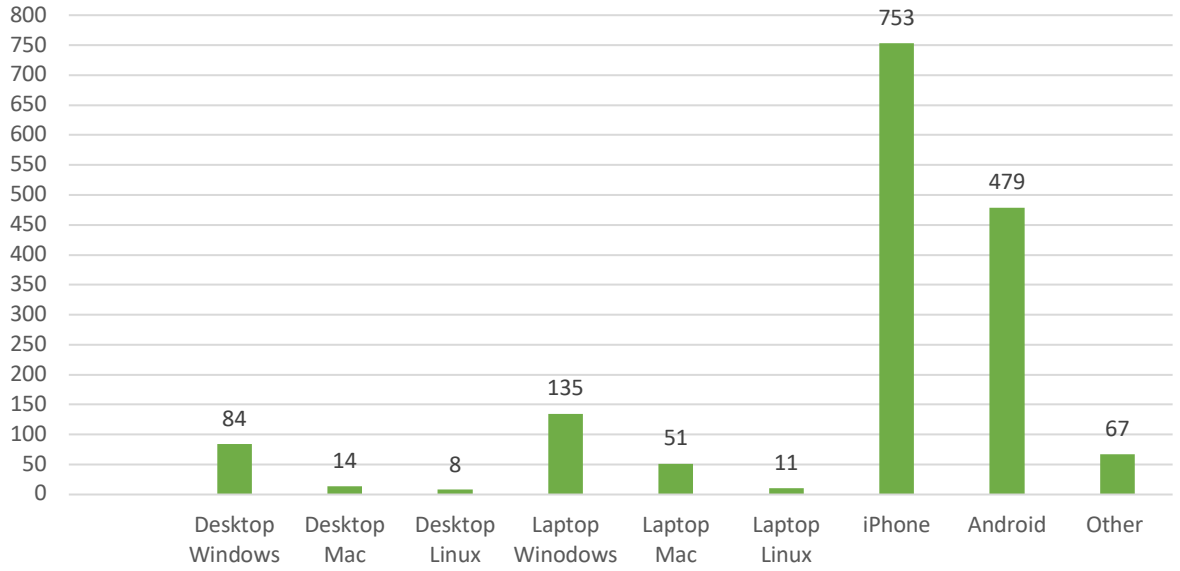
53,6% of the respondents answer that they have performed LDF during their practical year. This includes cases where respondents performed LDF alone, with their supervisor or with other police officers.

Table 5: LDF performed on hardware/OS

Count	1	2	3	4	5	6+	Total	Percent
Technology								
Desktop Windows	23	11	4	4	1	1	84	5,24
Desktop Mac	5	3	1	0	0	0	14	0,87
Desktop Linux	0	2	0	1	0	0	8	0,50
Laptop Windows	42	21	10	1	1	2	135	8,43
Laptop Mac	19	9	2	2	0	0	51	3,18
Laptop Linux	5	1	0	1	0	0	11	0,69
iPhone	65	78	43	33	11	36	753	47,00
Android	71	69	24	10	4	23	479	29,90
Other	15	6	4	4	0	2	67	4,18
Total LDF performed							1602	100,00

***** The column "*Total" is a minimum number as 6+ is counted as 6.*

Figure 13: LDF performed on hardware/OS



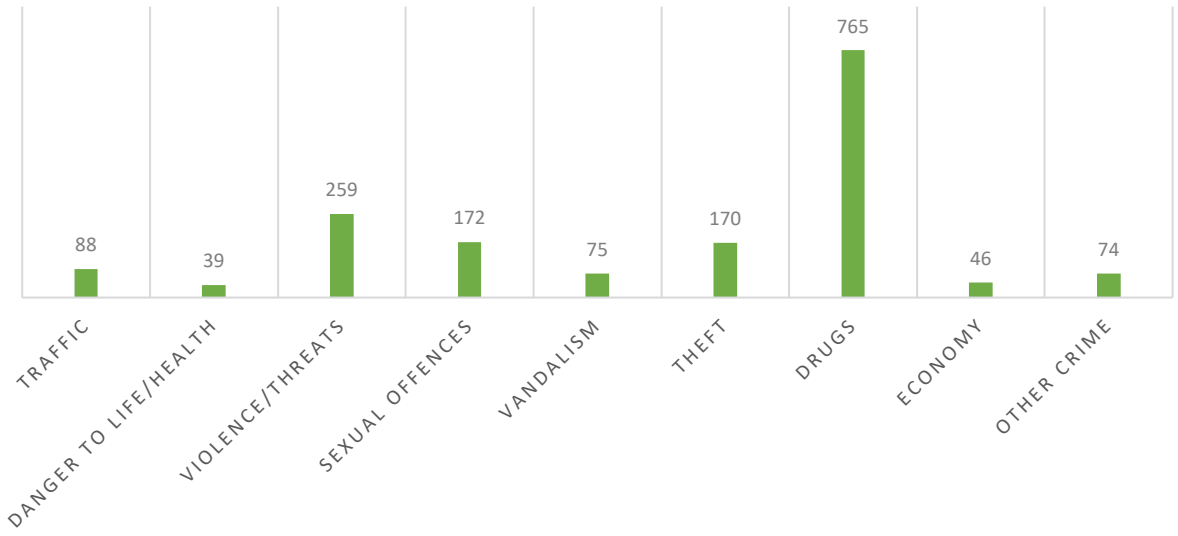
LDF was performed a minimum of 1602 times on different hardware/OS. Mobile phones are by far the largest group. LDF was performed on iPhone in a minimum of 753 cases (47%). Android second largest with a minimum of 479 cases (29.90%). Combined they have a total of minimum 1232 cases (76.90%). Windows laptops in third place with 135 cases (8.43%).

Table 6: LDF performed - crime categories

Count	1	2	3	4	5	6+	Total	Percent
Case types								
Traffic	33	7	9	1	2		88	5,21
Danger to life/health	23	6		1			39	2,31
Violence/threats	65	39	21	5	3	3	259	15,34
Sexual offences	77	23	8	2	1	2	172	10,19
Vandalism	25	15	4	2			75	4,44
Theft	53	22	12	4	3	1	170	10,07
Drugs	67	75	53	22	11	41	765	45,32
Economy	21	5	2	1	1		46	2,73
Other crime	31	5	6	1	1	1	74	4,38
Total LDF performed							1688	100,00

* The column "*Total" is a minimum number as 6+ is counted as 6. Statistical categories as defined in STRASAK report 2018 (Politidirektoratet, 2018). The case type "Danger to life/health" is in addition to the others.*

Figure 14: LDF performed - crime categories



LDF was performed in a minimum of 1688 cases in different crime categories. This number is larger than the total in table 5 due to the limitations in Forms as mentioned in the introduction to this chapter.

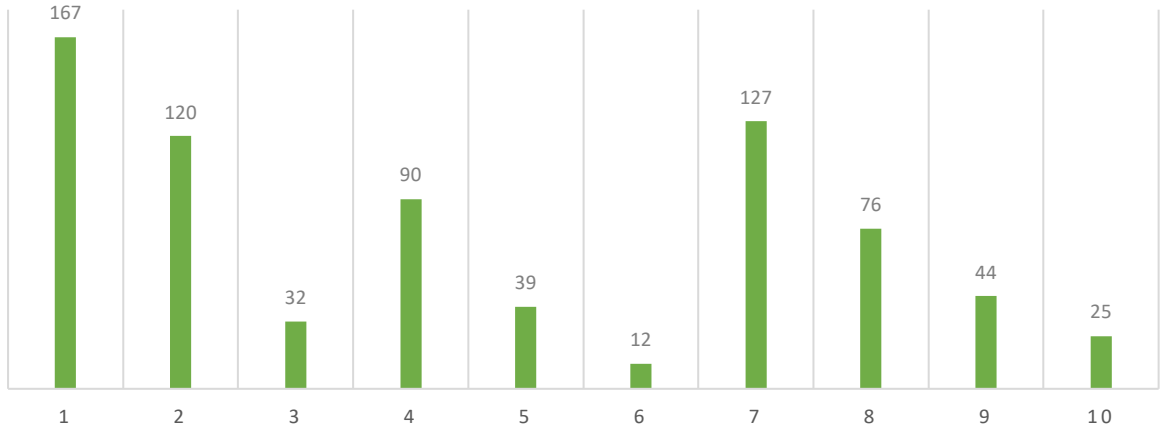
"Drugs" points out as, by far, the largest crime category in which LDF was performed. LDF was performed almost three times as much in this crime category as the second largest; "Violence/Threats".

Table 7: Reasons for conducting LDF

Reasons	Reference	Total	Percent
Because the device would never be examined by a specialist afterwards	1	167	22,81
Because critical data on the device would be lost if the device was not examined on site	2	120	16,39
Danger to life and health if not performing LDF	3	32	4,37
Turning off the unit would lead to loss of critical data	4	90	12,30
Only opportunity to access information such as cloud	5	39	5,33
I don't know	6	12	1,64
We saved time performing LDF on site	7	127	17,35
I was just asked to investigate the device	8	76	10,38
It was common practice to do it that way in the district I was practicing	9	44	6,01
Other	10	25	3,42
Total		732	100,00

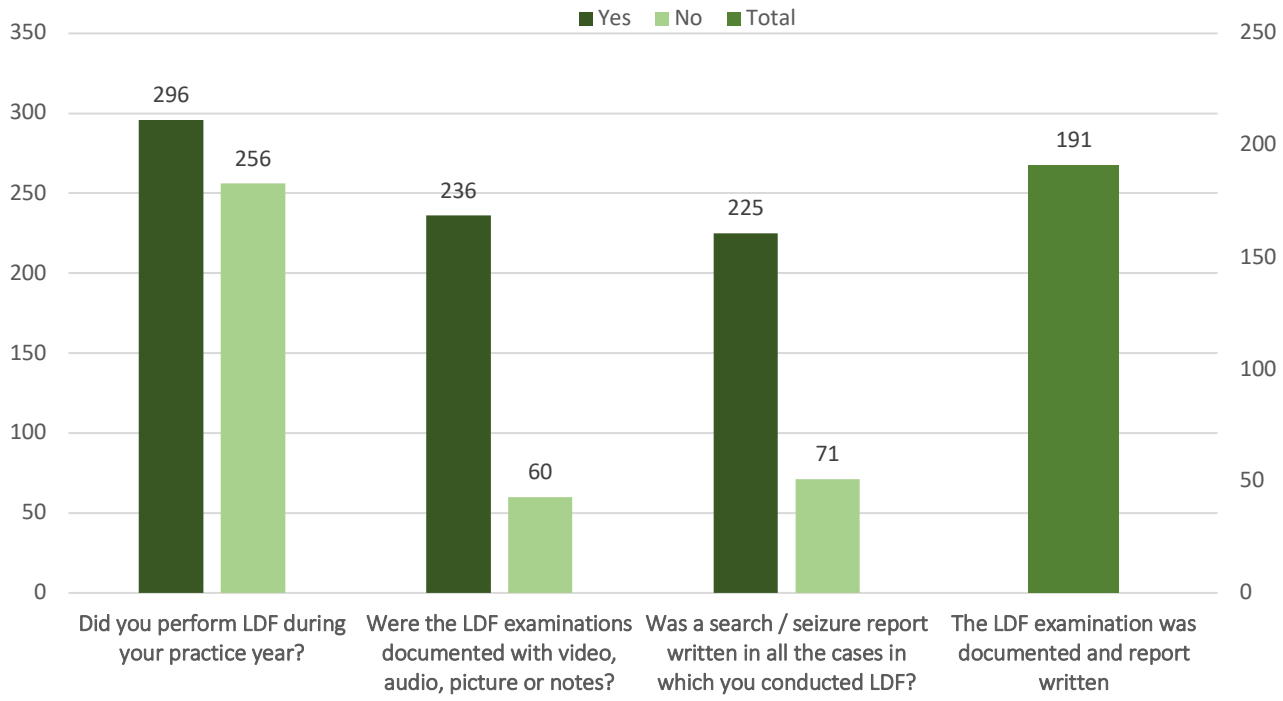
**The respondents could choose more than one option*

Figure 15: Reasons for conducting LDF



The two most significant reasons for performing LDF are “Because the device would never be examined by a specialist afterwards” (22.81%) and “Because critical data on the device would be lost if the device was not examined on site” (16.39%). These findings are particularly interesting and will be discussed in more detail in chapter 6 - Discussion.

Figure 16: LDF conducted, with or without documentation/reporting



191 of 296 (64.53%) respondents answered that they both documented and wrote a search/seizure report in every LDF examination. 105 of 296 (35.47%) respondents answered that they deviated from the methodology and mandatory routines in one or multiple LDF examinations. 60 of the 296 (20.27%) respondents did not document their LDF examinations. 71 of the 296 (23.98%) respondents did not write a search/seizure report in every LDF examination.

Table 8: Correlations between respondents theoretical and practical execution and how they rate the competence of their supervisor.

	How do you rate your competence in Live Data Forensic (LDF)?	How will you rate your supervisor´s competence regarding LDF??	Respondent's theoretical knowledge	Respondent's practical execution
How do you rate your competence in Live Data Forensic (LDF)?				
How will you rate your supervisor's competence regarding LDF?	.325**			
Respondent's theoretical knowledge	.230**	.030		
Respondent's practical execution	.058	.122	.001	

**. Correlation is significant at the 0.01 level (2-tailed).

In this table the respondents rating of personal competence represents all 552 respondents, including those without a permanent supervisor.

The correlation analysis revealed significant positive correlation between subjective rating of own competence in LDF and how well they rated their supervisors´ competence (r = .325, p = >0.001), There was also a significant positive correlation between subjective rating of own competence in LDF and their actual theoretical knowledge (r = .230, p >0.001, There was, however, no correlation between own rating of competence and their practical execution (r = .058, p =0.324). All correlations are reported in Table 8.

Table 9: Respondents, with and without permanent supervisor, rating of personal competence

Respondents without permanent supervisor	**N**	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
How do you rate your competence in Live Data Forensic (LDF)?	552	1	5	2,62	0,882
Valid N	552				

Respondents with permanent supervisor	**N**	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
How do you rate your competence in Live Data Forensic (LDF)?	444	1	5	2,65	0,895
How will you rate your supervisor's competence regarding LDF?	444	1	5	2,68	0,934
Valid N	444				

There is a slight difference between the respondents with a permanent supervisor and those without regarding the rating of personal competence. The respondents with a permanent supervisor rate their personal competence slightly higher and more towards their rating of their supervisor's competence.

6. DISCUSSION

6.1 Introduction

This thesis started by introducing the research problem and questions. This chapter will clarify to what extent we managed to answer these questions, and to what extent the answers helped us elucidate the research problem. The further discussion will be related to this and to Survey results. Possible consequences regarding LDF performed by FRs (First Responders) with lack of competence and the possible benefits by increasing competence, will also be addressed.

These are the research questions we introduced:

- To what extent do NPUC students perform LDF during their year of practice?
- Do they perform LDF according to basic principles and current methodology?
- Which electronic devices are the subject of LDF investigations?

6.1.1 To what extent do NPUC students perform LDF during their year of practice?

Table 2 shows that the respondents have been attending their year of practice in all the police districts in Norway. In that sense, it is safe to say that the data collected represent all of the country's Police Districts, and not just a few.

Table 4 shows that 53.6% of the respondents report that they have performed LDF alone, with their supervisor or other police officers. Based on feedback from former students and assumptions, we expected this number to be significant, but not this high. It is important to emphasize that the performance of LDF includes all cases where LDF have been performed. Our research does not include any overview of the number of respondents who performed LDF alone, with their supervisor or other police officers. We chose to formulate the question to include all performance of LDF due to the fact, that when the students are in their year of practice, they are under guidance of their supervisor or other police officers. Possible challenges regarding this, will be discussed further in section 6.2.

According to table 5 and 6 the respondents performed LDF in a minimum of 1602 times on different hardware and OS which related to a minimum of 1688 cases. This means that the respondents in total performed LDF more than 4 times each day in all the 365 days of the year. Collected data show that the respondents perform LDF, to a large extent, widespread throughout all the police districts in Norway.

6.1.2 Do they perform LDF according to basic principles and current methodology?

According to ACPO guidelines principle nr. 2 (chapter 2, section 2.3.1) those who perform LDF must be competent to do so. The students lack adequate LDF competence. Chapter 4 – Education, describes the student's education throughout all three years at the NPUC. When they start their year of practice (B2), their knowledge of LDF, based on what they have learned at NPUC, is very limited. Nevertheless, feedback from students are that they often possess more knowledge regarding LDF than police officers they work with. This is a paradox. Statements from the students like these are common:

"I got this task since I knew most about it"

"The phone was just handed to my, and I was told to examine it"

"*Nobody else at the scene knew anything about LDF, so I got the task*"

Selected answers from the Survey question nr. 31 (*Did you experience anything in practice regarding the use of LDF that is not affected by the questions in the Survey and that you would like to share?*) reinforces this further:

"A "cowboy" culture where the individual patrol themselves decide how much they care about the case, and therefore decide how much time they themselves will spend on gathering such information. In minor cases (such as theft) the information is not obtained unless it is done by an on-site patrol".

"That there were very few/ none in the patrols who could tell me which things were relevant to secure, how to do it or what to do afterwards. In my opinion, the teaching of B1 (first year)

was deficient and B2 (second year) did not make matters any better. It also happened on several occasions that phones we had seized were lost and had to be replaced".

"I experienced that the routines from the ICT department etc. were very good. However, the police officers themselves, on the site, had no common idea of LDF, solutions being "random"

Table 9 shows that respondents with a permanent supervisor have an average rating of their supervisor competence regarding LDF to be 2.68 (scale 1 (low) – 5 (high)). They also rate their own personal competence to be slightly higher than the respondents without a permanent supervisor. These are interesting findings and reinforce the assumption that students, even with minimal education in LDF, have the same level of competence as their supervisor. This is further reinforced by the feedback and statements as described in this section.

We consider the students to be very conscientious and honest. When they were ordered to do something by their supervisor or other police officers, we believe that they would execute that order. If all LDF examinations were performed by the respondents with their supervisor or other police officers, the results would be even more worrying. This would indicate that a large part of the LDF examinations performed by police officers failed in vital parts of the process.

Fig. 16 shows that of the 296 respondents who states that they have performed LDF, 191 (64.53%) has both documented the examination and written a search/seizure report. This means that 105 (35.47%) either failed one or both mandatory tasks in one or multiple LDF examinations. These are vital parts of the LDF examination and by failing to do so makes it impossible to maintain the fundamental principles in the DFP.

35.47% respondents answer that one or multiple LDF examinations performed by the respondents alone, with their supervisor or other police officers are not performed according to basic principles of the DFP. We emphasize that we cannot generalize the results to the Norwegian police, but it may be an indication of an unfortunate condition.

6.1.3 Which electronic devices are the subject of LDF investigations?

Figure 13 Shows that LDF mostly is performed on mobile phones. These examinations count for 1232 (76.90%) of the total 1602 examinations. iPhone is the largest group of mobile phones with 47%. The second largest group is laptops. Windows OS is largest with a share of 8.43%. Third is desktops with Windows OS (5.24%).

6.2 Possible consequences of LDF being performed in violation of methodology

The generalist of Norwegian police, including NPUC students, are primarily trained to be able to identify potential sources of digital evidence, secure/seize them and then transport them to the DFD for further investigation. These are all tasks which are described and belongs to the first phase of the methodology (DFP); the Identification Phase, described in chapter 2 - State of the art.

When performing LDF, one will, in practice, probably perform tasks in several phases of the methodology. Challenges and problems can and will probably occur when the FR perform LDF, since they are not likely to possess satisfactory competence in these phases of the methodology.

One of the most important reasons why the methodology and principles require competence is, in our opinion, that without having competence, one is unable to understand the implications of one's actions as described in the ACPO guidelines.

According to our Survey (figure 16), 35.47% of the respondents answer that one or multiple LDF cases is not carried out according to the established methodology. The potential for negative consequences in these cases are certainly present. Seen from the police/prosecution perspective, improper LDF execution may lead to e.g. failure to detect and secure evidence, alteration, destruction and/or degradation of evidence, or to the fact that the evidence found cannot be presented as evidence in the court of law.

Improper execution of LDF can in the utmost consequence lead to “Errors of Justice”. According to Asbjørn Rachlew (2009)[29] “Errors of Justice” can be defined as any deviation from the optimum outcome of the criminal case. He further writes that these errors can result in everything from wrongful conviction to failure to resolve the criminal case. An error of justice which leads to a wrong conviction, will cost resources and money, but first of all cause

[29] https://www.duo.uio.no/bitstream/handle/10852/22587/Rachlew_avhandling.pdf?sequence

major social costs for those who are implicated (Rachlew, 2009).

23.98% of the respondents state (figure 16) that a search/seizure was not written in every LDF examination they conducted. The execution of LDF is considered, according to the Norwegian Criminal procedure act and other legislation as the same as a search and seizure, i.e. a coercive measure. In Norway, it is "Spesialenheten for politisaker" (the equivalent to Internal Affairs), who are responsible for investigating cases in which it is suspected that the police or employees of the prosecutors have committed a criminal offence in the line of duty. In their annual report of 2011, (Spesialenheten for Politisaker, 2011) they stated the importance of notoriety in cases where coercive measures were used: *"It follows from the provisions of the Criminal Procedure Act and the prosecution instructions that notoriety about coercive measures must be ensured"* (Our translation) (ibid, p. 8).

"The fact that the police, as society's civilian apparatus of force, uses coercive measures against persons, and in violation of the legislation fails to secure notoriety about its use, is a serious matter. Lack of notoriety weakens society's ability to control that the police use their powers in a fair and just manner, both in terms of material conditions and decision-making competence. The legal security of the person subject to the use of coercive measures is also weakened. Among other things, it may be doubted whether the person the police has intervened against has been made aware of their rights. An approximate practice in relation to the notoriety requirements means that questions about the polices use of powers is in accordance with the legislative requirements can be asked" (our translation) (ibid, p. 8-9).

If the police use coercive measures on the wrong basis, or perform it incorrectly, the society can, over time, lose confidence in the police and its working methods. Ultimately, this could lead to a limitation of the ability to perform LDF to the same extent as today.
Our goal with our thesis has not been to narrow down the police opportunities to perform LDF. As we will show in the further discussion, the need for LDF will become increasingly important in the future. However, police must be conscious of their responsibilities, and laws and regulations must be adhered to.
Based on data collected in question 28 in the Survey, 82% of the respondents state that they know that it is necessary to write report on search/seizure after LDF is executed. 16% do not know. 2% answer that it is not necessary. The respondents provide various reasons not to write a report, but in our knowledge, there exists no valid reasons for not writing a report.

This is confirmed after conversation with several prosecution lawyers, including the training responsible prosecutor in South-East Police district, Thomas Kraglund.
Our findings may indicate an unfortunate situation in the Norwegian police regarding the execution of LDF.

6.3 Technology development and LDF

The first mobile phone that you actually could hold in your hand and in that sense call a "mobile phone" was available for the in 1992 with the Nokia 1011. In the summer of 2008, the first "smartphone" was introduced with the Apple iPhone. The first iPhone represented a paradigm shift in how we thought about and started using the mobile phone. With the iPhone and the introduction of Applications ("apps"), mobile phone usage became more similar to the way we use them today. From 2008 and to present day there has been almost an explosion in the number of users and the ways we use it.

The history of computers and laptops has many similarities to those of the mobile phone. With the release of Windows95 in 1995 and the Apple iMac G3 with Apple OS in 1998, the usage and development of computers and laptops increased very quickly. Today most people have access to, and can use, a mobile phone and/or a computer.

From 1998 towards today there has been a tremendous technological development, not only in the number of electronic devices each of us use, but also in the way we use these devices. For the police, this has meant an ever-increasing challenge in relation to the number of places it is possible to secure digital evidence. From securing simple text messages and contact information from the first mobile phones to today's challenges with e.g. cloud storage, encryption, password and biometric protection, has led to a rapidly growing need for expertise so that these challenges can be addressed. The list gets longer for each passing day and the need for expertise as well.

The challenge for law enforcement in Norway, and every other country that has applied the same DFP, is that by following the standard forensic process as earlier described, vital digital evidence can be lost forever. An example that represents several challenges for law enforcement is cloud storage. By following the traditional DFP, the device should be examined post-mortem by DFD. This would mean that you'd have to break the connection to

the cloud storage to be able to do that. As a result of this a huge amount of digital evidence, depending on the case could be lost. This could be digital evidence both in favour and in disfavour of the accused.

Cloud storage can be password protected and shared between multiple people. A potential challenge in relation to this is that another person has control of the content and thus can change and/or delete it. Information stored on servers owned by foreign companies has been a challenge to several investigations in Norway. The most famous case is the terror case "22. Juli case"[30] which took place 22.07.2011. As a part of the investigation Norwegian police wanted information regarding Facebook accounts used by the accused. Due to Facebook privacy rules the investigation was delayed considerably[31]

If one is to secure a mobile phone according to traditional DFP, this would mean that it in many cases would be network isolated and one would have the same problem related to cloud storage as in securing a computer.

Encryption, password and biometric protection and the content of Random Access Memory (RAM) are other challenges that need to be addressed. The Norwegian police experiences that encryption is an increasing challenge in criminal cases. According to an article in Politiforum[32] an increase in technological competence is needed to be able to handle this challenge in a proper way (Trædal, 2018).

Virtual private networks (VPN) is another challenge that needs to be considered and dealt with accordingly. VPN is a software-based solution often used by companies so that the employee may access the company's network even if the employee physically is located elsewhere. VPN is also widely used by persons who, for multiple reasons, want to access the internet without revealing their true IP address. Common to both is that they depend on connection to the Internet. Network isolation will terminate this connection and could make potential digital evidence inaccessible.

[30] https://en.wikipedia.org/wiki/Trial_of_Anders_Behring_Breivik
[31] https://www.aftenposten.no/norge/i/GGLll/facebook-forsinker-etterforskning
[32] Homepage: https://www.politiforum.no/

Smart Home Environments is gradually increasing. According to a minor thesis by A.F Goudbeek (Goudbeek, 2017) they represent several challenges for the investigators. One of the challenges is regarded the volatile digital evidence. Without knowing how these digital evidences are stored on the system, the power must be turned on, until knowledge about this is required (ibid, p. 46). This will make LDF necessary on site.

6.4 Current methodology and LDF

This section will discuss the extent to which today's methodology is appropriate for the electronic devices that the FR most frequently encounter. Does it fit just as well on a computer as on a mobile phone? It is important to emphasize that this is not an in-depth discussion and analysis of the differences and challenges regarding LDF on mobile phones and computers. The discussion will deal with some basic differences that represents possible challenges for the students and the FRs in general.

The Digital Forensic Process does not differ regarding which device that is to be examined, whether the system is "dead" or "alive". According to Flaglien "*special caution must be taken before any action, regardless whether the system is live or dead at the time of identification*" (Flaglien, 2018, p. 23). The students knowledge about LDF is that this is a deviation from the main rule and the traditional DFP within law enforcement in Norway. They are trained to identify and secure potential digital devices and deliver them to the DFD for examination. Nevertheless, LDF is performed in a large scale on mobile phones by student´s alone, with their supervisor or with other police officers acting as First responders.

At the NPUC the education in LDF has been mainly focused on computers. Our impression is that this also is the case within the LDF course at UCD. Flaglien (Flaglien, 2018) and Casey (Casey, 2011) seems to have the same focus. The reasons for this are beyond the scope of this thesis, but the rapid development in mobile phone technology and functionality may be a possible hypothesis. An article published in 2017 by Chernyshev, Zeadally, Baig and Woodward may reinforce this hypothesis further and give a possible explanation. In the article they state: *"Mobile forensics is inherently multidisciplinary and challenging because of the increasing heterogeneity of mobile device technologies and the features these devices support, which are usually far beyond basic voice calls and text messaging"* (Chernyshev,

Zeadally, Baig, & Woodward, 2017, p. 43). They further state that: *"The evolution of the mobile forensics discipline is ongoing and will continue to be influenced by heterogeneous platforms, the emergence of new device types, and the increasing pressure on device vendors to incorporate more sophisticated security measures into their products, thereby making evidence acquisition more complex and technically challenging"* (Chernysev et al., 2017, p. 45).

Within computers there is diversity, but also great similarities both in the way they are used and in functionality. The most used Operating Systems; Windows, macOS and Linux has inequalities, but they are similar in many ways regarding usage. The different Operating Systems has different lifespans and update frequencies, but it is rare that an update leads to the loss of "traditional" usage like e.g. mail, internet, office applications and so on. As an example, and in our opinion, Windows OS functionality has been recognizable all the way since ver. 3.1. This is not always the case for mobile phones. As mentioned in section 6.3, the introduction of the first "smart phone", iPhone in 2007, represented a paradigm shift in how the mobile phone was used. Since then the mobile phone has had an incredibly fast development and new functionality. This is a challenge for the DFD and FR.

According to a journal article published on Researchgate[33], the DFDs are very familiar with computers and computer operating systems, but still not as familiar with working with the varieties of mobile phones (Ahmed & Dharaskar, 2008).

Well-defined methods and best practice guides exist for digital evidence stored on a computer hard drive. Lawyers, investigators and researchers have discussed and refined these methods and practices which makes them to be considered as *forensically sound* as long as the guidelines are followed. For embedded systems, like the mobile phone, there is no well-defined methods or practices. A necessary consequence is continuously assessing the methods and how evidence integrity is preserved and follow the principle of *Chain of custody* (Sandvik, J.P, 2018).

The mobile phone is basically a computer in a small form-factor, but LDF examination on this device differ from a computer in many ways. The main rule is that if it is off, it is to remain

[33]Homepage https://www.researchgate.net/

off (Hamremoen, 2016). The difference begins when we manage to get control of the phone and gain access to the device. Usually the phone, depending on the case, is network isolated to prevent remote access and deleting of potential digital evidences. The next task for the first responder will be to prevent the lock screen from activating and make sure that the device has power. The final step is to transport the phone to a DFD.

If the FR has full access to a computer, network isolation is as relevant as on a mobile phone. Reasons for this will usually be the same as for a mobile phone. Digital evidence may reside in e.g. cloud storage, network-attached storage (NAS)[34], active social media accounts, Bluetooth connections, cellular data[35] etc. If the biggest threat to the device is remote wiping, and the digital evidence is elsewhere than the one mentioned, network isolation will be the right thing to do.

Cases which involves LDF examinations on computers, will usually allow more interaction with the system than on a mobile phone. Moving the mouse pointer over the "taskbar"[36] will often give the examiner useful information about e.g. running programs, time and date, network connections, documents and web browsers. This information will be viewable without opening the actual program. If the mouse pointer points on e.g. a running web browser program in Windows 10, the website displays in a small window directly above the program icon. If the examiner moves the mouse pointer on to this window, it displays in full size. Within the full-sized window, the examiner can view the content without clicking on the actual website.

On a mobile phone, this will not be possible to the same extent. On e.g. an iPhone with iOS ver. 13.2.3 the same information will not be accessible without more interaction with the device. To be able to view running programs the examiner must double-click the home button. This will make the running programs viewable, but some apps will display less information. For instance, a banking app will normally only display a "blank" window[37].

The tools for securing the content on a mobile phone is expensive. This is not something that the FRs have with them or have any training in. In situations where the FR has been equipped

[34] https://en.wikipedia.org/wiki/Network-attached_storage
[35] Cellular data is how a smartphone accesses the internet when it is not connected to WIFI.
[36] An element of a graphical user interface that typically shows which programs are currently running.
[37] Tested on the following Norwegian banking apps: DNB, Nordea, Norwegian & Vipps

with tools, the FR must be trained to use them. As described in a thesis by Friheim, software and hardware have random and systematic errors. To prevent misinterpretation, it is vital that the user of the different tools is competent and know how they work. Failure to this can ultimately result in people being wrongly convicted in a criminal case (Friheim, 2016).

A possible LDF scenario on a computer can be the discovery of pictures containing potential digital evidence that the FR wants to secure by copying them to an external storage media. If this process is documented, the storage media formatted, and the timestamps are documented prior to copying, this will in many cases be enough. It will not be *forensically sound,* but it will uphold the principle of chain of custody and most important secure potential digital evidence that otherwise could be lost if not secured on site. Picture file-size and Exif[38] data would probably be intact and possible to examine further at a later stage in the investigation. If one, or several of the pictures were e.g. child abuse/child exploitation material, it would be possible to generate cryptographic hash-values. The hash-values could be used to find out whether the pictures were registered in the ICSE database[39].

If the same LDF scenario took place on a mobile phone, the performance and result would most likely be different. The student and FR are trained to identify and secure different electronic devices containing possible digital evidence. Remote wipe prevention by network isolation is an important part of this regardless of access[40] to the mobile phone or not.

Even if network isolation was not performed, the FR would not have the same possibilities as on a computer. Documentation of the examination would most likely be with photos, movie or both, but no potential digital evidence would be preserved in its "original" form. The pictures would probably not be copied on to an external storage media, making further examination regarding timestamps, Exif data and hash-values impossible. If the case was serious enough one would consider sending the pictures by using Bluetooth, AirDrop[41], mail, SMS or other practical method, but depending on the compression method used by the application, file-size could change. This would result in a different hash-value from the resized images. Feedback from the students indicates that the primary method for securing potential digital evidence on a mobile phone is through taking pictures and/or video of the

[38] Exchangeable image file format (https://en.wikipedia.org/wiki/Exif)
[39] Interpol's International Child Exploitation (ICSE) database
[40] Open or locked with password, face id, biometric or another authentication
[41] https://support.apple.com/en-us/HT203106

examined phone. When these devices account for 76.90% of all student´s LDF examinations, many potential digital evidences are not adequately secured or secured at all.

The benefits of having a universal and technology-independent methodology (DFP) are many, but it can also present challenges. A universal and general methodology requires knowledge of the different phases (and it´s "surrounding" principles), and the content of each phase to be effective - and thereby act as a support and guide for the FR in the LDF process.

There are more challenges associated with executing LDF on a mobile phone compared to a computer. This is supported by other researchers, literature and professionals. The challenge becomes particularly large, considering that this is the device in which most examinations are carried out. Even if a new or different process is not needed, there is no doubt that LDF on mobile phones is carried out in a large scale due to the fact that technology development has made it necessary in many cases.

When many of these LDF examinations are performed by students and FRs, the need for education, training and best practice guides is huge.

6.5 The border between the generalist and the specialist

Based on this thesis, the answers from the survey and our experience from the Norwegian police, it is natural to ask the question whether there is a need for an increase of competence for the FR so they can perform tasks that currently is carried out by the DFD. What effect such an increase in competence could lead to is something the further discussion will try to elucidate.

It is a clear goal from POD that the generalist must increase their competence in the field of DF. In this way, the generalist/FR can perform what was formerly considered a specialist task. According to Ressursanalysen 2018, there are in total 16716 people employed in the Norwegian police, of which 9163 people in police positions (Politiet, 2018). The number of specialists in the field of DF is unknown, but according to a thesis by Heitmann, the number is too low (Heitmann, 2019, p. 7). He also describes that the total number of offences in 2018 was 318,556. In his Survey, the respondents were asked about how many of the last three

cases they worked with contained potential electronic evidence. 51.5% responded that all the last three cases contained electronic evidence (Heitmann, 2019, p. 89).

The number of backlogs is an increasing problem for several Police districts in Norway. East police district is the second largest police district in Norway related to number of employees, inhabitants (738,000) and criminal cases (Politiet, 2019). An NRK[42] online newspaper article described that East police district in 2018 had over 7000 cases waiting to be processed (Gimmingsrud & Nordli, 2018). In the same article the court in the city of Fredrikstad said that the decline in cases they received from the district for processing had dramatically decreased. Another online newspaper (VG)[43] article describes a situation where 43 Norwegian IP addresses related to users who had downloaded serious child abuse/child exploitation material were left for 107 days before local police acted. In the same article a DFD within the largest police district in Norway, Oslo Police District, said that 80% of his time is used to assist other police districts (Arntsen, Bringdal, & Stangvik, 2017).
These are just a few examples of the current situation regarding cases that awaits processing and the challenges DFD´s have. The exact number of employees in Computer Crime Units in Norway is restricted, but Heitmann indicates that East police district has a total of nine (Heitmann, 2019, p. 7). Related to mentioned articles and the fact that most cases involve potential digital evidence in some form, it is likely that the number of DFD is too low. This is confirmed by every DFD we have spoken to. The results from the survey points in the same direction. Table 7 shows that 22.81% of the respondents has answered that the reason for performing LDF on site was:

"Because the device would never be examined by a specialist afterwards"

The threshold for the DFD to assist the First Responder seems to be increasing and the huge workload leads to the DFD´s only has the capacity to prioritize the most serious criminal cases. The fact that less serious cases are not being prioritized, leads to a longer time to review the material, analyze the findings and finalize the final report. According to the journal article "Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists"[44], the time delay from when a DFD receives the digital evidence until the

[42] Norwegian National Broadcasting AS (our translation)
[43] Homepage: https://www.vg.no/
[44] Full article at https://www.sciencedirect.com/science/article/pii/S1742287616300044

completion of the analyze and report, is a significant bottleneck (Hitchock, Le-Khac, & Scanlon, 2016).

The journal describes research regarding what effect it had to train first-line personnel within the Royal Canadian Mounted police to handle simple tasks within electronic evidence. These tasks were performed without an DFD present using a *Digital Field Triage Model* (DFTM). DFTM is a model based on *The Computer Forensics Field Triage Process Model* (CFFTPM), proposed by Rogers et al. (2006). CFFTM will not be discussed further. Relevant parts of the DFTM will be briefly described and further discussed.
Digital Field Triage (DFT) is, according to the journal, designed to provide non-digital evidence specialist with the skills, knowledge and abilities to conduct limited forensic activities (Hitchock et al., 2016 after Rogers et al., 2006).

For the model to work, three fundamental concepts must be followed:

1. DFT cannot work in isolation and must work with a parent Technical Crime Unit (TCU)
2. DFT must maintain the forensic integrity of the digital evidence
3. A DFT assessment does not replace a TCU specialist

The first version of the model was implemented in 2009 by a parent TCU consisting of 25 members. 20 of these were forensic analysts. This TCU supported approximately 8500 employees policing Federal, Provincial and Municipal regions covering 127 police stations ranging in size from two to 800 members. The geographical area covered 954,000 square kilometers.

The model consisted of two types of courses for the selected personnel:

1. Digital Computer Field triage (DCFT)
2. Digital Mobile Field Triage (DMFT)

The primary objectives with the research was:

1. Increase the efficiency of an investigation by providing artefacts from digital evidence in a timely manner

2. Decrease the backlogs of files for analysis by digital evidence specialists[45] at a forensic laboratory

Results show that there has been a reduction of exhibits forwarded to TCU by approximately 75%. This means that the DFD are dealing with fewer files containing digital evidence. Reduction in time used on each file has led to an increase of files being analyzed each year, which in turn has led to a reduction in backlogs.

This experiment shows that an increase in competence gives effect. We have not investigated the extent to which this is directly transferable to Norway, but it is likely to believe that it would have an effect here as well.

An experience-based comparison is how fingerprints were secured by FR in the Norwegian police. Prior to year 2000 fingerprints, deposited on surfaces that was not straight, on e.g. bottles, tools and other evidence material was considered difficult. Often this kind of evidence material was secured by the FR and transported back to the Police Station to be examined by a Criminal Forensics Detective (CFD). This resulted in a huge workload for the CFD causing a bottleneck which in many cases was the cause of delay. As a result of this an increase of competence within criminal forensics was given to the FR. Today, the FR is expected to do this examination without the assistance of the CFD.

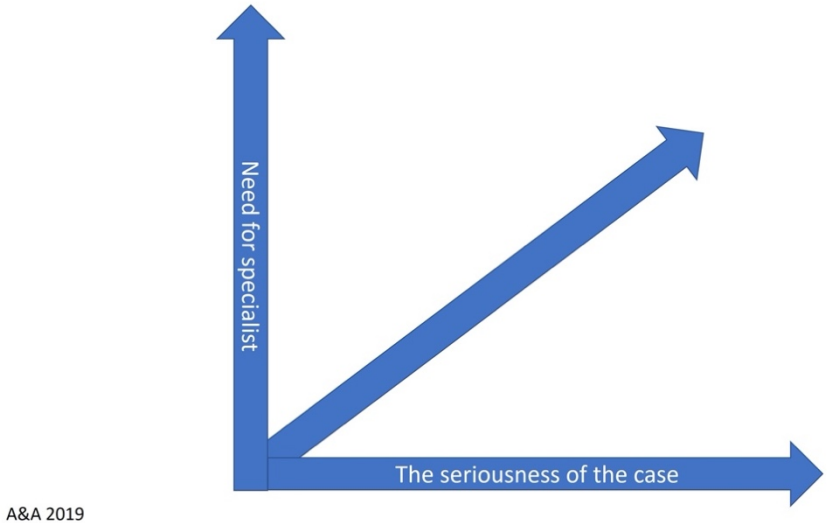
There is no doubt that digital evidence will continue to exist, increase and be a part of many criminal cases in the future. If the police are to be able to handle this development, there must either be more DFDs, or some of the DFD's tasks must be done by others.
To draw parallels between Criminal Forensics and Digital Forensics, it is tempting to say that LDF, especially on mobile phones, is the “fingerprint” of our time. Increasing the competence on LDF, especially on mobile phones, might have the same effect as the increase in competence for the FR had for fingerprints. This is something that future research should look into, but research from Canada reinforces this assumption.
One may also need to see LDF, especially on mobile phones in a different perspective. Casey writes that not changing data in practice cannot be done.
Casey states:

[45] We use the definition Digital Forensic Detective (DFD)

"setting an absolute standard that dictates "preserve everything but change nothing" is not only inconsistent with other forensic disciplines but is also dangerous in a legal context. Conforming to such a standard may be impossible in some circumstances and, therefore, postulating this standard as the "best practice" only opens digital evidence to criticisms that have no bearing on the issue of investigation". (Casey, 2011, p. 20)

In our opinion, future work must aim to develop a practice where Digital evidence is considered an opportunity and not a major obstacle. The generalist/FR must be thought and trained in a way that they feel competent to perform simple LDF examinations without the assistance of the DFD. Our model (figure 16) illustrates that the need for assistance will increase in correlation to the seriousness of the criminal case, but in less serious cases the FR should be able to perform LDF tasks without the aid of a DFD.

Figure 17: Correlation – seriousness and need for assistances model (NFAM)



It is our clear belief that the FR must be educated and trained so that they feel competent to conduct LDF even in cases which may appear challenging. This is perhaps the best way to gain practical skills in different scenarios. However, they must clearly bear in mind that the need for expert assistance increases in correlation with the seriousness of the case. In cases where you are legally authorized to perform LDF, and where a specialist due to different reasons would not examine the device retrospectively, there is clearly a "golden opportunity" to perform LDF. Of course, methodology and principles must be adhered to.
This is a mind-set we believe the FR in the Norwegian police should have. This will increase practical competence and could decrease the workload of the DFD.

7. CONCLUSION AND FUTURE WORK

7.1 Conclusion

Our research problem for this thesis is:

LDF is performed by NPUC students despite their lack of competence

By answering the research questions and the following discussion in chapter 6 our research problem was confirmed. The main features and results of this thesis can be summarized in this way:

Today's DFP model/methodology is adapted to both computers and mobile phones. Nevertheless, there are clear signs that there is a shortage in development of methods and best practice guides when it comes to LDF on mobile phones.

The respondents in the Survey performed LDF examinations in 1602 cases or more, despite the fact that they have no prerequisite to perform this. 64.53% of the respondents conducted all their LDF examinations according to methodology and guidelines. 35.47% of the respondents did not conduct all LDF examinations correctly. A deviation of this magnitude is an unsustainable situation for the Norwegian police that cannot continue. There is a need for increased/changed education and focus within the field of LDF.

The technology development, especially on mobile phones, makes LDF more relevant than before. The only competence requirement for the FR regarding LDF is the education from the NPUC. Formal competence requirements within methodology and LDF, especially on mobile phones, should be introduced and implemented.

The DFDs have a heavy workload. Measures must be taken to change this situation. Research from Canada shows that by increasing the competence of FR personnel this can lead to a reduction in workload for the DFD. Backlogs and workload reductions are important, but more importantly, laws and regulations must be adhered to, in execution of all LDF. Documentation and the principle of *chain of custody* must always be followed.

In our opinion, NPUC has the overall responsibility for ensuring that the generalist in Norwegian police receives an education in DF and LDF that is adequate.

7.2 Future work

7.2.2 Methodology

One must constantly assess and evaluate all methods and guidelines used. This also applies to Flaglien´s DFP. Does it fit into today's crime- and Techology situation, or does the linear process describe a condition we very rarely reach? Can LDF in the future still be considered a deviation from the established methodology, or is LDF today what we expect and must plan for in every police investigation?

7.2.3 Tools

For the DFD there is a variety of tools for acquisition of data from mobile phones like e.g. Cellebrite[46] and XRY[47]. For the FR there is currently a lack of appropriate tools to perform LDF. Access to, and training in adequate tools could be wise. A simple thing which could be implemented, is the ability to copy selected content of an iPhone/Android using e.g. a USB drive via Lightning/Micro-USB[48]. Such a solution will make copying without the loss of metadata such as EXIF[49] data in images possible. In many cases this will be sufficient. But, distribution of equipment like USB drives to all FR gives new challenges. Who will format them in a forensically sound manner before they are used? Who will handle the USB drive after copying? Who will reformat it? These challenges must be discussed and resolved before implementing a solution like this.

7.2.4 Education

NPUC educates the future First Responders, and in June 2020, 710 new FRs will graduate. As police educators, NPUC has a great responsibility, and must constantly take care to facilitate the best possible education. By adjusting the education slightly, we can, in our opinion, to a great extent compensate for the different problems data from our Survey reveals.

[46] https://www.cellebrite.com/en/home/
[47] https://www.msab.com/products/xry/

First academic year (B1)

The education for the students in their first academic year (B1) was no more comprehensive regarding LDF than knowing that it is a deviation from the methodology - and a task to be performed by competent personnel. It is not until they graduate from the NPUC that they are competent to perform simple LDF examinations. NPUC can increase the education within LDF and it is clear that there should be more focus on this in the first academic year, especially on mobile phones. Report writing in connection with LDF must be implemented in the education. The legal subjects within the NPUC must focus on the legal basis for handling and collecting electronic evidence, including LDF.

Second academic year (B2)

The individual Police District must be responsible for and ensure that LDF examinations are done properly. Students are in a mentoring situation and cannot be expected to be a resource in this area, and certainly not a solution to the different problems. The NPUC can however ensure that students reflect on LDF during their year of practice by introducing a written assignment, where the student must reflect on LDF practice.

Third academic year (B3)

The NPUC must constantly ensure that education is in line with the need for competence in the police districts. At the same time, it is important that the NPUC follows technology development and can be ahead with ideas and solutions. The subject Digital Policing and Investigation must during the third academic year, ensure that the students get such a high level of competence that they can become a resource in this area as soon as they graduate. From the academic year 2019-2020, the LDF teaching was expanded and changed. This is a step in the right direction, but further increase in competence is needed. We believe that thorough education in methodology is a vital part of this.

Future work must constantly seek to implement changes that reflects the needs of which the Norwegian police consider important for the FR in this field. Exchange of experience and regular contact between the NPUC and the police districts are important pieces in this work.

8. BIBLIOGRAPHY

Ahmed, R., & Dharaskar, R. (2008). Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective. Retrieved from https://www.researchgate.net/publication/255586187_Mobile_Forensics_an_Overview_Tools_Future_trends_and_Challenges_from_Law_Enforcement_perspective

Arntsen, E. O., Bringdal, T., & Stangvik, E. O. (2017). Norsk politi venter 107 dager på å ta overgrepsnedlastere. Retrieved from https://www.vg.no/nyheter/innenriks/i/rvk4m/norsk-politi-venter-107-dager-paa-aa-ta-overgrepsnedlastere

Association of Chief Police Officers (ACPO). (2012). ACPO Good Practice Guide for Digital Evidence. Retrieved from https://athenaforensics.co.uk/wp-content/uploads/2019/01/National-Police-Chiefs-Council-ACPO-Good-Practice-Guide-for-Digital-Evidence-March-2012.pdf

Casey, E. (2011). *Digital evidence and computer crime : forensic science, computers and the Internet* (Vol. 3rd ed.). Amsterdam: Academic Press.

Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile Forensics: Advances, Challanges, and Research Opportunities. *Digital Forensics, Part 1*. Retrieved from https://ieeexplore-ieee-org.ucd.idm.oclc.org/document/8123468

ECHR. (1950). *European Convention on Human Rights* Retrieved from https://www.echr.coe.int/Documents/Convention_ENG.pdf

Fahsing, I. A. (2016). *The makingof an expert detective: Thinking and deciding in criminal investigations.* (Doctoral Dissertation). University of Gothenborg,

Flaglien, A. O. (2018). The Digital Forensic Process. In A. Årnes (Ed.), *Digital Forensics*. Hoboken, NJ: Wiley.

Friheim, I. (2016). *Practical use of dual tool verification in computer forensics.*

Gimmingsrud, J., & Nordli, S. (2018). Over 7000 straffesaker venter på behandling. Retrieved from https://www.nrk.no/ostfold/7000-straffesaker-venter-pa-behandling-i-ost-politidistrikt-1.14206243

Gjerde, M. (2007). *Victims of success? Knowledge discovery amongst digital forensic investigators in the Norwegian police districts.* (Master thesis). University College Dublin,

Goudbeek, A. F. (2017). Forensic approach in Smart Home Environment. 80.

Kongeriket Norges Grunnlov, (1814).

Hamremoen, E. (2016). *Kriminalteknikk: Første enhet på åstedet (2.utg)*: Oslo: Gyldendal.

Haraldsen, G. (1999). *Spørreskjemametodikk: Etter kokebokmetoden*. Oslo: Ad Notam Gyldendal.

Heitmann, O. (2019). *Digital investigation: The malnourished child in the Norwegian police family.* (Master). Norwegian University of Science and Technology,

Hellevik, O. (2016). Lave svarprosenter fører ikke nødvendigvis til skjeve resultater. Retrieved from https://forskning.no/statistikk-innvandring-kronikk/kronikk-lave-svarprosenter-forer-ikke-nodvendigvis-til-skjeve-resultater/1167716

Hitchock, B., Le-Khac, N.-A., & Scanlon, M. (2016). Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists. *Digital Investigation, Volume 16, Supplement*. Retrieved from https://www.sciencedirect.com/science/article/pii/S1742287616300044

ICCPR. (1966). *International Covenant on Civil and Political Rights* Retrieved from https://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf

ISO. (2012). *ISO/IEC 27037:2012, Information technology - Security techniques - Guidelines for indetification, collection, acquisition and preservation of digital evidence*. Retrieved from https://www.iso.org/standard/44381.html

Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser? : innføring i samfunnsvitenskapelig metode* (3. utg. ed.). Oslo: Cappelen Damm akademisk.

Johannessen, A., Tufte, P. A., & Christoffersen, L. (2010). *Introduksjon til samfunnsvitenskapelig metode* (Vol. 4): Abstrakt Oslo.

Lov om straff (Straffeloven) (The Norwegian Penal Code), (2005).

Justis- og beredskapsdepartementet. (2015). *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*. Retrieved from https://www.regjeringen.no/contentassets/8de0db6aff3e4dd79c92519057af690f/strategi_ikt-kriminalitet.pdf

Kruger, J., & Dunning, D. (1999). Unskilled and unaware of it: How difficulties in recognizing one´s own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology, 77 nr. 6*.

Kruse, W. G., & Heiser, J. G. (2002). *Computer Forensics. Incident Response Essientials*. Indianapolis: Pearson Education.

Laliberte, S., & Gupta, A. (2004). The Role of Computer Forensics in Stopping Executive Fraud. Retrieved from http://www.informit.com/articles/article.aspx?p=336258

Leedy, P. D., & Ormrod, J. E. (2014). *Practical Research Planning and Design*. Harlow: Pearson Education Limited.

Lexico. (2019). Meaning of science. Retrieved from https://www.lexico.com/definition/science

Politidirektoratet. (2012). *Politiet i det digitale samfunn: En arbeidsgruppe om Elektroniske spor, IKT-kriminalitet og politiarbeid på Internett* Retrieved from https://medlem.ntl.no/Content/103500/cache=20122109105334/Politiet%20i%20det%20digitale%20samfunn%20juli%2012.pdf

Politidirektoratet. (2016). *Rammer og retningslinjer for etablering av nye politidistrikter ver.1.1*.

Politidirektoratet. (2018). *STRASAK - Rapporten: Anmeldt kriminalitet og politiets straffesaksbehandling*. Retrieved from https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/strasak/2018/strasak-2018.pdf

Politidirektoratet. (2019). *Nasjonale rolledefinisjoner med kompetansekrav - etterforskningsfeltet*.

Politiet. (2018). Ressursanalysen 2018. Retrieved from https://www.politiet.no/aktuelt-tall-og-fakta/tall-og-fakta/ressursanalyse/

Politiet. (2019). Organisering og ledelse - Øst politidistrikt. Retrieved from https://www.politiet.no/om/organisasjonen/politidistrikter/ost/om-ost/organisering-og-ledelse/

Politihøgskolen (PHS). (2017a). Curriculum Postgraduate Education For Nordic Computer Forensic Investigators Module 1: Core Consepts in Digital Investigation & Forensics. In. PHS.no.

Politihøgskolen (PHS). (2017b). Fagplan Bachelor - Politiutdanning 2017 - 2020. In.

Rachlew, A. (2009). *Justisfeil ved politiets etterforskning: noen eksempler og forskningsbaserte mottiltak.* (Doctoral Dissertation). Universitetet i Oslo, Det juridiske fakultet. Retrieved from https://www.duo.uio.no/bitstream/handle/10852/22587/Rachlew_avhandling.pdf?sequence

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence, 1*(3), 1-12.

Repstad, P. (2007). *Mellom nærhet og distanse : kvalitative metoder i samfunnsfag* (4. rev. utg. ed.). Oslo: Universitetsforlaget.

RFC 3227. (2002). *Guidelines for Evidence Collection and Archiving*. Retrieved from https://tools.ietf.org/html/rfc3227

Ringdal, K. (2007). Enhet og mangfold. Samfunnsvitenskapelig forskning og kvantitativ metode. 2. utg. Bergen, Fagbokforlaget Vigmostad & Bjørke AS. Scenekunst (2012, 11. januar). *Spesielle forutsetninger for tilskudd*.

Rogers, M. K., Goldman, J., Rick, M., Wedge, T., & Debrota, S. (2006). Computer Forensic Field Triage Process Model. *Digital Forensics Security and Law*. Retrieved from https://commons.erau.edu/jdfsl/vol1/iss2/2/

Saferstein, R. (2007). *Criminalsitics: An Introduction to Forensic Science*: Pearson Prentice Hall.

Sandvik, J.-P. (2018). Mobile and Embedded Forensics. In A. Årnes (Ed.), *Digital Forensics*. Hoboken, NJ: Wiley.

Singleton, R. A., & Straits, B. C. (2005). *Approaches to social research 4th ed.* New York: Oxford University Press.

Skjervheim, H. (1957/1996). *Deltakar og tilskodar og andre essay*. Oslo: Aschehaug.

Spesialenheten for Politisaker. (2011). *Årsrapport*. Retrieved from http://www.spesialenheten.no/Portals/0/Årsrapporter/Spesialenheten-Arsrapport-2011.pdf

Stelfox, P. (2013). *Criminal Investigation: An Introduction to Principles and Practice*. New York: Routledge.

Sunde, N. (2017). *Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation.* (Master). Norwegian University of Science and Technology & Norwegian Police University College,

Sunde, N., & Bergum, U. (2019). Dataetterforskning – en ungdom med voksesmerter. Retrieved from https://www.parat.com/norges-politilederlag-5410-406272/aktuelt/dataetterforskning-en-ungdom-med-voksesmerter

Svartdal, F. (2009). Psykologiens forskningsmetoder en introduksjon. 3. *Utg. Bergen: Fagbokforlaget*.

Tilstone, W. J., Hastrup, M. L., & Hald, C. (2013). *Fischer´s Tecniques of Crime Scene Investigation First International Edition*. CRC Press: Taylor & Francis Group.

Trædal, T. J. (2018). Når data krypteres, kan du være en kjempegod etterforsker, men du har fortsatt ikke kompetansen til å ta de kriminelle. Retrieved from https://www.politiforum.no/artikler/nar-data-krypteres-kan-du-vaere-en-kjempegod-etterforsker-men-du-har-fortsatt-ikke-kompetansen-til-a-ta-de-kriminelle/429706

UCD. (2018). University College Dublin: COMP41660: Live Data Forensics. In.

UNODC. (2013). *Comprehensive Study on Cybercrime*. Retrieved from https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

Wikipedia. (2019). Forensic science. Retrieved from https://en.wikipedia.org/wiki/Forensic_science

Årnes, A. (2018). Introduction. In A. Årnes (Ed.), *Digital Forensics*. Hoboken, NJ: Wiley.

9. APPENDIXES

9.1 Survey questions translated to English

Spørsmål | Svar

Live Data Forensics (English version)

In this study, we are interested in learning about your experience with Live Data Forensic (LDF) during your year of practice (second year of study) at PHS. We also ask some questions that give us an impression of your actual knowledge of the topic. By Live Data Forensic, in this survey, we mean the examination of an electronic device that is turned on and to which you have access. Direct examination is performed on the device, without the use of any special software. By "access" is meant that the device is not locked with a username/password or biometrics (fingerprint / face recognition, etc.). Examples of LDF may include review of call logs, messages, Internet history, photos, social media, notes and more.

It is important that you take your time, read the questions and the description carefully before answering.This is especially important when filling out matrices.

The survey is part of a Master's study for POB. Leif Erik Andreassen and pob. Geir Andresen in the subject Forensic Computing & Cybercrime Investigation at University College Dublin.

Your reply is completely anonymous and we do not have access to your name or identity.

You are not obliged to carry out/participate in the survey, it is completely voluntary!

Inndeling 1 ...

Background questions

1. Gender *

- Female
- Male

2. Age? *

Whole numbers, e.g. 21

Skriv inn svaret

3. Which mobile phone do you use privately? *

Android is the collective term for all mobile phones that use Android operating system, eg. Samsung, LG, Huawei etc. Serveral choices are possible.

- iPhone
- Android
- Other

4. Which PC/operating system do you use privately? *

Several choices are possible

- Mac
- Windows
- Linux
- Other

5. Which campus are you studying at? *

- PHS Oslo
- PHS Bodø
- PHS Stavern

6. In which police district did you practice? *

- Agder
- Møre og Romsdal
- Sør-Vest
- Trøndelag
- Finmark
- Nordland
- Sør-Øst
- Vest
- Innlandet
- Oslo
- Troms
- Øst

7. Did you have practice at a police station or a sheriff's office? *

- Police station
- Sheriff´s office

8. How do you rate your own competence in the subject "Digital policing" in relation to other students and police officers you have studied or worked with? *

By "competence" we mean knowledge and skills

	1	2	3	4	5	
Very low	○	○	○	○	○	Very high

9. How do you rate your competence in Live Data Forensic (LDF)? LDF is defined as examining and securing electronic evidence from a "live" digital device that you have access to. *

By "access" is meant that the device is not locked with username / password / biometrics

	1	2	3	4	5	
Very low	○	○	○	○	○	Very high

10. Did you have a permanent supervisor during the year? *

By "permanent supervisor" in this context is meant that you had a permanent supervisor while serving in the Patrol Section

- ○ Yes
- ○ No, I had several

11. How will you rate your supervisors competence regarding LDF? *

	1	2	3	4	5	
Very low	○	○	○	○	○	Very high

Knowledge questions

12. Is it possible to conduct LDF without changing data on the device? *

- Yes
- No
- I don't know

13. Imagine you are on a crime scene and have been ordered to bring a turned on desktop PC to your service location for further investigation. How do you want to turn off your PC before transport? *

- Use the usual shutdown routines provided by the operating system, ie to select "shut down" from the menu
- Pull the plug
- Turn off the PC using its own power button on the cabinet
- Press and hold the power button until the machine turns off

14. Imagine that you are on a crime scene and have been ordered to bring in a switched on mobile phone (locked with username / password / biometrics) to your service location for further investigation. How will you do it? *

- Network isolate (flight mode) and make sure it has power
- Make sure it has power and bag it
- No need to do anything as it is still locked
- Turn off the mobile phone and bag it

15. On a crime scene, you have been ordered to bring a turned on laptop / Mac (NOT locked with a username, password or biometrics) into the service location for further investigation. Which of the options below describes the best way to do it? *

- ○ Turn off the machine and bag it
- ○ Make sure that the machine has power and bag it
- ○ Network isolate, disable any screen lock, prevent machine from locking or running out of power

Inndeling 3 ...

Experience questions

16. Did you perform LDF during your practice year? *

The question includes LDF performed on mobile phones and computers (both portable and desktop) and cases where you performed LDF alone, with your supervisor or with others

- ○ Yes
- ○ No

17. What do you think is the reason you didn't perform LDF while you were in practice? *

Here it is possible to choose more than one alternative

- ☐ I did not feel that I had the competence
- ☐ Others did it
- ☐ I did not get into situations where LDF was applicable
- ☐ LDF was not performed because the device was brought to a specialist
- ☐ There were other service personell with more experience with LDF who wanted to do it themselves
- ☐ Other

18. In which case types did you perform LDF? *

Here you select the case type (s) you performed the LDF in. Example: You have performed LDF twice in drug cases and 1 time in a violence / threat case. Then tick "2" under drugs, "1" on violence / threats and "Not done" in all the others.

	Not done	1	2	3	4	5	6 or more
Traffic	○	○	○	○	○	○	○
Danger to life/health	○	○	○	○	○	○	○
Violence/threats	○	○	○	○	○	○	○
Sexual Offenses	○	○	○	○	○	○	○
Vandalism	○	○	○	○	○	○	○
Theft	○	○	○	○	○	○	○
Drugs	○	○	○	○	○	○	○
Economy	○	○	○	○	○	○	○
Other crime	○	○	○	○	○	○	○

19. On which device and operating system did you perform LDF? *

The question is seen in the context of the previous question. You must select a quantity for each unit. If you have not done any LDF on the particular device, select "Not done / applicable".

	Not done/applicable	1	2	3	4	5	6 or more
Desktop PC - Windows	○	○	○	○	○	○	○
Desktop PC - Linux	○	○	○	○	○	○	○
Desktop Mac	○	○	○	○	○	○	○
Laptop PC - Windows	○	○	○	○	○	○	○
Laptop PC - Linux	○	○	○	○	○	○	○
Laptop Mac	○	○	○	○	○	○	○
Mobile phone - iPhone	○	○	○	○	○	○	○
Mobile phone - Android	○	○	○	○	○	○	○
Other device	○	○	○	○	○	○	○

20. LDF is considered to be an exception from basic methodology where the general rule states that examination of electronic devices should be carried out, in retrospect, by competent personnel with the right equipment. What is the reason why LDF was nevertheless carried out in those cases from the previous questions? *

Here it is possible to choose several options

- [ ] Because the device would never be examined by a specialist afterwards
- [ ] Because critical data on the device would be lost if it the device was not examined on site
- [ ] Danger to life and health if not performing LDF
- [ ] Turning off the unit would lead to loss of critical data
- [ ] Only opportunity to access information such as cloud services, network storage, encryption, etc.
- [ ] I don't know
- [ ] We saved time performing LDF on site
- [ ] I was just asked to investigate the device
- [ ] Other
- [ ] It was common practice to do it that way in the district I was practicing

21. Were the LDF examinations documented with video, audio, picture or notes? *

If one or more of the LDF examinations were documented, answer "yes"

- ( ) Yes
- ( ) No

22. In what cases was the LDF investigation documented with video, picture or notes? *

Here you will select the case types where you documented the process using either video, pictures, notes or combinations of these. Mark the case type and number as before.

	Not done	1	2	3	4	5	6 or more
Traffic	○	○	○	○	○	○	○
Danger to life/health	○	○	○	○	○	○	○
Violence/threats	○	○	○	○	○	○	○
Sexual Offenses	○	○	○	○	○	○	○
Vandalism	○	○	○	○	○	○	○
Theft	○	○	○	○	○	○	○
Drugs	○	○	○	○	○	○	○
Economy	○	○	○	○	○	○	○
Other crime	○	○	○	○	○	○	○

23. Was a search / seizure report written in all the cases in which you conducted the LDF? *

- ○ Yes
- ○ No

24. In those cases where a search / seizure report was NOT written, what was the reason for it? *

- ☐ The case was not serious enough
- ☐ We did not find any evidence on the device that could be used in the case
- ☐ Vi forgot to do it
- ☐ Other reasons

25. In which case types was a report on search / seizure written? *

Here you should mark the number of times a search / seizure report was written for each case type. If no report was written, select "No Report".

	No report	1	2	3	4	5	6 or more
Traffic	○	○	○	○	○	○	○
Danger to life/health	○	○	○	○	○	○	○
Violence/threats	○	○	○	○	○	○	○
Sexual Offenses	○	○	○	○	○	○	○
Vandalism	○	○	○	○	○	○	○
Theft	○	○	○	○	○	○	○
Drugs	○	○	○	○	○	○	○
Economy	○	○	○	○	○	○	○
Other crime	○	○	○	○	○	○	○

26. Was there a written or oral consent from the police prosecutor to search / seize in the cases in which you executed the LDF? *

- ○ Yes, in all of them
- ○ Yes, but not in all of them
- ○ No

27. In those cases where a concent was not obtained from the police prosecutor, what was the reason for this?

Several options possible

- ☐ There was no need for it in the case (s) concerned
- ☐ Fresh deed or fresh tracks
- ☐ There was a danger of forfeiture of evidence
- ☐ I don't know

28. Is it necessary to write a search / seizure report after conducting LDF investigations on a mobile phone or computer? *

- ○ Yes
- ○ No
- ○ I don't know

29. Decide on the following statements and choose the one that best suits the district in which you practiced *

- ☐ My district had known and established routines / procedures for managing electronic devices / evidence
- ☐ The district had inadequate procedures for handling electronic devices / evidence
- ☐ I got no particular impression of the district's handling of electronic devices / tracks
- ☐ I got the impression that the handling of electronic devices / evidence on site was often random and was determined by the interest of the personell involved
- ☐ Other

30. Did you find that the knowledge you acquired in the subject "Digital policing" matched the expectations of the district in which you practiced? *

	1	2	3	4	5	6	
To a very small extent	○	○	○	○	○	○	To a very large extent

31. Did you experience anything in practice regarding the use of LDF that is not affected by the questions in the survey and that you would like to share?

Skriv inn svaret

32. Is there anything specific that we should be more or less focused on in the course of "Digital Policing" to be better prepared for your year of practice?

Skriv inn svaret