

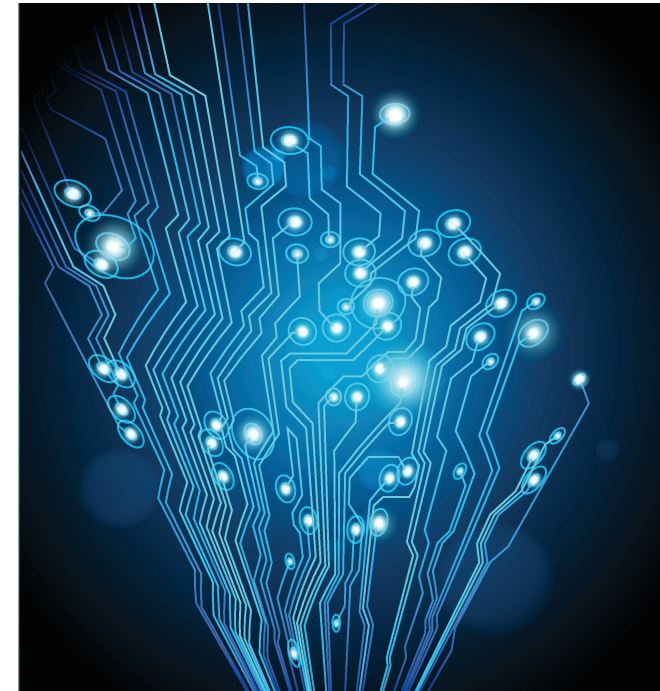
Tom Erik Erlandsen

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

Tom Erik Erlandsen

# Fallacies when Evaluating Digital Evidence Among Prosecutors in the Norwegian Police Service

June 2019







Norwegian University of  
Science and Technology

# Fallacies when Evaluating Digital Evidence Among Prosecutors in the Norwegian Police Service

Information Security: Digital Forensics and Cybercrime Investigation (MISEB)

Submission date: June 2019

Supervisor: Katrin Franke

Co-supervisor: Rune Nordvik  
Andrii Shalaginov

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



# Abstract

Digital evidence has been a part of the evidential picture in courtrooms for several years, but uncertainty still seems to surround them. The digital evidence literacy of the judiciary can potentially introduce fallacies of how the digital evidence is perceived, evaluated and weighed. This could especially present a challenge in legal systems where evidence rarely is dismissed by the court but taken into a total consideration of evidence during court proceedings. While there has been a lot of research on the ever-changing technical elements of digital evidence, there has been little research presented on how the police prosecutor evaluate and weigh the different digital evidence. This thesis presents a unique case study which explores how the Norwegian Police Prosecutor evaluates digital evidence in three created complex criminal cases. The fictive criminal cases included suspect and witness statements, police reports and background information, which all interconnected with the different digital evidence artefacts, simulating the real-life situation of evidence evaluation for the prosecutor. The results of the case study indicate that without a clearer understanding of the intricacies of digital evidence among police prosecutors in the Norwegian Police Service, we risk errors of justice.

# Sammendrag

Digitale bevis har vært en naturlig del av bevisbildet i retten i flere år, men fortsatt ser det ut til at digitale bevis skaper usikkerhetsmomenter. Rettsvesenets manglende forståelse for digitale bevis kan potensielt føre til feilslutninger som kan påvirke hvordan digitale bevis blir oppfattet, vurdert og veid i retten. Spesielt kan dette være en utfordring i rettssystemer hvor bevis sjelden blir avvist av retten, men hvor de istedenfor blir inkludert i en samlet helhetsvurdering av bevis. Mens det har vært forsket en del på de tekniske elementene omkring digitale bevis, så har det vært forsket lite på hvordan påtalejuristen vurderer og veier digitale bevis. Denne masteroppgaven presenterer en unik saksstudie som utforsker hvordan påtalejuristen i norsk politi vurderer digitale bevis i 3 fiktive komplekse straffesaksscenarioer. De fiktive straffesakene inkluderer mistenkt- og vitneavhør, politirapporter og bakgrunnsinformasjon – og hvor alt er knyttet sammen med de digitale bevisene for å skape en naturtro bevisvurderingssituasjon for påtalejuristen. Resultatet av saksstudien indikerer at uten en bedre forståelse av digitale bevis blant påtalejurister i norsk politi, så vil vi risikere justisfeil.

# Preface

I would like to thank the Norwegian University of Science and Technology for giving me the chance to learn, and for challenging me as a master student.

A special thanks to my supervisor Professor Katrin Franke, for good guidance and honesty, together with co-supervisor Andrii Shalaginov.

Hilde Bakke, I am forever grateful for all your help.

Very special thanks go out to my mentor and thesis co-supervisor Rune Nordvik, together with the rest of the NCFI team at the Norwegian Police University College, who has motivated me for years.

Thanks to OJ for support on editing.

At last I would like to thank my colleagues in the Norwegian Police Service for their good support, it was much appreciated.

# Table of Contents

List of Figures .....	xi
List of Tables.....	xi
List of Abbreviations (or Symbols) .....	xi
1 Introduction .....	12
1.1 Motivation .....	12
1.2 Research Problem .....	13
1.3 Research Questions .....	13
1.4 Research Method.....	14
1.5 Scope of the Thesis .....	14
1.6 Thesis Outline.....	14
2 State of the Art.....	15
2.1 Background .....	15
2.1.1 Criminal Investigation.....	15
2.1.2 Digital forensics .....	17
2.1.3 Digital forensic process .....	18
2.1.4 Technical qualities and the potential for errors .....	19
2.2 Evidence .....	21
2.2.1 Digital evidence .....	22
2.2.2 Evidence evaluation.....	22
2.2.3 Evidential value .....	24
2.2.4 Admissibility of evidence .....	25
2.2.5 Presenting digital evidence .....	26
2.3 The prosecutor qualifications and quality .....	27
2.3.1 Competence .....	27
2.3.2 Quality.....	29
2.3.3 Errors of justice .....	29
3 Method .....	31
3.1 Introduction .....	31
3.2 Research Methodology .....	31
3.3 Research Procedure .....	31
3.3.1 Sampling .....	31
3.3.2 Data collection.....	32
3.3.3 Data analysis.....	33
3.3.4 Creating criminal case scenarios .....	33
3.3.4.1 Scenario 1.....	35



3.3.4.2	Scenario 2.....	37
3.3.4.3	Scenario 3.....	42
3.3.4.4	Post scenario questions.....	43
3.3.5	Quality.....	43
4	Data Analysis .....	45
4.1	Introduction .....	45
4.2	Scenario 1 .....	45
4.2.1	The phone activity: .....	45
4.2.2	Call records obtained from the telecom provider: .....	46
4.2.3	The CCTV footage: .....	46
4.2.4	The manual analysis of the GPS: .....	47
4.2.5	General Comments.....	47
4.3	Scenario 2.....	47
4.3.1	Mismatching Checksum.....	48
4.3.2	Chat Log .....	49
4.3.3	Mailaddress .....	49
4.3.4	Illegal Images – General Comments .....	49
4.3.5	Illegal images from the phone .....	50
4.3.6	Illegal images from the computer.....	51
4.3.7	Illegal images from the browser history .....	51
4.3.8	Browser history: .....	52
4.3.9	Anti-virus search.....	52
4.3.10	Missing Messenger chat on the phone:.....	53
4.3.11	General comments from the participants during scenario 2: .....	53
4.4	Scenario 3.....	54
4.5	Quality and competence.....	55
5	Discussion.....	59
5.1	Which potential occurrences of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence may be identified?.....	59
5.1.1	Scenario 1.....	59
5.1.1.1	The phone activity from the suspect's mobile phone:.....	59
5.1.1.2	GPS unit .....	60
5.1.2	Scenario 2.....	61
5.1.2.1	Mismatching checksum .....	61
5.1.2.2	Mail address .....	61
5.1.2.3	Illegal images .....	62
5.1.2.4	Browser history .....	63

5.1.2.5	Antivirus search .....	63
5.1.2.6	Missing Messenger chat .....	64
5.1.3	Scenario 3.....	64
5.1.4	Summary .....	65
5.2	Which of these occurrences may be identified as potential fallacies due to lack of knowledge and competence of digital forensics principles? .....	66
5.2.1	The phone activity timeline from the suspect's mobile phone .....	66
5.2.2	The manual analysis of the GPS unit.....	67
5.2.3	The missing identification of digital evidence .....	67
5.2.4	The mismatching checksums of the suspects computer .....	68
5.2.5	The illegal images .....	68
5.2.6	The browser history from the suspects computer .....	69
5.2.7	The performed anti-virus search on the suspects computer .....	70
5.2.8	The missing Messenger chat on the suspects mobile phone .....	70
5.2.9	The IP search from scenario 3.....	71
5.2.10	Summary .....	71
5.3	What are the consequences if these fallacies occur, and how can they be mitigated? .....	72
5.3.1	Consequenses.....	72
5.3.2	Mitigation.....	73
6	Conclusions.....	76
6.1	Digital evidence were not evaluated and weighed in compliance with the technical quality of the evidence .....	76
6.2	Fallacies due to lack of knowledge and competence were identified .....	77
6.3	Consequences and Mitigation .....	77
7	Future work .....	79
8	References .....	80
9	Appendices .....	84

# List of Figures

Figure 2.1: The figure shows the general outline of the process a criminal case follows through a justice system .....	16
Figure 2.2: The figure shows the criminal investigation process model .....	17
Figure 2.3: The figure shows the collection and processing process model .....	17
Figure 4.1: The phone activity.....	45
Figure 4.2: The manual analysis of the GPS .....	47
Figure 4.3: The distribution of identification of digital evidence.....	48
Figure 4.4: Illegal images from the phone .....	50
Figure 4.5: Illegal images from the computer.....	51
Figure 4.6: Illegal images from the browser history .....	51
Figure 4.7: Browser history .....	52
Figure 4.8: Distribution of warrants .....	54
Figure 4.9: Distribution of trust .....	55
Figure 4.10: Distribution of trust in automated tools .....	56
Figure 4.11: Distribution of knowledge on forensic software.....	57
Figure 4.12: Questions from members of court .....	57

# List of Tables

Table 4.1: Evidential value on identified evidence .....	48
--	----

# List of Abbreviations (or Symbols)

NCPC	Norwegian Criminal Procedure Code
DFD	Digital forensic detective
DNA	Deoxyribonucleic acid
ACPO	Association of Chief Police Officers
Malware	Malicious Software
IP	Internet Protocol
SMS	Short message service
FBI	Federal Bureau of Investigation
IT	Information Technology
CCTV	Closed-circuit Television (surveillance)
GPS	Global Positioning System
NCIS	National Criminal Investigation Service (KRIPOS)
GEO	Geography
ISP	Internet Service Provider
DDos	Distributed denial of service
VPN	Virtual Private Network
OÅO	Obligatory Yearly Training

# 1 Introduction

During my career in digital forensics, I have had multiple appearances in court as a police witness, and it has always impressed me how well the police prosecutor and the other members of court were arguing their cases. Judicial consequences of traditional evidence seem to be argued with ease, and the context in which the evidence is presented in is understood by the court. But as a police witness, I have also experienced presenting digital evidence in court, which suddenly made the process of evaluating and weighing evidence seem to become increasingly more difficult.

The same insecurity has to some extent been observed with regards to police prosecutors, especially when they were set to establish the correct connection between judicial weight and technical quality of digital evidence.

This made me interested in gaining insight into if lack of knowledge and competence on digital evidence and digital forensic principles could introduce fallacies into the prosecutor process of evidence evaluation, leading to digital evidence being given an evidential value not in compliance with the technical quality of the evidence, thereby presenting digital evidence in court which could potentially and unintentionally mislead the members of court.

This thesis presents a case study where 14 prosecutors from the Norwegian police service evaluated and weighed digital evidence artefacts in a criminal case setting.

To gain necessary insight into the black-box process of evidence evaluation, a situation where the context and the contents of the evidence evaluation could be controlled was created. To simulate the process of controlled context evidence evaluation, 3 fictive complex criminal case scenarios were created. The scenarios included background information as police statements from witnesses and suspects, technical reports and police reports presenting different digital evidence artefacts of various technical and judicial evidential qualities.

All criminal case background information and different digital evidence artefacts were created to interconnect with each other, by this simulating natural real-life situation for the prosecutor, gaining insight into the cause-and-effect relationship of the various technical evidence qualities and the evidence evaluation results.

## 1.1 Motivation

The effects of digitalization and the increased use of technology have an impact on all parts of society, including where evidence necessary for solving criminal investigations may be located. With more of the sources of evidence being digitalized, evidence now often resides in a digital format. This rise in sources of digital evidence has gradually made digital evidence a naturally part of the evidential picture in all kinds of criminal investigations.

At the same time digital evidence is also becoming increasingly important in all aspects of criminal investigations. This has led to an increased pressure being put on delivering fast-track digital evidence, and this led me to my research project "*Verification of commercial automation in mobile forensics*". The results of this project indicated that

without proper verification, digital evidence gathered and recreated from a mobile phone with an automated content analysis can lack completeness (1). Given the results of the study, there may be a potential of digital evidence being misinterpreted, especially if the person set to evaluate the evidence do not possess the level of knowledge and competence needed to understand the basic principles surrounding digital evidence and digital forensics.

While there has been some research on the potential of errors with regards to the handling of digital evidence in criminal investigations (2), and errors of justice within the criminal investigation (3), there has been little focus on the knowledge and competence of the police prosecutor on evaluating technical irregularities in digital evidence artefacts, especially with a Norwegian legal viewpoint.

In an open and democratic police the potential challenge to the rule of law regarding poorly evaluated digital evidence should be taken seriously. Insight into the prosecutor process of evaluating and weighing digital evidence may assist in mitigating potential future errors of justice, and by this help uphold the rule of law.

The thesis might be relevant for the police prosecutor, police officers and detectives, members of court, and the digital forensics community at large.

## 1.2 Research Problem

On the basis of this, a research challenge was formed:

How does the lack of knowledge and competence of digital evidence and digital forensics principles introduce fallacies in to the rule of law particular with regards to the prosecutor process of evaluating and weighing digital evidence in compliance with the technical quality of the evidence?

The research challenge was a continuation on the results of my research project, where the results indicated that if an automated analysis were not manually verified, the evidence could lack completeness. Lack of evidential completeness may open up for potential misinterpretations of digital evidence if the results are not verified or questioned, for instance by the police prosecutor in the process of evaluating and weighing digital evidence.

## 1.3 Research Questions

To be able to answer the research challenge, some sub-challenges were defined. These were:

- Which potential occurrences of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence may be identified?
- Which of these occurrences may be identified as potential fallacies due to lack of knowledge and competence of digital forensics principles?
- What are the consequences if these fallacies occur, and how can they be mitigated?

## 1.4 Research Method

The research method in this thesis had a qualitative design and a collective case study approach in an interview format.

Data was collected by interviewing and observing 14 police prosecutors from the Norwegian Police Service through 3 different fictive criminal investigation scenarios.

3 fictive complex criminal case scenarios were created. The scenarios included connecting background information as police statements from witnesses and suspects, technical reports and police reports presenting different digital evidence artefacts of various technical and judicial evidential qualities. All artefacts were created to interconnect with each other, by this simulating natural real-life situation for the prosecutor, gaining insight into the cause-and-effect relationship of the various technical evidence qualities and the evidence evaluation results.

## 1.5 Scope of the Thesis

This thesis has a Norwegian legal viewpoint, and a technical focus.

The focal points have been on digital evidence being weighed and evaluated in compliance with the technical quality of the evidence, and if traces of fallacies due to lack of knowledge and competence on digital evidence and digital forensic principles potentially are introduced into the evidence evaluation process.

The thesis also focuses on the consequences such technical fallacies may have for the rule of law.

## 1.6 Thesis Outline

In chapter 2, the state of the art and theory related to the research problem will be presented, including theory on competence, evidence, digital forensics, criminal investigations and evidence evaluation.

Chapter 3 presents the research design, and choice of methodology of the thesis, and discusses potential weaknesses.

Chapter 4 presents the collected data in a data analysis.

Chapter 5 present the discussion and interpretation of the data.

Chapter 6 contains the conclusions.

Chapter 7 presents future work.

## 2 State of the Art

### 2.1 Background

This master thesis is a continuation of my research study (1), where parts of the undersection 2.1.4 (Technical qualities and the potential for errors) are included. The section has been further developed, rewritten, referenced, and updated.

This chapter include a presentation of the criminal investigation (see chapter 2.1.1), digital forensics (see chapter 2.1.2), the digital forensic process (see chapter 2.1.3), the digital forensic principles (see chapter 2.1.4), and technical quality of (see chapter 2.1.5).

#### 2.1.1 Criminal Investigation

This thesis addresses the prosecutor process of digital evidence evaluation, and as this is a part of the criminal investigation process. A brief description of the criminal investigation is therefor required, including the rules and regulations that govern the investigation, and roles and models within investigations.

Criminal investigation is one of the main responsibilities of the Norwegian police service. Investigations of potential criminal acts are opened and exercised by the police (4).

What guide all investigations is the need of purposefulness, and the Norwegian Criminal Procedure Code (NCPC) §226 describe and regulate the objective of the investigation (5). For this thesis, the § 226, letter a) and b) are especially interesting.

The NCPC § 226 states that purpose of the investigation are to; a) decide the question of indictment, b) to serve as preparation for the court of the question of guilt and the potential question of the appropriate level of the reaction.

Myhrer defines the criminal investigation as (6);

"a purpose guided collection of information for determining the basis of whether or not a criminal reaction should be inflicted upon someone due to their committed acts"

In an investigation there will be many roles involved. The main roles of the investigation include the police prosecutor, the investigative detective, and the investigative leader (6). Due to the scope of the thesis, the role of the digital forensic detective (DFD) will be given a short presentation in addition to the role of the police prosecutor.

The police prosecutor has an educational background in the Master of Laws. In addition to potential post graduate studies from the Norwegian Police University College. The police prosecutor has also an obligatory 105-hour start-up course at the Norwegian Police University College (7, 8).

The prosecutor has an overall responsibility as an investigative lead with regards to which investigative steps to undertake to fulfil the legal requirements of the criminal case. The actual involvement of the prosecutor will naturally depend on the seriousness of criminal case in question, and in all practical sense investigations opened and

exercised all the time without the prosecutions involvement, due to delegation of authority (9).

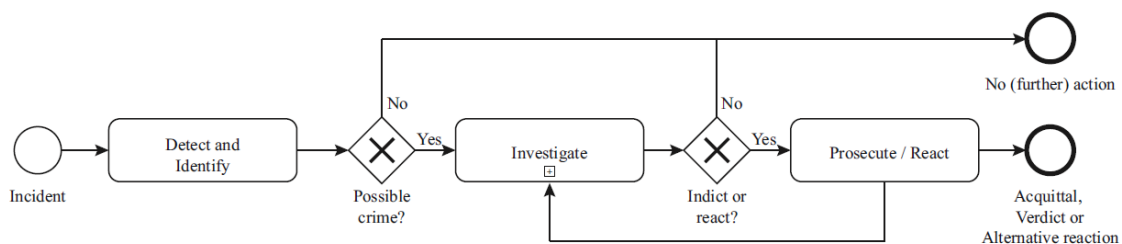
In Norway the prosecution is an integrated part of the police service (9).

The tasks of the prosecution can be divided into 4 main groups; investigative lead, decide if an indictment should be stated or not as a result of the investigation on the basis of the information and evidence collected, act as a prosecutor in court, and enforce the execution of sentences (9). Due to the scope of this thesis, the prosecutor task of deciding on if an indictment should be stated on the basis of the evidence of the case will be the only focus of the roles of the Norwegian police prosecutor.

A criminal investigation or criminal case has multiple stages and could be described from several viewpoints and models. Myhrer represent a legal viewpoint, and name these stages the investigation stage, prosecution stage, judgment stage, completion stage, and archive stage (9).

Fahsing presented in his doctoral thesis *the investigative cycle*, a model for the investigation process which covers information collection and testing of information in a repetitive cycle (10, p.102). The model covers the collection of all relevant information; *collect*, the control if the information is relevant, accurate, and reliable; *check*, the analysing and cross-checking of the data from various sources; *connect*, the construction of relevant and competing hypotheses; *construct*, the consideration of how to test the hypotheses; *consider*, and the consultation of others to challenge your own beliefs; *consult*.

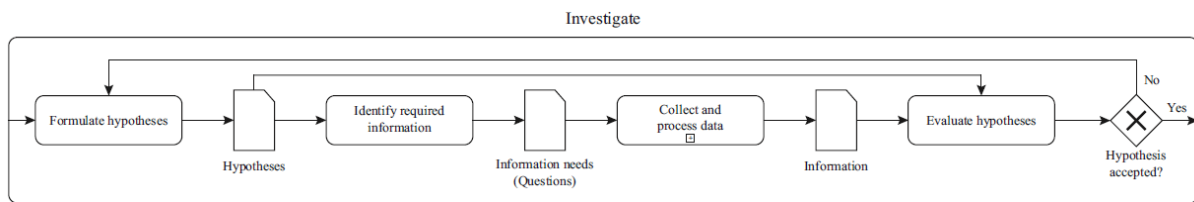
Stig Andersen has presented a preliminary process model for criminal cases and investigations (11). The model is built on hypothetico-deductive thinking and visualizes the different steps of the criminal investigation. The criminal case process model visualizes the relationship between crime detection, investigation and prosecution.



**Figure 2.1: The figure shows the general outline of the process a criminal case follows through a justice system**



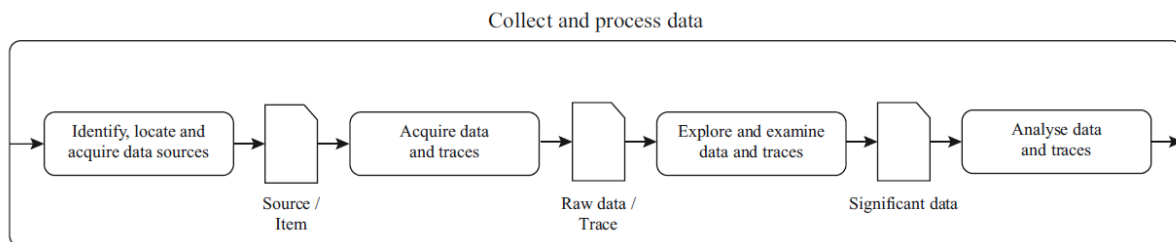
Using the criminal case model, it would be easy to visualize the focus of this thesis, and on which stage the focus lies. The evidence evaluation process of the prosecutor as focused on in this thesis would be found in the "indict or react" stage and partially in the "prosecute / react" stage, depending on the results of the evidence evaluation.



**Figure 2.2: The figure shows the criminal investigation process model**

The evidence evaluation could also result in the prosecutor needing more information to decide if a indictment should be written, by this ordering specific investigative steps and cycling back to the "investigate" stage, and to the "information needs" stage of the investigate model, see figure 2. The information need of the prosecutor could result in new evidence being collected and processed, which in the end would lead to the prosecutor again evaluating evidence at the "indict or react" or "prosecute / react" stages shown in figure 2.1.

The "collection and processing process model" also go into detail about the collection and processing of data, which would be especially useful for describing, visualizing, and understanding digital evidence processes, see figure 2.3.



**Figure 2.3: The figure shows the collection and processing process model**

Even though this thesis focus on the prosecutor evidence evaluation process, the prosecutor normally also would be involved in decisions in other stages of the investigation as being responsible for the total investigative effort. However, the prosecutor as investigative leader is not the focus of this thesis.

### 2.1.2 Digital forensics

The term digital forensics as used in this thesis would only relate to the criminal investigation process conducted by the police.

Forensic science can be referenced as when scientific methods are used to establish legal facts. Forensic science can include for instance; DNA-analysis, handwriting examination, forensic psychology, forensic toxicology, drugs-analysis and interpretation, weapons and ammunition and forensic pathology (12). In addition to the 7 different fields of forensic sciences, digital forensics is regarded as the 8<sup>th</sup> field.

In this sense, digital forensics can be seen as forensic science applied to digital information (13, p.17). or in other words; the application of computer technology to a matter of law.

Digital forensics are often divided into 6 subsections; computer forensics, software forensics, database forensics, multimedia forensics, device forensics, and network forensics (12).

### 2.1.3 Digital forensic process

The digital forensic process can be seen as the forensic standard when working with digital evidence, and would by this be within the scope of the thesis.

Flaglien describe the digital forensics process as (13, p.28).

"The digital forensic process supports a structured and sound investigation of digital evidence from any device capable of storing or processing data and information in a digital form".

Flaglien divide the digital forensic process into 5 steps; identification, collection, examination, analysis, and presentation.

These steps describe the identification of potential sources of digital evidence, collection of the digital evidence by forensic imaging, the examination and pre-processing of collected data, analysing the data to identify important information, and presenting the evidence in a report and / or in court. The digital forensics process can be repetitive, depending on the results during the process. Thus, the process can be rolled back to a previous step, and repeated, if new evidence is introduced during an investigation. Following the structure of the digital forensic process is meant to ensure good evidence integrity in the investigation.

The steps in the digital forensics process are guided by some principles. These principles are known as the digital forensics principles, and are a set of principles to guide the digital forensics detective (DFD). The first of the principles are *forensic soundness*; or forensically soundness, is often used to describe best practice and legal requirements of how to handle digital evidence. The term can involve every aspect of the digital forensic process, and points to the ideal state. Flaglien describe forensic soundness as (13, p.29);

"A process or method can be considered forensically sound if it maximizes the probability for finding the strongest, admissible evidence with the resources available, together with documentation of the process, key assumptions, and uncertainties."

The next principle is *evidence integrity*. This principle is the core of all forensic work, and points to the preservation of the evidence in original form. In digital forensics this integrity is often controlled for by having algorithms calculate the mathematical value of the digital evidence, and then cross-checking the values of the evidence in original form and the forensic copy, by this establishing the integrity of the evidence image file (14, p.6). These algorithms can differ in complexity and are called *cryptographic hashes*.

The chain of custody points to the ability to preserve the evidential integrity through all steps of the digital forensic process, and to be able to document it. The documentation should involve at least information about; who handled the evidence, which processes and procedures were performed, when the collection and forensic imaging was performed, where the evidence was collected, how the evidence was collected, and why the evidence was collected (13, p.35)

The Association of Chief Police Officers (ACPO) has issued a Good Practice Guide for digital evidence. For the scope of this thesis, and the role of the Norwegian police

prosecutor as an evidence evaluator with regards to the overall responsibility of the quality and outcome of a criminal investigation (15, p.6), I present the principles:

*Principle 1:*

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

*Principle 2:*

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

*Principle 3:*

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

*Principle 4:*

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

Digital forensic are performed on a daily basis in the Norwegian police service. The ACPO principles implies that the prosecutor being the overall responsible for the investigative effort would need the necessary knowledge and competence on digital forensics and the digital forensic principles to ensure the quality of the investigation. This would apply both to the ordering of new investigative steps, and to identify errors.

#### 2.1.4 Technical qualities and the potential for errors

This thesis addresses the problem of digital evidence not being weighed in compliance with the technical quality of the evidence. This requires some elaboration on the digital artefacts with regard to the scenarios.

The number of digital artefacts that can be presented as evidence is huge, and there can be just as many issues and potential errors influencing the technical quality of these artefacts, so it would not be possible to cover all these in this thesis. I will therefore focus on the artefacts in the scenarios of the thesis.

There can be many reasons for digital evidence artefacts having issues with the technical quality with regards to its potential value as evidence, and both potential man-made or automated processes that could influence the quality. However, the use of automation and verification play a role in the case study scenarios, so a brief presentation of the facets of the subject is required.

Automation has played a part in digital forensic for many years, and the use of automated forensic tools is almost unavoidable due to large digital evidence datasets combined with the hardships of analysing data at bits and byte level (16). Often the automated forensic tools are easy-to-use, and the use would not require digital forensic competence, which is practical regarding the inaccessibility of the DFD in many criminal cases. However, there could be clear risks combined with judicial personnel without digital forensic knowledge and competence evaluating digital evidence artefacts from automated tools. Digital evidence artefacts might contain important evidential information without any obvious links between the artefact and the evidence, by this

obfuscating the true value of the artefact thus making the evaluation of the potential evidential value of digital evidence difficult (17, 18).

Another challenge automated forensic tools can present is that the non-technical police officer may appear more knowledgeable than s/he actually is (19). This obfuscation can be misleading and introduce difficulties for the prosecutor when s/he are to evaluate the competence of the police officer producing the digital evidence, which can be of importance for identifying potential weaknesses in the digital evidence. This could increase the possibility for unintentionally trusting digital evidence with low technical quality.

There are more things to consider when evaluating digital evidence produced with automated tools. One of the main limitations of automation is the inflexibility it presents. With the proliferation of new mobile applications and frequency of released version updates, there will be difficult to keep the automated forensic analysis tool up to date. This inflexibility would also inflict on the tools ability to adapt to a specific case (19), which could further complicate the digital evidence evaluation process for the prosecutor. If the process of interpreting digital evidence is inaccurate, leading to erroneous data being presented to the prosecutor for evaluation, all the trailing assessments may be compromised, potentially beyond the knowledge of the prosecutor (20). In such a situation, the error would be difficult to identify, and could easily end up as an error of justice (see chapter 2.3.3).

Therefore, with the use of automation in digital forensics there will be an increased need for verification. Verification can be seen as a confirmation of validation by the use of laboratory tools, techniques and procedures (21). A lack of competent manual verification of output from automated forensic tools can affect the result of an investigation, by overlooking artefacts not found by the automated analysis, leading to incorrect evaluation of the digital evidence (1, 16, 19).

This could especially present a challenge in countries with no strong restrictions on the admissibility of digital evidence in court, like in the Norwegian Judicial system (see chapter 2.2.2 and 2.2.4).

In judicial systems with free evidence admissibility and free evidence court evaluation like Norway, there is an existing risk of digital evidence produced by an automated analysis tool being presented as digital evidence without proper verification. As more sophisticated automated analysis tools are developed, the difficulty to validate and verify their results. It is important to remember that mistakes made due to a poor digital forensic process can lead to errors of justice, and that the prosecutor will play a significant role in identifying these weak processes. To be able to do this, knowledge and competence on how these digital forensic processes work are needed, also among the judiciary (22).

In this thesis browser history and cached information from internet play a role as digital evidence artefacts. A presentation of these artefacts is therefore required. Browser history can be explained as a log of the visited web pages. When surfing the internet, the web browser saves information like web pages and images to the computer with the purpose of making the surfing experience seamless and fast. The idea behind this is that the browser by this can anticipate the next web page visit, and by this load the information faster. The implications of this could be that the browser may save information you necessarily have not visited. These artefacts are saved to a temporary

cache, and the stored information can be called temporary internet files (23, p.213) . These temporary files and artefacts are often recreated during a digital forensic analysis but could due their nature have a technical low quality, all the time the uncertainty of the web visits is not verified.

Another digital evidence artefact in the case study scenario is time. Time is of great importance in the most traditional sense in an investigation, but also within digital forensics time is one of the most important digital evidence artefacts. To establish a timeline of digital events, time will of course be one of the key elements. But unlike time in the analogue world, data can travel around the world in a second, and on its way it can pass through multiple layers and platforms, which could complicate the understanding of time a bit. **How** time was registered, **which** time was registered, and **when** was time registered, are all important questions of the digital evidence. In digital forensics, time is not only time, and multiple formats of time exist. One of the fundamental mistakes in digital forensics would be to forget to check the time setting of a device due to the potential time-skew between actual time and the device registered time. For instance, could a third-party mobile phone application register timestamp differently internally than the actual time within the database of the application. This applies to the how, which and when of time registration. A mobile phone chat application registers a chat message sent at a specific time due to how the application is programmed to do this. The host phone could in theory register time on another programming basis, and to make the picture complete; the forensic analysis tool and host computer could also register timestamp different altogether, and failing to document and control the factor of time could result in erroneous forensic results (23, p.208). This makes timestamps an artefact of utmost importance in digital forensics.

In the case study scenarios, antivirus software is one of the artefacts. Antivirus software helps protect digital devices, in most cases a computer, against malware. Malware can be described as malicious software or programs. The antivirus software searches through files, programs and web pages, and looks at data for known threats and also sometimes monitors the behaviour of programs installed on the computer. If a threat is found by the antivirus software, the threat will be flagged or dealt with as the antivirus software is set up to react by the user. The antivirus software uses databases containing information of known malware as reference when searching. If this database is not updated, or the antivirus software encounter new malware not registered in the database of the software, there is a possibility for the malware not being discovered and flagged. Using more than one antivirus software tool, and performing new searches if there has been time passed since the last search, would be preferable if there is an uncertainty of whether the computer is infected or not (24).

The last artefact is the IP-address, and the tracing and identification of the user of an IP-address. To properly trace an IP-address you will need to run a WHOIS search on the IP-address to find the internet service provider who runs the specific IP-address. When the internet service provider is identified, the police then contact the provider and ask for user / subscriber information of the user of the specific IP address at the specific time in question.

## 2.2 Evidence

This thesis has a technical focus, and not a judicial. But when addressing evidence evaluation, it would be difficult to avoid some legal aspects regarding evidence.

The thesis as stated also has a Norwegian legal viewpoint, and the different legal terms regarding evidence would be based on Norwegian law definitions.

This chapter include a presentation of digital evidence (see chapter 2.2.1), evidential value (see chapter 2.2.2), evidence evaluation (see chapter 2.2.3), evidence admissibility (see chapter 2.2.4), and presentation of evidence (see chapter 2.2.5).

### 2.2.1 Digital evidence

Evidence can be seen as anything that can be relevant to the court when establishing the true facts of the case (25, p.508). However, this legal definition implies that evidence can exist without having evidential value.

Within the scope of this thesis the term *evidence* will be referenced as *digital evidence*, and there are multiple definitions of digital evidence.

Smith and Kenneally views digital evidence as (26);

"the manifestation of temporal and spatial features of human-machine and machine-human transactions".

Brian Carrier defines digital evidence as; "*an object that contains reliable information that supports or refutes a hypothesis*" (14, p.4), which is the definition Årnes bases his definition on (13, p.19):

"Digital evidence is defined as any digital data or objects that contain reliable information which can support or refuse a hypothesis of an incident or crime."

In this thesis the definition from Årnes will be used when describing digital evidence.

### 2.2.2 Evidence evaluation

Even though this thesis has a technical focus, the problem of the thesis addresses the evidence evaluation process of the police prosecutor. A short presentation of evidence evaluation with from a Norwegian judicial perspective would be required to address the problem of the thesis.

Court convictions are based on facts. If the Norwegian court judge is not able to establish agreement between the different parties of a court case on which facts of truth the case should be decided on, the facts would be settled through a judgment of the evidence, by this establishing if the different alleged facts are proved beyond reasonable doubt in an overall assessment (27, p.11).

In Norwegian law evidence evaluation can concern the *evidence evaluation* of the courtroom judge deciding the outcome of a court case. In this meaning, evidence evaluation would imply the weighing of all evidence in a case to establish the truth, and through this pass sentence. However, it can also concern the evidence evaluation of the police prosecutor when assigning *evidential value* or *evidential weight* to digital evidence collected and analysed in an investigation, getting ready for issuing an indictment or not.

The police prosecutor is seen as the first guarantor for the rule of law in the Norwegian judicial system, and evidence evaluation is one the main traits of the prosecutor (4, p.36).

In this thesis, the term evidence evaluation would be based on the prosecutor process of evaluating and weighing digital evidence collected during an investigation, with the aim

of assigning the digital evidence evidential value based on the quality of the evidence, and what it would prove with regards to the question of indictment.

Evidence evaluation can be described as a thought-process where evidence is evaluated with regards to establishing its judicial value. Value in this sense meaning the level of inherent conviction the evidence would possess (25, p.80). This value or weight would be depending on the reliability of the evidence, the authenticity, and of the accuracy of the evidence.

This thesis having a Norwegian legal viewpoint, the laws and regulations of the Norwegian judicial system will be of importance. The Norwegian judicial system has implemented the principle of *free evidence evaluation*. This principle is built upon the notion of the ability of the judge best being capable to establish the truth of the case if s/he is not bound by rules of the law, also with regards to the method chosen for the evidence evaluation (25, p.105). Kolflaath divides the evidence evaluation into 2 different directions; the impression-based and the reason-based evidence evaluation (25, p.510-11). The impression-based evidence evaluation is guided by intuition and feelings, where the absence of reasoning is defining. This has led to the somewhat widespread notion of a judicial logic of *overall assessment*. Even though overall assessment of evidence is supported by Norwegian Supreme Court rulings, the danger of overall assessment being just another notion of a *gut feeling* is however present. It is therefore important to strive for the rationally overall evidence assessment, based on reason. The reason-based evidence evaluation is more demanding, and implies the use reasoning in the evidence evaluation, by this focusing on the actual content of the evidence, rather than the elements of feelings and intuition.

Kolflaath argues for a more structured and methodical approach for the evidence evaluation, and that this approach could increase the accuracy of the evidence evaluation. He continues to debate the reasons for the lack of structure in the evidence evaluation within Norwegian law. One reason could be the connection to the respect for the autonomy of the free evidence evaluation when seen in the light of the principle of free evidence evaluation. Another possible reason Kolflaath present is the notion of that evidence evaluation can be performed by any just and reasonably equipped person by using common sense has manifested itself thoroughly in the Norwegian judiciary community. The same attitude has manifested itself into the fact that evidence evaluation has been almost totally absent as a subject in law schools in spite of the massive significance evidence evaluation has for the society.

However, while common sense and a reasonable know-how of human cognitive witness psychology would get you far in evaluating human witness statements and relations, there is reason to question the abilities of the evidence evaluator with the same ballast as guidance when evaluating digital evidence (25, p.63) . Lie debate around the role of the forensic expert witness in the context of the Norwegian law. He states the problem of technology being increasingly more difficult to evaluate for judges, and by this the worry if the technology behind forensics findings really are as forensically sound as stated by the police and prosecution. This presents an alienation and uncertainty, due to the lack of understanding of how the technology actually works (25, p.64).

This consequence of these factors for the Norwegian police prosecutor would be both a potential lack of competence in or structured methods of evidence evaluation, and a complicating element of technology playing into the evidence evaluation.

There has been very little research on the evidence evaluation process as far as I have found, especially in a Norwegian context. In 1999 a research report was published that described research conducted within 2 Norwegian police districts in the Norwegian police service. The focus of the research was on the quality of the police investigation on the behalf of the Norwegian department of justice (28). In this research, a questionnaire was sent to 10 police prosecutors, where they were to answer questions about a selection of their last criminal cases.

This research was however more focused on the quality of the efficiency of the police prosecutor, and the quality of the proceedings, and not quality as described in this thesis. However, some of the findings from this study were interesting. One of these was the inconsistency between prosecutors of understanding the level of the evidential requirements for when a case could be indicted (28, p.68). This finding can potentially connect to the confusion of the evidence evaluation process as described by Kolflaath. Another interesting aspect of the research was the answers given by the prosecutors when asked what had importance for the quality of an investigation, where close cooperation between the prosecutor and the detective, and consciousness of what quality is, what affects quality, and which demands one should have to the investigation, was mentioned. The research did not assess the evidence evaluation, and digital evidence was not a part of the scope of the research.

### 2.2.3 Evidential value

The thesis addresses the problem of assigning evidential value to digital evidence based on the technical quality. This would require a superficial presentation of the judicial discussion about evidential value.

In Norwegian law terms, evidential value is not much used. The legal term *evidential weight* can be described as the inherent force of conviction the evidence projects. In this thesis the term evidential value will be used, with regards to the evidential weight.

To establish the evidential weight or value evidence would be the focus of an evidence evaluation, as described in section 2.2.2. To be able to assess if the defendant has behaved as described in the indictment, evidence are presented to the court. These pieces of evidence can be of various types, but due to the scope of this thesis, digital evidence will have the focus.

In a criminal case it needs to be proven beyond reasonable doubt that the defendant has behaved as described in the indictment. This is defined as reaching the *evidentiary standard of proof*. In Norwegian criminal law this is described as being close to 100% certainty (25, p.513-14).

To reach the required evidential level, one would need to prove the fact of the case beyond reasonable doubt. This will often be decided by the judicial weight or evidential value of evidence. When using digital evidence as an example; the judicial weight or evidential value could be dependent on several factors, for instance the technical quality of the digital evidence and if the digital evidence is proving what it needs to prove.

For instance, a recreated SMS message could have a high technical and forensic integrity, but this would not matter if the SMS message did not contain any information about the crime in question. This would give the SMS message high technical quality and integrity but no information value, hence a low evidential value. The similar would apply if the recreated SMS message had a low technical and forensic integrity but contained



information about the crime. This would give the SMS message low technical quality and integrity, but high information value, hence a low evidential value. In this sense the actual content of the SMS message could help in proving the crime, but if there was no way to decide if the SMS message had been sent or received, and this was the focal point of the criminal case, the evidence would have been interesting for the criminal case, but it would not prove anything.

Real-life evidence evaluation is a bit more complex than this. In Norwegian law the last example of the recreated SMS message with low evidential value due to the low technical quality still could have been debated in court due to the principle of free admissibility of evidence and the principle of free evidence evaluation. This is because in Norwegian law evidential value are connected to the courts right to freely evaluate evidence, and the principle of free evidence admissibility. This further implies that it is the court which assesses and weighs credibility of the quality of the digital evidence (25, p.103).

This would imply that to say anything about the evidential value, you also would have to say something about evidence evaluation and evidential requirements. (25, p.104) .

When reading about the topic evidence and evidence value it is easy to recognize the need for substantial legal competence when set to establish evidential value. When mixing digital artefacts into this process it quickly gets even more complicated.

Smith and Kenneally problematizes the evidentiary implications of humans not being able to give eyewitness testimony about computer processing in the same way as they are making firsthand observations in real-life situations (26).

“People make interferences and draw conclusions using tools that indicate what is going on inside the computer and networks”.

Put into context of this thesis this would mean that a DFD could state in a legal report that a forensic tool ran at a specific time, and produced analysis of the digital evidence as presented. But the actual data was registered and processed according to the underlying programming and could have be victim of alteration without the DFDs knowledge or suspicion, yet the DFD presentation of the digital evidence would still be the same. The conclusions are being made by the algorithms of the forensic software. This would complicate determining evidential value, especially for a prosecutor without any knowledge and competence on digital evidence or technology.

#### 2.2.4 Admissibility of evidence

As stated, this thesis has as a technical focus, but a Norwegian legal viewpoint. A short presentation of the basis of evidence admissibility in Norwegian law is therefore required.

In the Norwegian judicial system there is free admissibility of evidence. The Norwegian Criminal Procedure Code, § 292, 2<sup>nd</sup> subsection regulates this part, and it has also been supported by several Supreme Court rulings (25, p.128).

The principle of free evidence admissibility is a central principle in the Norwegian legal system. Evidence is rarely dismissed, but instead evidence credibility is taken into an overall assessment of evidence during the court proceedings (25, p.91) .

The Norwegian judicial system there is also the principle of free evidence evaluation, see chapter 2.2.2. This together with the principle of free admissibility of evidence put a lot of responsible on the prosecutor and the court judges, due to the possibility of evidence and digital evidence of low technical quality entering the courtroom, were the judges are

to decide on the evidential value of the different evidence. The evidence will then be evaluated together in an overall assessment, see chapter 2.2.2.

### 2.2.5 Presenting digital evidence

As the prosecutor mainly relates to legal documents produced during the criminal investigation, the problem of the thesis would by this require a presentation on how the digital evidence would be presented to the prosecutor.

The prosecutor will read the legal documents of the criminal case and evaluates the evidence as they are presented in for instance police reports or police statements. The prosecutor then decides if the suspect should be indicted, and of which crimes the indictment should consist of, all depending on if the evidence support or refute the suspicion. This implies that the digital evidence would be presented or described in a legal document, like a police report. The police report is legally regulated in the Norwegian police instructions (29), and the law of police (30). The general rule imposes on the police officer to; "*write reports on the acquired knowledge that may have an interest to the work of the police*" (31, p.15).

The thesis will not cover all the details and rules of the police report, but as mentioned the prosecutor mainly relates to legal documents in the role as evidence evaluator, reports will be of some importance.

The prosecutor relates to legal documents and is skilled in the art of argumentation-theory and good common language. As Kolflaath states;

"The language is the lawyers' most important tool."

He also points out that rules are abstract and are conveyed through language. The laws are also written, and a large part of the prosecutor daily work would involve interpretation of textual laws (32, p.13) . The point here is that the prosecutor uses the written language to convey legal arguments, including the evaluation of evidence. This may have profound influence on how the prosecutor would read and interpret legal text documents, or in the scope of the thesis; how digital evidence is perceived.

Or as Kolflaath states it, language precision is important, and especially within a judicial context, where the use of unclear language could result in grave consequences (32, p.14). He points to examples from the Norwegian Supreme Court, where the use and meaning of a few words are debated deeply, resulting in rulings which influence the society in many different ways. The result of this would be that both the police officer and the DFD, possibly with a technical educational background without training in legal reporting, would gain a lot to perfect their reports and the way they argue and present digital evidence in reports.

In Norwegian law, the principle of orality has strong basis. The principle means that the judge only get the evidence presented orally in court and this also will have an influence on how digital evidence is perceived (25, p.100). The court as evidence evaluator is outside the scope of the thesis but will be mentioned as it also would influence the prosecutor in the evidence presentation.

Smith and Kenneally emphasizes that the technical experts need to become story tellers. The total context and details of the digital evidence must be constructed and presented to make sense of the material. This behoves the DFD to the use of metaphors, and effective visual aids for the often non-technical members of court.

According to Kolflaath stories in court could be seen as giving meaning and context to the evidence, and due to this the question of evidential value would in all aspects be to find which role the evidence could play in the story (25, p.518). The story-telling could however present challenges. Due to the nature of the story-telling format, with the feeling of the pieces falling into place, evidence could easily be given wrong value if the evidence evaluator sees connection where there only is concurrence (25 p.522, ).

Casey debates that concerns about the validity and reliability of forensic results are motivating formalization on how evidence is evaluated and presented. Many DFDs are confused of the expectations that they should evaluate digital evidence and express conclusions on terms of the probability of the evidence, which would inflict on the role of the prosecutor. The DFD should be mindful when presenting the facts of a forensic result to the prosecutor, so that the presentation do not support or refute a specific point of view. It would be to the role of the prosecutor to combine the forensic result and the evaluation the legal probability. Some argue for the use of models and studies to decide the probability issue. However, these models base themselves again on assumptions the outcome would be dependent on, by this reflecting the beliefs of the developers of the model. There will always be human judgment and subjectivity involved in results (33).

Digital evidence artefacts are in large created by software and hardware constantly under development. The same will apply for the forensic tools that are used to analyse the digital evidence. This factum would require careful presentation of the results of a digital forensic investigation, so that the prosecutor is left with the probability evidence evaluation.

## 2.3 The prosecutor qualifications and quality

### 2.3.1 Competence

The basic competency level of the Norwegian prosecutor consists of a Master of Laws degree, and the obligatory 105 hours of start-up course delivered by the Norwegian Police University College (7, 8).

None of these study plans include training or basic knowledge on digital evidence, which is somewhat odd with regards to the fact that the mistakes in digital investigations are getting more attention and raising criminal justice concerns (34).

Barbara Endicott-Popovsky and retired Superior Court Judge Donald J Horowitz discuss the unintended consequences of digital evidence for the US legal system. They emphasize the problem of the literacy of both lawyers and prosecutors regarding digital evidence, and that law schools do not address digital evidence, yet digital evidence is a part almost every crime. They stated that:

“Without an institutionalized understanding of the nature and use of digital evidence, we seriously risk a justice system increasingly subject to confusion and inaccuracy, with innocent individuals wrongly convicted and incarcerated, suffering additional collateral penalties and damage for the rest of their lives.”

They present an awareness program to counter the digital literacy of the judiciary, which include a workshop in collaboration with FBI, a televised lecture series, and a digital forensics course for law and computer science students (17).

Smith and Kenneally debates the ramifications of the “*electrification of evidence*” and stated that IT experts are increasingly needed to understand and interpret the nature

and significance of evidence, and that properly judicially arguing and evaluating digital automated events will be dependent on how well the IT expert are able to reliability principles to the facts of criminal case (26), and that recognizing this fact would mean that IT experts need to be recruited into juries. They further debate the legal confusion surrounding digital evidence and the standards around digital evidence reliability, and the need for a just legal framework regarding the trustworthiness of digital artefacts.

"The conservative nature of the justice system has attempted to apply the traditional physical-world concepts and principles of proof to digital evidence".

If the Norwegian justice system having discarded their use of a jury system takes this development into serious consideration, the competence of the members of court needs to be revised. If not, the technical IT expert without any law degree could in all aspects be the one deciding the outcome of criminal cases and law disputes in the future.

Casey states that evidence evaluation requires higher levels of knowledge specialization and quality oversight. Casey further cites ACPO 2012 (15) and present an example of evidence evaluation of digital evidence where "*the presence of indecent images of children on a computer would not in itself be sufficient evidence of possession, as the possessor must be aware of the images.*" To establish likelihood or intent, evaluating other digital evidence artefacts would be needed (35). Casey underlines the need for distinguishing between technical processes and evidence evaluation to avoid challenges with unqualified personnel evaluating digital evidence, and that these challenges could include incorrect conclusions.

Casey argues that keeping up with the advances in technology will open up for a more academic approach to criminal investigations, and that cooperation between law enforcement and academia would be beneficial for all parties involved (36).

Due to the complexity of the challenge with digital evidence reliability and quality, best practice guides are developed, implemented and maintained (37).

Such best practice guides could also be implemented for the prosecutor with regards to digital evidence. The US justice department issued already in 2007 a guide for prosecutors called "*Digital evidence in the courtroom*" (38). In this guide they list facts and explain concepts in simple terms and state the need for this due to the:

"adoption of new technology often outpaces society`s development of a shared ethic governing its use and the ability of legal systems to deal with it."

The guide also covers the need for the prosecutor to show in court the persuasive value of digital evidence by ensuring that the integrity of the digital evidence is upheld. The guide also lists some need-to-know facts the prosecutor must be familiar with, such as chain-of-custody, laboratory policies and procedures, and rules and principles for digital evidence generally in all stages of the investigation.

In 2017 an analysis report on the Norwegian prosecution was released, the prosecution analysis (4). The prosecution analysis comments on the competence of the police prosecutor and points out that the prosecutor competence level in general had too many inconsistencies, and that increased competence on investigative processes was a necessity (4, p.172). In the question of the prosecutor having the right competence, the report concluded that an increase of the competence on investigative steps and processes was needed, and that a systematic approach to this would be the best

solution. The report advocates for a strategic, systematic and obligatory build up of the prosecutor competence (4, p.196).

The prosecution analysis also comments on the lack of post graduate studies at the Norwegian Police University College specifically designed for the prosecutor, and that a positive change in the adaptation for and prioritization of competence in the police districts possible would be needed (4, p.200).

The competence of the police prosecutor should also be seen in the light of the quality reform the Norwegian police service is undergoing, where the specialization are increasing. The need for increased specialization and combined with increased a competence level within the prosecution, for instance on digital policing, could be argued for. Investing in the prosecutor competence would result in better abilities on identifying and mitigating errors of justice.

### 2.3.2 Quality

The attorney general has stated that the prosecutor has a specific responsibility to defend the rule of law and its basic principles. He has also set some overall objectives for the criminal investigation which are; high quality, high clearance rate, short processing time, and adequate reaction (39) Some specific comments to the evidential requirements and the evidence evaluation are also presented. The comments involve statements of which level the evidential requirements should be set for criminal cases. The attorney general specifies that the prosecution will need to be convinced of the guilt of the defendant to issue an indictment, which implies that the same strict level of evidential requirement and evidence evaluation as the courts should be met also by the prosecutor (39, p.15).

Tor-Geir Myhrer has written a report with regards to the role and responsibilities of the police prosecutor. Myhrer defines quality as (6, p.14);

“An activity which is conducted according to certain standards.”

Myhrer states something interesting in the scope of this thesis, that the main challenge with quality is not to define it, but to measure it. He discusses the challenge of weighing the different quality objectives from the attorney general against each other, when there is not issued any guidance to how this should be done.

In this thesis, quality will point to the technical quality of digital evidence, in the sense of the level of technical *correctness*, meaning there are no technical facets influencing the digital evidence and the digital evidence can by this be trusted to be correct and to represent the truth.

The thesis do not address the judicial quality objectives as a whole, and the technical quality of digital evidence as described here would mainly be a underlying part of the high quality objective of the attorney general in the sense of digital evidence quality.

### 2.3.3 Errors of justice

Errors of justice can be defined as (40, p.4);

"Any departure from an optimal outcome of justice for a criminal case"

In the technical context of this thesis this definition is a bit wide, and would also cover other aspects beyond the scope of this thesis.

Forst also state that due process errors fall into the category of errors of justice (40, p.17), or as Rachlew points out; if a police officer due to lack of knowledge produces unreliable evidence unintentionally it shall be treated as a systemic error of justice (3, p.4).

The systemic error of justice as described by Forst and Rachlew fits the problem of this thesis, and will be the description used.

Rachlew states in his doctoral thesis that errors of justice not only relate to the end result of a criminal investigation, but also the processual decisions made of the prosecutors in judiciary chain the criminal case, which is some of problem this thesis seeks to gain insight into (3, p.5).

If the potential literacy of the prosecutor regarding digital evidence resulted in poorly evaluated digital evidence and an error of justice, the prosecutor would most likely not identify the error. This is what Rachlew calls one of the insidious traits of the error of justice. In spite of the error, the end result could for the prosecutor feel correct and s/he could even get credibility for the result (3, p.5). This could help feed the belief of correctness, further prolonging errors of justice possible leading to threats to the rule of law.

To avoid errors of justice, one would need to identify these errors. To identify errors in the digital evidence evaluation would require knowledge and competence on digital evidence, which in itself should be basis enough for the prosecutor and the judiciary to seek this knowledge.

Rachlew states that an open and democratic police service would regulate and correct the most obvious errors of justice internally. This thesis comply by Rachlew`s way of thinking, focusing on potential errors of justice due to erroneous evidence evaluation (3, p.33).

# 3 Method

## 3.1 Introduction

In this chapter the framework, methodology, procedures, and quality of the research will be presented and accounted for.

The thesis is a continuation of my preliminary study (1).

## 3.2 Research Methodology

The focus of this study is to gain insight into the black-box process where the prosecutor evaluates and weighs digital evidence, and if lack of competence on digital evidence potentially may introduce fallacies into this process. This specific process has been little-studied, and it is also a somewhat multilayered complex process.

To be able to do this a qualitative methodology was chosen, in the form of a collective case study approach. A case study, or ideographic research, can be particularly suitable when looking into a poorly understood situation, and uses observations, interviews and for instance written documents (41, p.271-72).

## 3.3 Research Procedure

To be able to answer the supportive research questions and to test the hypothesis, I needed to simulate a situation where the prosecutor is presented digital evidence, and where the digital evidence was evaluated and weighed.

### 3.3.1 Sampling

To be able to answer my research problem, I needed prosecutors from the Norwegian police service. The prosecutor has a specific function and educational basis, and the numbers of prosecutors in the Norwegian police service are limited. The prosecutors are also a group of people with very busy work schedules, which made the process of participant collection quite work demanding.

I interviewed 14 police prosecutors in this study, where of all work in a police district in the Norwegian police service. A representative sample in a qualitative study would be one that is presumed to represent a population (41, p.279). By interviewing 14 police prosecutors in 2 different police districts in different parts of Norway, police districts of different size, and in 4 different cities, I felt this sample could be representative for the prosecutor in the Norwegian police service.

When choosing participants for the study, I decided to focus on 2 different police districts. I reached out to the leadership in those police districts and got written permission to contact their prosecutor departments. The prosecutor departments helped me spread the information letter describing the study to the prosecutors, and at the same time gave permission to the prosecutors to spend time participating in the study. Due to the busy schedules of the prosecutors, I was advised through the leadership of the prosecutor departments to contact each prosecutor personally. I then contacted the

prosecutors to present the study, and to ask if they were interested in participating, ask for consent, and make an appointment for the interview.

This process turned out to be time consuming, due to the special nature of the process I was to study, see section 3.3.2.

When informed of the focus of the study, the leadership in one of the police districts I contacted informed me of prosecutors which in addition to the Master of Law degree had taken post graduate studies in digital forensics at the Norwegian Police University College. I also contacted these and was able to get 2 prosecutors with post graduate studies in digital forensics to participate in the study. These would represent the non-typical prosecutor, and in this sense outliers in the participant sample.

### 3.3.2 Data collection

The data collection was planned and set up as a semi-structured personal interview (41, p.160), which made me able to ask follow-up questions. This was of great importance due to the focus of the study, where collecting the participants reasoning was crucial.

This way of structuring the data collection was also very helpful due to the complexity of the different scenarios, which made me able to make sure every participant understood the scenarios they were to evaluate when they were presented to the participants.

There were also some ethical considerations that needed attention. Evidence evaluation is a situation where the prosecutor not only employs his or her professional experience and education, but also common sense. This makes the nature of the evaluation process personal and almost a bit private. Being invited into and taking part of such a process could open up for the participants feeling vulnerable, especially taking into consideration that the participants were put in a situation where they might feel measured. The prosecutors are also a highly educated group, which hold a high status within the police service. This could potentially introduce a fear of loss of status on the participants' behalf, if the interviews and the data were not properly managed.

The somewhat private nature of the evidence evaluation resulted in the need for approaching the participants with care, both during the sampling procedure, during the interviews, and with regards to protecting their professional careers by ensuring no personal data would be registered.

Due to this, I quickly discarded using video or recordings during the interviews, and also discarded registering any personal information at all, including which police district the participants worked in. This forced me to set up the interviews and the scenarios so that I would be able to collect the data I was interested in collecting, without having to both register personal data of any sort or record any part of the interviews, including names.

I therefore chose to create a scenario question form including the post scenario interview questions where I could note their answers as the participants was asked the different scenario and interview questions, and where the participants would give their consent by ticking a box on the front of the form. In addition to this, I created an interview guide and an informed consent form, which all participants were handed a copy of before giving their consent.

After the interviews, the notes were then transcribed by computer into a digital scenario question form and given a number, further enhancing the protection of the participants' privacy.



When all of the interviews were finished and transcribed into digital scenario question forms, I was ready for the data analysis.

### 3.3.3 Data analysis

To be able to analyse the data correctly in accordance with the context the data was collected, I divided the data into the following categories:

- Scenario 1
- Scenario 2
- Scenario 3
- Quality and competence

These categories were further broken down into sections and subsections, depending on the level identification of digital evidence by the participants during the scenarios, the level of reasoning of the participants, and the scenario context.

When defining the measurement strategy of the study, I chose a solution where the participants were instructed to either assign a low or a high evidential value to the digital evidence artefacts when evaluating them. The evidential values given in the scenarios by the participants were then counted, converted into percentage for the whole sample, and organized into the section where they belonged in the context of the scenarios or post scenario questions.

The reasoning of the participants for choosing the different evidential values were divided into low or high, and organized into sections representing the specific evidential value for the specific piece of digital evidence artefact.

When all the participants gave the same reasoning for choosing evidential values, the term "all" were used. When there were more than 50 % of the participants agreeing on something, the term "majority" were used. If there were more than one, but fewer than 50 %, the term "several" was used. If fewer than 50 % of the participants agreeing on something, the term "some" or "minority" were used. If only one participant stated something, the term "one" or "one of" were used.

### 3.3.4 Creating criminal case scenarios

The specifics of the different criminal case scenarios including the inserted digital evidence artefacts will be accounted for in the chapter sections 3.3.4.1, 3.3.4.2 and 3.3.4.3.

In chapter section 3.3.4.4 the post interview question will be accounted for.

A presentation of the general layout will be presented here.

The prosecutor mainly relates to legal documents produced during the criminal investigation. The prosecutor reads the legal documents of the criminal case and evaluates the evidence as they are presented in for instance police reports or police statements. The prosecutor then decides if the suspect should be indicted, and of which crimes the indictment should consist of, all depending on if the evidence support or refute the suspicion.

To be able to gain the necessary insight into the black-box process of evidence evaluation, I needed to create a situation where I controlled the context and the contents of the evidence evaluation. It would then be possible to gain insight into the cause-and-

effect relationship of the various technical evidence qualities and the evidence evaluation results. By manipulating the independent variable being the scenario details with the digital evidence artifacts, evidence evaluation being the dependent variable. This would also increase the internal validity of the study, having regulated environmental conditions of the situation (41, p.104).

To simulate such a process of controlled context evidence evaluation, I chose to create 3 different criminal case scenarios, representing both different criminal case types and different evidence evaluation situations. This would also increase the internal validity of the study by collecting multiple sources of data, *triangulation* (41, p.104).

The reason for choosing 3 different criminal case scenarios and evidence evaluation situations was to possibly gain insight on if there were any identified difference in the evidence evaluation between the case types and situations, and to get more true data due to a broader collection base to avoid one-sided data collection. I therefore put my years of experience from the Norwegian police service and technical forensic background to good use and created 3 fictive complex criminal case scenarios including interconnecting background information as police statements from witnesses and suspects, and technical reports and police reports presenting different digital evidence artefacts of various technical and judicial evidential qualities. All of the criminal case background information and different digital evidence were made to interconnect with each other, by this simulating natural real-life situation for the prosecutor, and relating the different digital evidence to evidential value.

The chosen scenario criminal case types consist of a traffic accident case, a criminal case concerning possession of sexualized child abuse images and sexualized chat with minors, and a 16-year old girl victim of weekly sexual abuse who is planning to commit suicide. The reasons behind choosing these criminal case types and evidence evaluation situations were not random and will be accounted for in the chapter sections describing each criminal case scenario.

The format and quality of the different police reports were not randomly chosen, nor will the titles and function of the persons writing them, and this be accounted for in the chapter sections describing each criminal case scenario.

The simulation of the evidence evaluation situation also needed to be felt as natural as possible for the prosecutor to avoid collection data not accurately describing what I wanted to gain insight into. I therefore chose to interview the participants in their normal workspace, by this deviating as little as possible from the participants naturally environment.

In a criminal investigation, the evidential value of digital evidence could be constantly changing as the investigation moves forward, and new evidence was discovered. The evidential value of evidence could for instance depend on if the other collected evidence supported or refuted the evidence in question.

To be able to simulate a situation where the digital evidence had a perceived constant evidential value, I chose in scenario 1 and 2 to simulate the situation where the prosecutor is presented a criminal case that was ready to be processed to the court, which normally would mean that no new evidence would be introduced in the criminal case at that point. In such a judicial situation the evidential value on the digital evidence would be perceived as a constant factor by the participants, by this mitigating any

misunderstandings on the evidential value that could affect the outcome of the case study and the quality of the data.

Evaluation of evidential value can be differentiated on many levels due to the degree of common sense involved in the evaluation. To be able to record evidential values which would be possible to work with, I chose to record either a high or a low evidential value. The participants were therefore told to either assign a low or a high evidential value to the digital evidence artefacts when evaluating them.

A low evidential value would simulate a low technical quality, and vice versa.

A high evidential value would simulate a high technical quality, and vice versa.

The specific digital evidence artefacts for each scenario will be accounted for in the scenario chapter sections.

### **3.3.4.1 Scenario 1**

Scenario 1 simulated a traffic accident case. This criminal case type was chosen due to the normalness of the crime, and because this is a case type the prosecutor normally do not spend a lot of time to evaluate.

A summary of the scenario-plot; Traffic accident, car against pedestrian:

Tuesday the 2<sup>nd</sup> of April 2019 at 16:09 Marte Kirkemo drove to work in her elderly BMW. On her way through the small city of Lillevik, just passing the railway station, she hit Peder Ås with her car in the middle of a pedestrian crossing, resulting in both his legs being broken. Marte Lillevik instantly stopped her car and called the Emergency services 113.

The police officers that were sent to the scene of the accident collected 4 pieces of digital evidence, both directly from the scene of the accident and through investigating the accident. The different pieces of digital evidence were; the suspect's mobile phone, from which a table from an automated mobile phone analysis forensic tool showing a timeline of the most recent phone activity was included in the police report, call records collected from the service provider of the suspect's mobile phone, CCTV video footage showing the actual accident, and a manual on-the-scene analysis of the GPS in the suspect's car. There was also background information given on the weather and road conditions, witness statements connecting Marte Lillevik to rumors of drive while being active on Snapchat, and the suspect statement where Marte Lillevik claimed to not to have been active on Snapchat on the time of accident.

The participants were then handed a police report presenting the digital evidence, the statements given to the police, and some background information on the weather and road conditions.

The participants were then asked to 1) identify digital evidence that would be of importance to the indictment, and 2) to evaluate and weigh the digital evidence, assigning the evidence either a low or a high evidential value, and to justify their answers.

The digital evidence introduced into this case was not randomly inserted.

**The 1<sup>st</sup> piece** of evidence was the timeline from the automated mobile phone analysis forensic tool, where the time phone activity up to Marte Lillevik's call to the Emergency services 113 at 16:09:58 was presented. The phone activity showed that Marte Lillevik had sent and received Snapchat messages in the 3-4 minutes leading up to the call to 113, the last Snapchat message being sent merely 10 seconds before the call to 113,

thus indicating that Marte Lillevik hit Peder Ås with her car because she was preoccupied with Snapchat while driving.

The reason for choosing this particular digital evidence artefact has mainly two reasons; firstly, my preliminary study, where the results indicated that automated mobile forensic tools without manual verification would lack evidential completeness, especially application data like this (1). Secondly, my own experiences, where I have had just this piece of evidence and situation in one of my own criminal cases. Without manual verification and database examination, there would be no way to say how the database register the timestamp of message sent, or if this data is correct.

In my casework, the database examination showed that the last active action from the user of the mobile phone was several minutes before the accident, not 10 seconds, and that the Snapchat messages in question were delayed due to reasons unknown, and left the system at the registered timestamp, possibly due to bad cell tower coverage.

Due to the lack of information about any manual verification, and the fact that the analysis was done by an automated mobile phone analysis forensic tool, and reviewed by a non-technical police officer, the evidential value and technical quality assigned to this evidence was therefore set to low.

The digital evidence artefact was inserted into the scenario to see if the participants would question the automated analysis or the lack of competence of the police officer, thus indicating a lack of knowledge and competence on the basic digital forensic principle of tool and evidence verification.

When choosing the traffic accident approach, insight of how the participants would evaluate evidence on a case type which is rarely investigated in depth and a case type of which there are a lot of, could be gained. This is also a case type where the DFDs seldom are involved, so it would be natural for the participants that the normal non-technical police officer presented the digital evidence in a normal police report. It is also a case type where automation would be likely used to a larger extent, due to the inaccessibility of DFDs.

**The 2<sup>nd</sup> piece** of inserted digital evidence was call records obtained through the telecom service provider of the suspect. The call records were obtained by the fictive police officer to verify the time of the call to 113, and thereby the date and time settings on the suspect's mobile phone. This would also further verify that the time between sent and received Snapchat messages and the call to 113 was correct, by this obfuscating the incorrectness of the Snapchat registered timestamps of messages sent. A time skew of 12 seconds was inserted into the call records, to complicate the verification of the time settings for the participants, even though this would not have any impact on the digital evidence artefact. The call record artefact would however be considered having a high evidential level and technical quality in itself, but the main reason for inserting the artefact was to support the perceived correctness of the phone activity, and to see if the participants gave this digital evidence artifact a high evidential value and how they reacted to the 12-second time skew.

By introducing the call record artefact, there would be possible to see if the participants questioned the time skew, thus indicating a lack of knowledge and competence on basic digital forensics.

**The 3<sup>rd</sup> piece** of inserted digital evidence artefact was the CCTV footage showing the accident. This artefact was inserted to increase the number of artefacts, and to see if any of the participants questioned the collection or quality of the footage, by this potentially indicating a lack in the forensic principle of a documented audit trail. The artefact was also inserted to strengthen confirmation bias, due to the footage showing that Marte Lillevik did not brake or try any evasive maneuvers before hitting Peder Ås in the pedestrian crossing. This would further support the notion of Marte Lillevik being preoccupied with her phone while driving. The evidence was given a high evidential value due to the video being correct and not changed in any way.

**The 4<sup>th</sup> piece** of inserted digital evidence artefact in the scenario was a GPS unit found in the elderly BMW Marte Lillevik was driving. This GPS unit was manually analyzed on the scene by the police officer that wrote the report, and the police officer could read out of the GPS unit that the car had an average speed of 46 km/t during the last drive. This artefact was inserted to increase the number of artifacts, and to see if any of the participants questioned the not forensically sound manual analysis, or the lack of competence of the police officer, by this indicating a lack in knowledge and competence on basic digital forensics principles. This artefact was given a low technical value, due to the incorrect analysis, lack of documentation, and lack of competence of the police officer.

I chose to introduce the normal police report format commonly used when writing up reports, a format that are describing and easy-to-read. This report format fits into the criminal case type chosen for scenario 1 and would be the format the prosecutor would expect to see evidence presented in within such a criminal case.

The fictive police officer who in the scenario wrote the report worked as a patrol-officer at a small-town police office, by this simulating the non-technical police officer. This can be read from the signature of the police report. Nor the report, or the title / function of this police officer, indicated in any way digital forensics knowledge or an official skillset on performing digital forensic analysis, yet the police officer states in his report that he did.

By implementing this factor, there would be possible to see if the participants questioned the competence of the police officer regarding performing a forensic analysis, or the digital evidence the police officer presented through the not verified automated analysis.

### **3.3.4.2 Scenario 2**

Scenario 2 simulated a criminal case concerning possession of sexualized child abuse images and sexualized chat with minors. The case type was chosen because this is one the most common case types concerning digital evidence, and it would be easy to implement more technical artefacts of a broader base than in scenario 1 and 3. This was also the most complicated of the 3 scenarios.

When choosing this criminal case approach, insight of how the participants would evaluate evidence on a case type which is typically investigated in some depth could be gained. This is also a case type where the DFDs often are involved, so it would be natural for the participants that the DFD presented the digital evidence in a technical police report.

Summary of the scenario-plot; possession of sexualized child abuse images and sexualized chat with minors:

During a investigation of serious sexually abuse criminal case in early 2018, the Norwegian national criminal investigation service (NCIS) identified a Skype chat log on the suspect's computer. Identification through following IP addresses, the NCIS were able to identify several other chat participants who were involved in sexualized chat with minors. The NCIS opened investigations on all identified chat participants. One of these participants, Peder Ås, lives in your police district, and the NCIS therefore sent over the criminal case against Peder Ås to your police district.

Peder Ås was earlier convicted of participating in sexualized chat with minors som years back.

Peder Ås was arrested and interrogated just after the criminal case was received from the NCIS in 2018, and the mobile phone and computer belonging to Peder were seized and forensically imaged.

Due to case backlogs the criminal investigation against Peder Ås has been untouched since the arrest, now 1 year later. During this period of time, the criminal case has gotten a new investigative leader and prosecutor. In a clear-all-old-cases event in the following year, the prosecution of the case has been handed over to you. The criminal investigation against Peder Ås was prioritized, and the image files from the computer and mobile phone analyzed.

The participants are then handed a technical police report presenting the digital evidence, a report presenting a representative choosing of the illegal images found, the statements given to the police, and some background information on Peder Ås.

I chose to introduce the technical police report format commonly used when writing up DFD reports (), a format that list a lot of technical information and could be difficult to read. This report format fits into the criminal case type chosen for scenario 2 and would be the format the prosecutor would expect to see evidence presented in within such a criminal case.

The suspect claimed to be innocent, and when confronted with the police finding 1504 illegal images on the mobile phone, computer, and browser history, the suspect explained that he had not any such images, and if there were any, he would have to be a victim of a computer virus or hacking. If there were any illegal images on the mobile phone, then somebody must have possibly sent them to him on Snapchat, Kik, or Messenger chat. But if this was the case, then he would have deleted such pictures immediatly. So, there could not be any illegal images on neither the mobile phone nor the computer.

The participants were then asked to 1) identify digital evidence that would be of importance to the indictment, and 2) to evaluate and weigh the digital evidence, assigning the evidence either a low or a high evidential value, and to justify their answers.

The digital evidence artefacts introduced into this case was not randomly inserted.

**The 1<sup>st</sup> piece** of digital evidence to be inserted was the mismatching checksum of the image file of the suspect's computer. To ensure the integrity of digital evidence, checksums of the original evidence and the image file are computed, and then matched. If there is a mismatch, the integrity of the image file would then be compromised. In this case this checksum did not match the original evidence, hence this artefact would be of great importance. Not discovering this artefact would mean that the criminal case against Peder Ås would be based on evidence which could not be connected to the original

evidence, while it really should be dismissed. The checksum could be given both a high and a low evidential value; the deciding factor of success will be based on the participants' justification for choosing so. They may choose a low value because the artefact has a low technical quality or high because it is important to uncover this error. Either way, it would be the identification of the artefact and the reasoning who determines if the participants understand this artefact.

The mismatching checksum artefact was introduced to see if the participants had knowledge and competence on digital evidence integrity principles and chosen because it always will be an important factor in all criminal cases which includes digital evidence.

**The 2<sup>nd</sup> piece** of digital evidence inserted was the browser history of the suspect's computer. The browser history was exported out of the image file with an automated forensic tool. In the browser history 1500 visits to web pages containing images of sexually abused children was found.

No information on where the browser history was located on the suspect's computer was included into the technical report. This lack of information was inserted because the location would be of importance when deciding the evidential value of the artifact. For instance, from which user and browser type was the browser history extracted from, by this indicating that the browser history could in theory belong to another user than the suspect. As the browser history stand alone without supporting information, it would have a low evidential value.

By introducing the browser history, there would be possible to see if the participants questioned the lack of information connecting the browser history to the suspect, thus indicating a lack of knowledge and competence on the basic digital forensic principle of a documented audit trail and browser forensics and internet caching.

**The 3<sup>rd</sup> piece** of digital evidence artefact inserted into the scenario was the Skype chat log coinciding with the same chat log the NCIS cases were build upon. Information in the technical report stated that the NCIS had correctly identified Peder as one of the chat participants through IP searches and obtaining user / subscriber information from Skype. The chat log in itself was considered having a high evidential value due to the correctness of the NCIS identification. This artefact was introduced to complete the scenario picture, and to connect Peder to the sexualized chat, by this introducing confirmation bias as to Peder also being guilty of possessing illegal images.

**The 4<sup>th</sup> piece** of digital evidence artefact inserted into the scenario was the mail address of Peder Ås connected to the Skype chat. This artifact was introduced to complete the scenario picture, and to connect Peder to the sexualized chat, by this introducing confirmation bias as to Peder also being guilty of possessing illegal images. The mail address was considered having a high evidential value due to the correctness of the NCIS identification. Not identifying the mail address, would indicate a lack of knowledge and competence of the basic digital evidence value chain, connecting Peder to the NCIS case chat log.

**The 5<sup>th</sup> piece** of digital evidence artefact inserted into the scenario was the negative search result on the suspect's mobile phone regarding Messenger chat. Peder stated that if there were any illegal images found on his mobile phone then somebody must have possibly sent them to him through one of the applications Snapchat, Kik, or Messenger chat. But if this was the case, then he would have deleted such pictures immediately. So, there could not be any illegal images on neither the mobile phone. The automated

analysis of the mobile phone could not find any Messenger chat. Remnants of Kik and Snapchat were found, but no traces of any illegal activity on neither of these 2 applications could be found on the suspect's mobile phone.

The reasons for introducing this artefact were that my preliminary study result indicated that automated mobile forensic tools without manual verification would lack evidential completeness, especially application data like Messenger (1). Without manual verification and database examination, there would be no way to say if Messenger chat resides on the mobile phone or not. Secondly, the widespread popularity of the Messenger chat application, which indicates the probability of encountering this artefact in real-life situations. There was also the reason of connecting the information in the scenario, due to the file path of the illegal images found on the mobile phone, which indicated that the images had a connection to Facebook. The artefact would by this obfuscate the correctness of the illegal images found on the suspect's mobile phone. This will be accounted for in the section for the illegal images evidence.

By introducing the missing Messenger chat artefact, there would be possible to see if the participants questioned the result of the automated mobile phone analysis, thus if not, indicating a lack of knowledge and competence on the basic digital forensic principle of tool and evidence verification. The digital evidence artefact was assigned to a low evidential value, due to the fact there had been no verification of the automated analysis. This indicating that there might be Messenger chat on the mobile phone, and that the statement given by the suspect could be correct.

**The 6<sup>th</sup> piece** of digital evidence artefact inserted into the scenario was the illegal images found. The technical report presented 1504 illegal images found.

The scenario evidence and information build up and indicate that none of these illegal images contradicts the suspect statement, and that the suspect therefore could be innocent regarding this part of the crime.

2 images were found on the suspect's mobile phone, 2 images on the suspect's computer, and 1500 images from what the technical report described as the browser history. A representative selection of 16 images was presented in an illegal image report, including the file paths of the images. The images were legal pictures, taken by me, and inserted "Illegal image" into the picture.

Firstly, the mobile phone images. The technical report describes them as being found, and then lists the file path to their location on the image file, but the file path is not explained. The file path presented points to a cache for Facebook images, by this indicating that there would be Facebook or Messenger on the suspect's mobile phone. The fact that the images reside in a cache, would also indicate that the images as they are presented in the technical report very well could have been sent to the suspect's mobile phone, as he states in his police statement, and by this coincide with the suspect statement (1).

By introducing the mobile phone images artefact, there would be possible to see if the participants questioned the location of where the images were found or recognizing that the technical quality of the artefact was low due to the fact the illegal images resided in a cache. Not acknowledging this fact indicates a lack of knowledge and competence on basic digital evidence and forensics.



Due to this, the digital evidence artefact was assigned to a low evidential value and a low technical quality.

Secondly, the 2 illegal images from the suspect's computer. The technical report describes them as being found, and then only lists the file path, without any further information. As with the 2 illegal images found on the suspect's computer, these are located in a cache connected to a Firefox browser, and it will not be possible to state if the suspect has had any active participation in the illegal images residing in the cache.

By introducing the computer images artefact, there would be possible to see if the participants questioned the location of where the images were found or recognizing that the technical quality of the artefact was low due to the fact the illegal images resided in a cache. Not acknowledging this fact indicates a lack of knowledge and competence on basic digital evidence and digital forensics. Due to this, this artefact was assigned a low evidential value and a low technical quality.

The 1500 illegal images from the browser history were described in the technical report as being collected from the browser history. The report stated that the browser history showed 1500 web pages that pointed to child abuse material. The browser history was exported out from the suspect's computer using a forensic tool, and then transferred over to a new installation of Linux, with an anonymous internet connection. The investigative detective and the DFD then continued to go through all the browser history, going online one web page at a time, clicking on the links in the browser history, and documenting the child abuse material by taking screenshots of the illegal images. The information about Linux and anonymous internet connection was inserted to obfuscate the obvious incorrect way of forensically acquire the images.

By introducing the 1500 illegal images from the browser history artefact, there would be possible to see if the participants questioned the location of the images and the process of how the images was acquired. If not, this would indicate a lack of knowledge and competence on basic digital forensic and evidence principles.

The artefact was assigned to a low evidential value and a low technical quality, due to the fact the illegal images resided on the internet and not the suspect's computer, and because there would be no way to state that the images were the same as when the browser history visits one year ago due the dynamics of the internet.

**The 7<sup>th</sup> piece** of digital evidence artefact inserted into the scenario was a negative anti-virus search.

The technical report stated that an anti-virus search had routinely been performed on the suspect's computer when it was imaged at the time of the arrest one year ago. The technical report further stated that the search came out negative, and that there were no signs of the computer being infected by a computer virus, or otherwise hacked. There was no information in the report on how this was performed, or which tool that was used. This indicating that there could be a computer virus on the computer and that another search should be performed as one year had passed since the last search. This could indicate that the suspect's statement was correct.

By introducing the negative anti-virus search artefact, there would be possible to see if the participants questioned the result of the anti-virus search, thus if not, indicating a lack of knowledge and competence on basic knowledge of digital forensics and malicious computer viruses. The anti-virus search artefact was assigned to a low evidential value

and a low technical quality, due to the fact the search had been performed one year ago, and only with one tool. Indicating that the statement given by the suspect could be correct.

### **3.3.4.3 Scenario 3**

Scenario 3 simulated a situation where the prosecutor is at home on off-hours prosecutor duty a late Friday night, and receives a phone call from the police Emergency Centre regarding a 16-year old girl, victim of weekly sexual abuse who is planning to commit suicide and the following need for the prosecutor to quickly issue a warrant or not.

Summary of the scenario-plot; Off-hours prosecutor duty:

Friday 12 of April 2019 at 22:00 the police Emergency Centre received a phone call from a chat moderator named Peder Ås employed at mayday-chat.no, a specialized anonymous chat service for kids that have been a victim of sexualized child abuse. The chat moderator explained that he Tuesday evening had been chatting with a girl claiming to be 16-year old, and the girl had written about being sexually abused by her father almost on a daily basis for 8 years. Due to this she had now thoughts about committing suicide. Before the chat ended, the chat moderator was able to get the girl to agree on that they where to continue the chat Friday evening. Friday evening at 21:05 the same girl came online again, and the chat continued. The girl explained that her father was on his way home, and that she knew she was going to be sexually abused this evening, because her father had been drinking, and the abuse always happened when he was drunk. The girl seemed extremely despaired and frightened. The girl stated that she was going to commit suicide later that evening, and then the girl abruptly ended the chat session.

Being a chat moderator, Peder Ås has access to the IP addresses of the person he is chatting with. Peder noted the IP address, and quickly got online and performed an IP address search. The results of the search showed that the IP address pointed to a physical address in the town of Lillevik.

The chat moderator called the police Emergency Centre and was connected to the police Emergency Centre in Lillevik. Peder explained the situation to the operator and sent over screenshots of the chat together with the information about the IP address, and where the IP address pointed to in Lillevik through a screenshot of a map of an online IP GEO search. With this information together with searches in the Norwegian population register, the operator at the police Emergency Centre managed to pinpoint a physical street address, and identify the persons living at the street address. On the pinpointed street address, there were registered 2 persons. A 15-year old girl and her 45-year old father.

Due to the immediate risk to life and health, it was considered to be of great importance to perform an immediate search and arrest on the premises of the pinpointed street address. The leader of the police Emergency Centre called the off-hours prosecutor to present the case, and to get the prosecutor to issue a search warrant to avoid suicide and sexual abuse.

The participants were then asked if they 1) would issue a warrant, and 2) justify their answer.

In this scenario, I chose a different approach, where increased time pressure was introduced into the evaluation process. The specific situation and case type were chosen because it would introduce a rather significant time pressure into the evidence evaluation. It was also a format of evidence evaluation the participants would recognize and that was known to them, by this strengthening the correctness of the situation and the data I wanted to collect, mitigating the participants treating the case study scenario as a test.

The fictive chat moderator who in the scenario performed the IP search worked at a chat service, by this simulating the 3<sup>rd</sup> party introducing digital evidence to a criminal investigation. This was inserted to see if the participants questioned and verified 3<sup>rd</sup> party information. In the scenario information the participants were handed, there was no information indicating that the police Emergency operator in any way had digital forensics knowledge or an official skillset on performing and evaluating IP address lookups.

By implementing this factor, there would be possible to see if the participants questioned the competence of the police Emergency operator regarding performing and evaluating IP address lookups, or the technical quality of the performed IP search.

The lack of technical quality of the IP search in this scenario opened up for error. The chat moderator had access to the IP address of the girl in question, but the IP GEO search he performed together with the police Emergency Centre to locate the actual physical location of the user of the IP address, was not forensically sound or correct.

The digital evidence artefact IP GEO search was inserted to obfuscate the IP address lookup and IP address identification. It would then be possible to see if the participants questioned the process of the IP search and identification, or recognized it as being technically wrong.

The reason for choosing this specific artefact and situation have 2 reasons, 1) I have experienced the situation and the mix-up of an IP GEO search can happen to prosecutors, and because identification of IP addresses is one of the most common digital evidence artefacts.

The only way to establish the correct connection would require a user / subscriber request to the internet service provider (ISP) who runs the IP address in question, and this would by law have to be initialized by the police. The actual physical location of the user of the IP address in the scenario would therefore be wrong, indicating that no warrant should be issued.

#### **3.3.4.4 Post scenario questions**

To gain a better and deeper understanding of the results of the study, and to increase the triangulation, post scenario interviews were also conducted.

The main focus of this part of the study was to gain insight into how the participants themselves were evaluating digital evidence and competence.

The questions were therefore concentrated around the participants own experiences on digital evidence evaluation, their approach to the evaluation process, and the competence they possessed.

#### **3.3.5 Quality**

I was particularly aware of the *Hawthorne effect* (41, p.104) during my interviews. This is described as the reactivity effect of the participants changing their behaviour due to the research situation, and by this increasing their attention and performing better than normally in a real-life situation resulting in the data collected being

This study being a case study where the participants were presented scenarios they were to solve, the possibility for the participants treating the scenarios as a test were absolutely present. To counter this effect I implemented a situation where I controlled

the context and the contents of the evidence evaluation. This would increase the internal validity of the study (41, p.104).

To simulate such a process of controlled context evidence evaluation, I chose to create 3 different criminal case scenarios and post scenario questions, representing both different criminal case types, different evidence evaluation situations, and the participants own assessment of their methods of choice when evaluation digital evidence. This would increase the internal validity of the study by collecting multiple sources of data, also called *triangulation* (41, p.104).

By creating detailed scenarios set up with police reports and witness statements, similar to the normal criminal cases the participants normally evaluate, I created a close to real-life setting as possible, by this increasing the reliability of the study (41, p.278).

I also chose do the interviews in the participants' normal work space deviate as little as possible from the real-life setting of the evidence evaluation. This increased the external validity of the study (41, p.105).

External validity was also addressed in the sampling procedure, where 14 police prosecutors were chosen as participants, and where of all work in 4 different cities in 2 different police districts in the Norwegian police service. A representative sample in a qualitative study would be one that is presumed to represent a population (41, p.279). By interviewing 14 police prosecutors in 2 different police districts in different parts of Norway, police districts of different size, and in 4 different cities, I felt this sample was representative for the prosecutor in the Norwegian police service (41, p.105). Two of the participants were also identified as outliers, due to their non-typical competence.

When addressing and acknowledging my own personal biases, I have worked in the Norwegian police service for several years, the majority of this period within cybercrime and digital forensics. This has without a doubt influenced me during the thesis work.

# 4 Data Analysis

## 4.1 Introduction

The chapter is organized according to the setup of the scenarios and the categories of the questions during the post scenario interviews.

In the scenario sections 1 (section 4.2) and 2 (section 4.3), the sections are organized into undersections which consists of the categories of digital evidence that were identified and evaluated by the participants in the scenarios, and general comments provided by the participants during the evidence evaluating process. To be able to measure the participants given evidential value of the digital evidence, the value of the evidence was scaled into having either a high or low evidential value. When the participants themselves stated that the evidence in question would have high or low evidential value, this was then recorded together with the reasoning behind their choice.

Scenario 3 (section 4.4) has no undersections but consist of the distribution of answers and the reasoning behind the answers, and general comments. In this section the general comments were not organized into an own undersection.

The post scenario interview questions (section 4.5) has no undersections and was titled *quality and competence*.

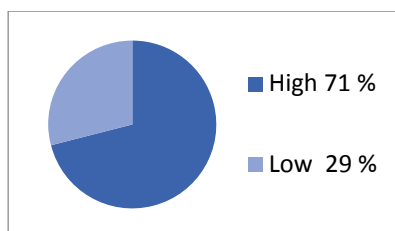
## 4.2 Scenario 1

All of the participants were able to identify the different digital evidence presented in the police report; the phone activity, call records obtained from the telecom provider, CCTV footage from the railway station, and a manual analysis of a GPS found in the car. All of the participants also meant that the digital evidence would be of importance in relation to the indictment.

When asked to evaluate and weigh the different digital evidence presented in the report, and giving their reasons for establishing evidential values, the participants gave the following answers:

### 4.2.1 The phone activity:

71 % of the participants gave this evidence a high evidential value, and 29 % gave a low evidential value.



**Figure 4.1: The phone activity**

The majority of the participants gave the evidence a high evidential value because they felt it had decisive importance in establishing negligence with regards to proving that the suspect had been actively using her phone while driving.

A few of the participants were confused about some of the irrelevant technical facts, like the 12-second time-skew between the phone and the obtained telecom call records, and if this would have an impact on how the Snapchat application recorded timestamps. The 12-second time-skew was also seen as normal, and of no consequence, by one of the participants.

Some of the participants needed further clarification on the level of active participation shown by the accused, and whether the phone activity was user or system generated.

One of the participants felt the technical information given in the report was *tech noise* and that s/he would have talked to a DFD before weighing the evidence.

The majority of the participants stated that they assumed everything were in order with the analysis.

It was also commented on the difficulty of arguing against such evidence by the defense attorney, and that it would be like trying to argue against a blood test analysis. The participant compared the use of an automated forensic tool with a forensic analysis; the level of uncertainty about the results would be at a minimum.

An absolute minority of the participants gave the evidence a low evidential value.

They questioned the entries from the timeline, and what such entries actually were proving. They needed more information on how the Snapchat application saved and registered data in the database application, and how the automated analysis tool parsed and interpreted these entries.

#### 4.2.2 Call records obtained from the telecom provider:

All the participants gave the obtained call records a high evidential value.

The reasons for giving this evidence a high evidential value were mainly that it would strengthen the total evidential picture, and that it would verify the time settings and time stamps of the phone activity. The call records were also seen as a way to verify if there had been any calls or text messages deleted from the phone, and by this strengthening or weakening the evidence.

One of the participants commented that the call records were also delivered by a trusted national 3<sup>rd</sup> party telecom provider, and that this gave the evidence increased credibility.

#### 4.2.3 The CCTV footage:

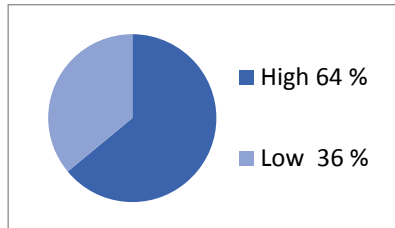
All of the participants gave the CCTV footage a high evidential value.

The reasoning behind this were that the footage would show negligence through the fact that no evasive action was taken from the driver, and that it would confirm other evidence in the criminal investigation, like the given statements and reports. A few of the participants also stated the video would show that the accident happened in the middle of the pedestrian crossing, and that the degree of negligence could easily be established due to this fact. Because the video showed that the victim entered the crossing from the left, thus should have been seen early. One of the participants also stated that the footage could be important for reconstructing the accident.

One of the participants questioned the technical quality of the footage, and the process behind the collection of the video.

#### 4.2.4 The manual analysis of the GPS:

69 % of the participants gave the manual analysis of the GPS unit in the car a high evidential value, while 31 % saw it as having a low evidential value.



**Figure 4.2: The manual analysis of the GPS**

Of the participants that gave the evidence a high evidential value, some mentioned that it confirmed the statement the accused had given, and that it was the only way to verify the speed of the car. One of the participants also pointed out that even if the average speed was not above 50 km/t, this could still be considered to be high due to the fact that the accident happened in a densely trafficked environment with a lot of braking, stopping and so on.

The participants that gave this evidence a low evidential value pointed out that it only would give an indication of the speed of the car, and that it did not prove anything.

These participants stated that this evidence was manually analysed, and that we could not know anything of the reliability of this GPS unit, or how it registered data.

#### 4.2.5 General Comments

Several of the participants emphasized that some of the evidence could be sown together, even if some single pieces of evidence had a low evidential value, and by this increase the evidential value in an overall evidence assessment.

The majority also commented on that the report format was easy to understand.

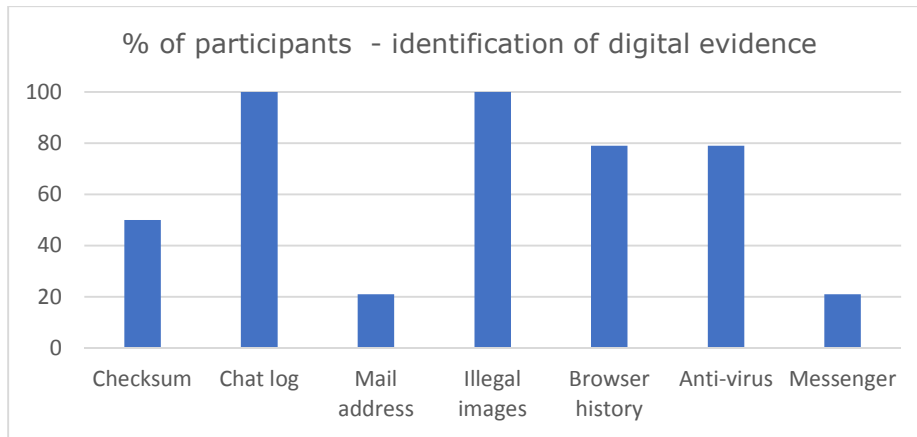
### 4.3 Scenario 2

In this scenario the participants were asked to identify different evidence from the technical police report that could be important in relation to the indictment, and in this scenario some of the participants did not identify all of the digital evidence.

All of the participants did however identify the illegal images and the chat log as important.

79 % identified the performed anti-virus search and the browser history, 50 % identified the mismatching checksum, and 21 % identified the mail address and the missing messenger chat application from the phone, as important.

See figure 4.3.



**Figure 4.3: The distribution of identification of digital evidence**

When the participants evaluated and weighed the different digital evidence presented in the report, the participants gave the answers as seen in table 4.1. The column on the right side of the table shows the percentage of the total of participants that identified the evidence in question. Further on, the two columns marked as low and high evidential value show the distribution between the participants giving the evidence a low or a high evidential value.

Out of the evidence that all the participants identified, the chat log and the illegal images, the only evidence that all the participants agreed on was the chat log. All of the participants gave this a high evidential value.

Type:	High evidential value:	Low evidential value:	% of the total of participants that identified the evidence:
Mismatching checksum	100 %	-	50 %
Chat log	100 %	-	100 %
Mail address	100 %	-	21 %
Illegal images from the phone	43 %	57 %	100 %
Illegal images from the computer	43 %	57 %	100 %
Illegal images from the browser history	29 %	71 %	100 %
Browser history	36 %	64 %	79 %
Anti-virus search	73 %	27 %	79 %
Missing Messenger chat	67 %	33 %	21 %

**Table 4.1: Evidential value on identified evidence**

100 % of the participants also identified the illegal images as important. However, there was a lot of uncertainty about the evidential value when the participants were to evaluate the illegal images, and this produced differentiated reasoning among the participants.

Further comments on their reasoning can be found in chapters 4.3.1 through 4.3.11.

#### 4.3.1 Mismatching Checksum

50 % of the participants identified the mismatching checksums of the image file from the suspects computer, and all of them gave this evidence high evidential value.



The participants gave it a high evidential value because the image file should not be used as evidence without proper verification, and not because it was strong evidence against the suspect.

The participants mentioned that without the section in the report explaining that the checksums were supposed to match, most of the participants would not have noticed the mismatching checksum. Due to the mismatching checksums, some of the participants started doubting the quality of the technical report.

Several participants stated that they did not know what checksums was, and that it was seen as *technical noise*.

#### 4.3.2 Chat Log

All of the participants gave the chat log a high evidential value because the chat log connected the accused to the action he was charged with. Several of the participants questioned the lack of timestamps and wanted more information about the time frame of the chat log.

One of the participants questioned where the chat log was found in the file structure of the suspect computer and wanted to verify that this location could coincide with Peder Ås as the user of the computer.

#### 4.3.3 Mailaddress

21 % of the participants identified the mail address as important, and they also gave it a high evidential value. The reasoning behind this was with regards to the identification of Peder Ås as the person identified in the chat log.

One participant also wanted to contact the mail provider to get user / subscriber information on the mail address, by this establishing the time frame of the activity of the address. For instance, if the address was registered 2 days ago or 2 years ago.

#### 4.3.4 Illegal Images – General Comments

100 % of the participants identified the illegal images as important. However, with regards to the illegal images found on the suspect's computer and mobile phone, there was some inconsistency around the evaluation and weighing of them judicially, internally within the group of participants. Some chose to comment on the images as one, and others divided them into images from the phone, images from the computer, and images from the browser history.

The file paths presented in the technical report created uncertainty, because the majority of the participants were not able to determine the degree of intent shown by the suspect by looking at the file paths. They stated this was due to lack of technical competence on their behalf, and the lack of conclusions from the DFD in the technical report. Several of the participants stated that they would have consulted a DFD, or called the DFD as a witness in court, to explain the report with regards to the file paths.

Even though several of the participants gave the illegal images a low evidential value due to the uncertainty of the degree of intent of the suspect, the participants still meant that the evidence supported the other evidence in the investigation in an overall assessment because it said something about the interests of the suspect.

It was also commented that the court probably would not care much about where in the file structure the illegal images were found, but that the defence attorney might have. The participant would not have made a problem of the file paths if it was not argued by the defence attorney. This was commented with regards to this being an old case, and that the efficiency of the investigation also was of importance.

One of the participants recognized the pictures from the browser history as being collected from the internet one year after the suspect last used the computer but chose to still give them a high evidential value. The participant was clear on the fact that the internet is dynamic, and that the images could have changed since the suspect visited the web pages. As long as this fact was clearly stated to the court, and how this evidence was procured online, then the members of court would be able to weigh and assess this evidence in court.

With regards to the illegal images from the browser history, and the lack of quality of this digital evidence, one participant commented on how aware the prosecutor really had to be when choosing which digital evidence to present to court. The court would often know far less about assessing quality of digital evidence than the prosecutor, and it could be easy to introduce errors that would not be argued even if they had a low evidential value.

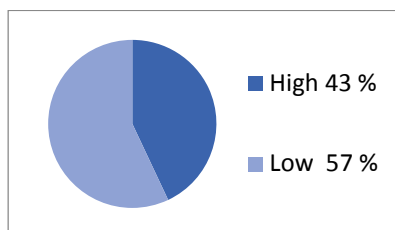
It was also commented on that the suspect in his statement stated that he claimed to not remember seeing any illegal images. The participant stated that this would not be correct, because if he ever had seen an illegal sexualised image of a child, he would not forget it.

The participants with post graduate studies in digital forensics recognized that none of the findings regarding the illegal images evidence actually contradicted the statement given by the suspect, and that there had to be something wrong with the report. The participant also stated that the report could produce a serious possibility of error of justice, and that this case should have been dismissed a year ago.

#### 4.3.5 Illegal images from the phone

43 % of the participants gave the illegal images from the phone a high evidential value, while 57 % gave it a low evidential value.

The distribution of the given evidential values are visualised in figure 4.4.



**Figure 4.4: Illegal images from the phone**

None of the participants gave any special comments on giving the illegal images from the phone a high evidential value but chose to give overall comments on the images instead. But these participants based their decision without reasoning.

Of the participants that gave the illegal images a low evidential value, the lack of confirmation from a DFD if the images were actively stored was an important reason. If

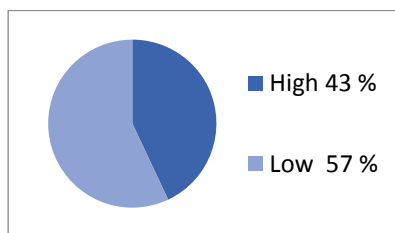
the DFD could not give such confirmation, the illegal images would be left out of the indictment.

Some of the participants also recognized that the file paths pointed to a cache, and that this did not have to derive from an active action by the suspect. The participants also recognized that Facebook was mentioned in the file path, and that this fact would have to be investigated further, especially seen in light of the missing Messenger chat application, which the file path could be a part of. The participant also stated that the evidence could coincide with the statement made by the accused.

#### 4.3.6 Illegal images from the computer

43 % of the participants gave the illegal images from the computer a high evidential value, while 57 % gave it a low evidential value.

The distribution of the given evidential values are visualised in figure 4.5.



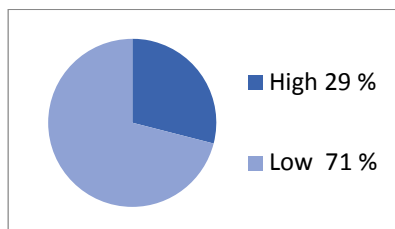
**Figure 4.5: Illegal images from the computer**

Some of the participants that gave the illegal images on the computer a high evidential value also wanted to know more about the degree of active intent concerning where the images were stored in the file structure of the phone, which also is the same reasoning some chose for giving the evidence a low evidential value.

The participants with post graduate studies in digital forensics pointed out that the file path in the report leads to an internet cache in the Firefox browser, and by this it would be almost impossible to prove intent, and that this evidence very well can coincide with the statement given by the suspect.

#### 4.3.7 Illegal images from the browser history

29 % of the participants gave the illegal images from the browser history a high evidential value, while 71 % gave it a low evidential value. The distribution of the given evidential values are visualised in figure 4.6.



**Figure 4.6: Illegal images from the browser history**

The participants that gave the illegal images from the browser history a high evidential value, stated that this evidence showed the suspects interest in illegal sexualized images, and that the browser history images by this would strengthen the other evidence as such.

When establishing that the evidence had a low evidential value, the reasoning varied some. However, lack of confirmation on the degree of active participation from the suspect was something several of the participants mentioned.

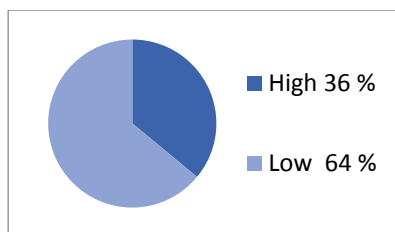
Some of the participants were also unsure if the illegal images acquired from the browser history, and the way they had been acquired, were possible to indict by law. A few of the participants commented that the pictures resided on the internet, and thus could not be a part of the indictment. This due to the fact that the suspect did not have these images in his possession, and because the internet is not a constant factor, and is ever-changing.

One of the participants even stated that this evidence was pure nonsense.

#### 4.3.8 Browser history

36 % of the participants gave the browser history a high evidential value, while 64 % gave it a low evidential value.

The distribution of the given evidential values are visualised in figure 4.7.



**Figure 4.7: Browser history**

When giving the browser history a evidential value, some of the participants gave the same reasons for their choice, even if they chose differently.

Of the participants deciding on giving the browser history a high evidential value, they all stated that this evidence supported the rest of the evidence in the investigation, and that it showed that the suspect had visited these web pages containing child abuse material. They also stated that the suspect did not just "wander into 1500 web pages" containing child abuse material, and that it proved conscious intent.

Some of the participants giving this evidence a low evidential value stated that this evidence only supported the other evidence, and would go into the overall evidence evaluation, but that it would strengthen the modus operandi of the suspect. They also mentioned that the sheer number of web pages (1500) would say anything about how much the suspect had been involved in this activity.

One of the participants stated that this only showed an activity into web pages with child abuse material, and that this fact together with the amount of web pages (1500) was interesting information. However, s/he needed more clarification on the how's and the why's, and that these facts alone could coincide with the statement given by the suspect of him being a victim of hacking or a virus.

Very few of the participants questioned where in the file structure the browser history had been located, and if this could have an impact on the quality of the evidence.

#### 4.3.9 Anti-virus search

79 % of the participants identified the anti-virus search to have importance.

73 % of these participants chose to give the anti-virus search a high evidential value, and all of them stated that the performed negative search would weaken the suspects given statement and credibility, because the negative search indicated that the suspect had not been hacked or gotten his computer infected by computer virus.

A few of the participants that gave it a high evidential value wanted another anti-virus search performed, due to the time passed since the last search, and preferably the use of more than one anti-virus tool for this job.

27 % of the participants gave the search a low evidential value, some wanted another search performed, because there may have been viruses that had not been discovered the first time due to time passed and outdated databases, and they needed more information on the possibility of virus infection.

#### 4.3.10 Missing Messenger chat on the phone:

Only 21 % of the participants identified the missing Messenger chat application as important. This was one of the evidence the fewest of the participants recognized as an important digital evidence.

However, the reasoning also differentiated between the participants.

The participants that gave the evidence a high evidential value did so because it weakened the suspect's statement and credibility.

The participants that chose to give the evidence a low evidential value, did so because it would be possible to find databases on the phone that the automated analysis tools not necessarily parsed and interpreted. The fact that remnants of a Messenger application could not be found in the automated analysis actually did not mean much. It only meant that this tool did not find any traces of it, and there could be several reasons for this. The participants wanted a deep manual analysis of the phone, where specific manual searches after the Messenger application database were performed, because there could be databases residing in the phone the tool did not find. The participants also mentioned that we could not possibly know what this tool had done with the data we put into it, and this was the reason this evidence had little evidential value.

#### 4.3.11 General comments from the participants during scenario 2:

Some of the participants had some general comments on this scenario.

One of the general consensuses was that the report format in this scenario, *the technical report*, was hard to evaluate, and a lot harder to evaluate and read than the traditional police report format.

Several of the participants stated that the technical report was a format that gave decreased accessibility to the presented evidence, and it made the digital evidence difficult to understand. The technical reports with all their technical evidence almost made the participant sleepy and unfocused, and it became hard to ask the right questions.

One of the participants commented that while s/he was evaluating the scenarios with the digital evidence, s/he suspected that police prosecutors in general probably could take this kind of digital evidence evaluation a bit lightly. This became clear for the participant now as s/he was set to evaluate digital evidence in the scenarios.

Another participant mentioned that if you looked at the investigation as a whole, you would see that the evidence resided everywhere, and in totally different parts. Some evidence could be found in the browser history, some on the phone, and so on. This would strengthen the evidence in an overall assessment of the evidence.

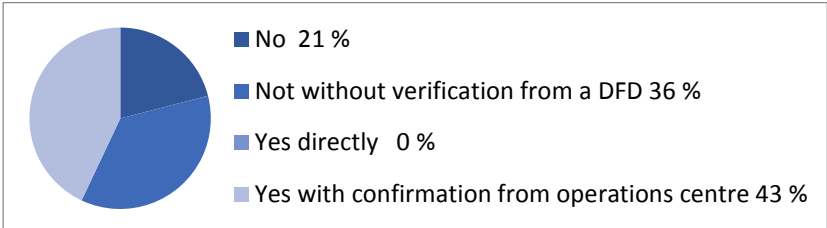
One participant commented that automated push-button forensic tools are made to handle the volume cases, but that we still would need further verification for the last percentage of completeness and credibility.

### 4.4 Scenario 3

In scenario 3, the participants were to decide if a search and seizure warrant could be issued.

None of the participants would issue a warrant directly. 36 % of the participants would not issue a search without verification of the IP search and identification from a DFD, while 43 % of the participants would issue a warrant if the police operations Centre confirmed that the IP search and identification was correct. 21 % of the participants would not issue a search and seizure warrant at all, and first try another approach like sending a police car to the address.

The distribution of the decisions on search warrants are visualised in figure 4.8.



**Figure 4.8: Distribution of warrants**

Of the 21 % that decided not to issue a warrant, some of these participants wanted to first try to send a police car to the address to access the situation. The participants reasoned that there was no need to evaluate the IP search at this point, because they would achieve the same objective by sending a police car to the address on the basis of a principle of necessity health check and talked to the identified father and daughter. If the situation still was unclear, the IP search could be evaluated.

One of the participants commented that it would be difficult not to issue a warrant in a real-life situation, if you got a call like this on a Friday night.

Of the 36 % that would have needed verification from a DFD before a search warrant was issued, their reasoning was based on the fact that the information about the IP search was from a 3<sup>rd</sup> party, and uncertainty of the quality of an IP GEO search. The majority of the participants did not know what an IP GEO search was and needed more verification.

Of the 43 % that needed the police operations central to confirm the address before issuing a warrant, the reasoning coincided with the reasoning given by the 36 % that needed verification from a DFD before issuing a warrant. The difference was that the participants from this group would have settled on a confirmation from the leader of the police operations central before issuing a warrant instead of a DFD.

However, one of the participants compared the IP GEO search to the "Find My iPhone" function, and that it would be very difficult to be conclusive when presented to results from such searches.

One of the participants commented that in a real-life Emergency situation like this, it would be very difficult not to issue a warrant, when being contacted by the leader of the police operations central.

Another participant stated that if there were no indications of this being the wrong address, and if the leader of the police operations central could ensure the correctness of the IP GEO search, the warrant would have been issued.

None of the participants would have issued a warrant directly.

The participants with post graduate studies in digital investigation and forensics would not issue a warrant without a proper user / subscriber request to the internet service provider who runs the IP address, by this identifying the address of the subscriber of the IP address at that specific time.

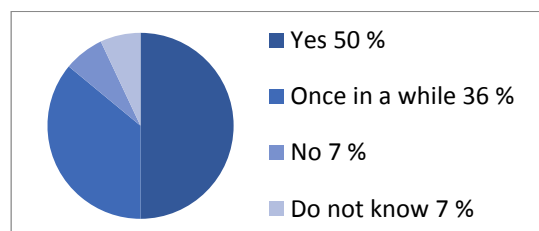
## 4.5 Quality and competence

This section contains data analysis of the post scenario interview questions.

57 % stated that there had been digital evidence present in all of their last 3 court cases, while 43 % had digital evidence present in the last 2 out of 3 court cases. None of the participants had any cases without digital evidence present as one of their last 3 court cases. In these cases, 79 % of the evidence had been mobile phones, followed by social media evidence at 71 %, and computers at 57 %.

100 % of the participants stated that they trusted digital evidence that was produced and presented by a DFD.

When the digital evidence was produced by a non-technical police officer or detective, the distribution of trust was more evenly distributed, as visualized in figure 4.9.



**Figure 4.9: Distribution of trust**

86 % of the participants stated that they would evaluate the competence of the person producing digital evidence that they were set to evaluate, while 14 % did not.

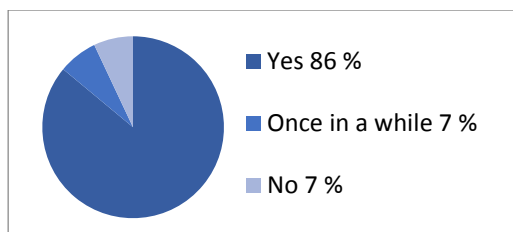
The majority of the participants stated that when they evaluated the competence of the person that produced the digital evidence, they used personal knowledge as the most preferred way to evaluate competence, and that they would contact the person that had written the report. The majority also evaluated the function or work title of the person that had written the reports. For instance, if the produced material was delivered by an IT engineer or a police recruit. Some of the participants would evaluate the process leading to the digital evidence, and if the digital evidence at hand had been discussed with a DFD before it had been presented to the participant.

100 % of the participants stated that they evaluated the evidential value of digital evidence.

The participants had different approaches for the process of evaluating digital evidence. The majority of the participants mentioned that discussing the evidence over with a DFD, or with the person who produced the evidence was a preferred way of action when evaluating digital evidence. The majority of the participants also focused on the police report that would present the digital evidence they were to evaluate. One of the participants mentioned that the prosecutor mainly evaluates documents, and that the quality of the report therefore was of great importance. Some of the participants would evaluate how the evidence was presented in the report, and by using common sense, see if the report had any logical faults. Others would evaluate if the report was written objectively and nuanced, and if the report presented the necessary evidence that coincided with the points of the criminal case. It was pointed out that the report needed to have good language, good conclusions about the evidential value, and that the participant by this would understand the evidence. One of the participants stated that by having a basic understanding of digital forensics, s/he could be able to give the evidence proper evidential value.

An interesting observation made when the participants were evaluating digital evidence in the scenarios, was that some of the participants mixed the technical evidential value with the judicially evidential value, and thus evaluated the evidential value purely through what it could prove or enlighten of the unanswered questions the investigation without considering the technical evidential value. This was also commented on by one of the participants, which stated that the prosecutor would perform a judicial evaluation of the evidence, and that it would be almost impossible for a prosecutor to evaluate technical value of digital evidence.

86 % of the participants trusted that digital evidence had been verified when produced by an automated forensic tool, 7 % did so once in a while, and 7 % did not trust automated forensic tools, see figure 4.10, *level of trust in automated forensic tools*.



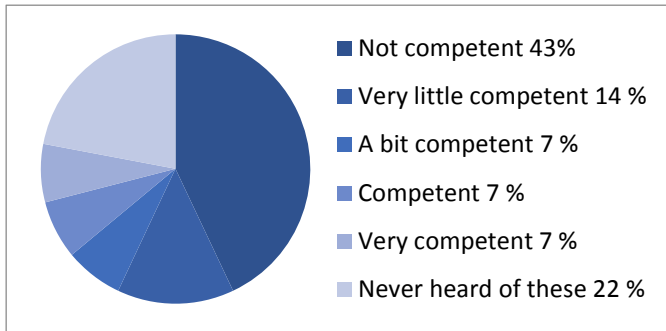
**Figure 4.10: Distribution of trust in automated tools**

Several of the participants stated that they would trust the presented evidence, unless it contained obvious faults, and that the quality of the report was important. If the report did not leave any unanswered questions, was precise, and the criminal case at hand was properly enlightened, the reasons for doubting the quality would be non-existent.

One of the participants evaluated the complexity of the produced evidence and looked at what kind of competence one would need to produce the evidence. For instance, if the evidence was produced by taking a photo of the screen of a phone, or by acquiring the phone forensically. When the participants evaluated their own competence on digital evidence produced with specific automated analysis tools like Griffeye Analyze, Internet



Evidence Finder, Cellebrite Physical Analyzer, and XRY Reader, they gave the following answers, visualized in the figure 4.11 below.

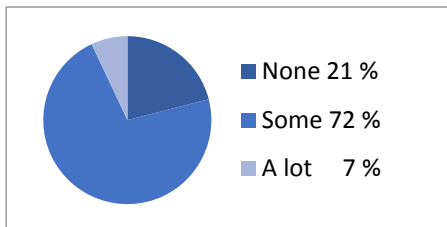


**Figure 4.11: Distribution of knowledge on forensic software**

A majority of the participants stated that they were competent if they were to prosecute criminal cases which included different digital evidence.

Of the presented cases in the questionnaire, the DDos attack case was the case that the participants set as the one they were least competent of handling. On the other end of the scale, the case with the young girl getting a nude photo spread by the use of a mobile application was the case that most of the participants stated that they were competent to handle. Similar results could be observed when looking into which digital evidence the participants stated that they were least competent to evaluate. 29 % stated digital currency as Bitcoin and Ethereum, 21 % stated ransomware and 21 % malware, 21 % stated VPN, as being digital evidence, they had the least competence on.

72 % of the participants had experienced that the members of court had questioned the quality of digital evidence by asking some questions, while 21 % had experienced some questions, and 7 % a lot of questions.



**Figure 4.12: Questions from members of court**

71 % of the participants had gotten training or additional competence on digital evidence since joining the Norwegian police service, while 29 % had not.

The participants mentioned several of the hindrances they felt worked against them when it came to digital evidence evaluation. These were:

- If the police reports were too technical, and by this too complex, it would be easy to overlook digital evidence, and thus lose the necessary logic needed for the evidence evaluation.
- If the digital evidence were poorly explained in the police report, it could lead to the prosecutors not understanding the evidence they were set to evaluate.
- The unavailability of a DFD to discuss the digital evidence with

- If the digital evidence grew old in a case, this would set the criminal case in a lot less favourable position. So, an increase in the efficiency of the investigations.
- Logical faults in the police reports presenting digital evidence, or if there were none or few conclusions on the evidential value.
- Not having enough basic knowledge about digital evidence.
- Time pressure.
- Case backlogs.

The participants mentioned several bullet points on what they thought could improve the process of evaluating digital evidence. These were:

- The majority mentioned increased competence / training as important
- The majority also stated that to have somebody to ask and discuss digital evidence with was favourable, preferably a DFD. These discussions could also be performed in a formal frame, like an investigation meeting.
- The participants also wanted improved presentations of the digital evidence, and more use of visualisation
- Some also mentioned that they wanted to earlier take an active part of the investigative leadership
- Some also sought less technical information in the reports, and more conclusions and probability statements from the DFD

## 5 Discussion

In this chapter, I will discuss the gathered data from the data analysis and answer the research problem by addressing and discussing the research sub-problems.

The chapter is organized into sections, where each sub-problem is assigned an own section. Each of the sections has undersections, depending on the number of occurrences identified.

Section 5.1 discuss which of the potential occurrences of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence may be identified.

Section 5.2 discusses which occurrences may be identified as potential fallacies due to lack of knowledge and competence of digital forensics principles.

Section 5.3 discuss the consequences are if these fallacies occur, and how can they be mitigated.

Findings from section 4.5 in the data analysis will be discussed when answers given in this section complement other findings throughout the chapter. General comments given by the participants throughout the interviews will also be discussed where they fit in the material.

### 5.1 Which potential occurrences of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence may be identified?

Only the potential occurrences of digital evidence artefacts not being evaluated and weighed in compliance with the technical quality are discussed in section 5.1.

#### 5.1.1 Scenario 1

Scenario 1 described a traffic accident, where the police officers on the scene had collected 4 pieces of digital evidence, both from the scene of the accident, and through investigating the accident. The different pieces of digital evidence were; a mobile phone, from which a table showing a timeline of the most recent phone activity was included in the police report, call records collected from the service provider, a CCTV video showing the actual accident, and a manual on-the-scene analysis of the GPS in the suspect's car (see chapter 3.3.4.1 and appendix).

##### 5.1.1.1 The phone activity from the suspect's mobile phone:

71 % of the participants assigned the phone activity with the Snapchat activity a high evidential value because they felt it had decisive importance in establishing judicial negligence, (see chapter 4.2.1). This supports the findings where 86 % of the participants stated that they trusted digital evidence had been verified when produced by an automated forensic tool. With regards to the trust in automated forensic tools, one participant stated that to argue against the result of an automated analysis from a forensic tool would compare to the hopeless struggle of arguing the correctness of a

blood analysis result. This comment emphasizes the indication of lack of knowledge and competence of digital evidence and digital forensic principles, where the participants trust the analysis result of automated tools, as described (see chapter 2.1.4).

A few participants that gave the evidence a high evidential value was confused by the time skew between the phone activity and the obtained telecom call records and stated that the needed verification of this would have an effect on how the phone activity was presented. The time skew was one of the inserted scenario artefacts made to confuse and test the participants competence, and not recognizing this would be an indication of lack of knowledge and competence of digital evidence and digital forensic principles. To request further verification would introduce unnecessary time consuming digital forensic work to the criminal investigation, which is in conflict with what the attorney general has stated as quality, (see chapter 2.3.2).

Some of the participants that gave the phone activity a high evidential value stated that they needed further clarification on the level of active user participation needed for creating the registered Snapchat activity, and by this the participants which needed more clarification could possibly have ended up with a low evidential value as an end result, due to their questioning of the technical quality of the evidence.

There were however some participants that gave the evidence a high evidential value and did not question the technical quality of the evidence. One of the artefacts inserted into the scenario was the timeline from the automated analysis tool, and it was inserted to check if the participants would question the findings (see chapter 3.3.4.1 and 2.1.4). Here they did not question the findings, which would indicate lack of knowledge and competence of the challenges of automation. Therefore, giving the phone activity high evidential value could qualify as a potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence.

In my experience, a lot of prosecutors often lack digital forensics knowledge, and tend to have the impression that automated forensic tools deliver a complete forensic copy of the mobile device, with all installed applications fully presented. This fallacy can potentially lead to wrong conclusions and could pose a threat to the credibility of digital evidence in the long run (see chapter 2.1.4).

#### 5.1.1.2 GPS unit

64 % of the participants gave the manual analysis of the GPS unit a high evidential value, and the stated reasons for weighing this evidence high were purely judicial, indicating by this the lack of proper evaluation of the technical quality of the GPS evidence and the competence of the police officer performing the analysis.

The GPS unit artefact was inserted into the scenario to check if the participants would question the competence of the police officer and the lack of documentation or audit trail (see chapter 3.3.4.1 and 2.1.3). None of the participants which assigned this evidence with a high evidential value questioned the technical quality of the evidence, the competence of the police officer or the lack of an proper audit trail, and therefore giving the GPS unit high evidential value could qualify as a potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence due to breaches to forensic principles.

## 5.1.2 Scenario 2

Scenario 2 simulated a criminal case concerning possession of sexualized child abuse images and sexualized chat with minors. The case type was chosen because this is one of the most common case types concerning digital evidence, and it would be easy to implement more technical artefacts of a broader base than in scenario 1 and 3. This was also the most complicated of the 3 scenarios (see chapter 3.3.4.2 and appendix).

In this scenario not all participants identified all the digital evidence as important. All of the participants did however quickly identify the illegal pictures and the chat log as important. There were a lot of inconsistencies around how the illegal pictures were evaluated and weighed.

### 5.1.2.1 Mismatching checksum

50 % of the participants did not identify the mismatching checksums as important, which would be a breach to the digital forensic principles (see chapter 2.1.3 and 3.3.4.2).

The mismatching checksum artefact was inserted into the scenario to test for just this fact, and by not recognizing this artefact would then indicate lack of knowledge and competence of the digital forensic principles of evidence integrity.

All of the participants which identified the mismatching checksums gave this a high evidential value because the image file should not have been used as evidence without proper verification, and not because it had a high value as evidence per se.

None of the participants who did not identify this as important digital evidence questioned the technical quality of the mismatching checksums, and therefore not identifying the mismatching checksums could qualify as a potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence due to lack of knowledge of the digital forensic principles of evidence integrity.

### 5.1.2.2 Mail address

The mail address in itself did not open up for errors; however, the identification of it could be misinterpreted.

79 % of the participants did not identify the mail address as important.

The mail address artefact was inserted into the scenario to test for lack of knowledge on mail tracing and the digital evidence chain.

The low percentage of participants who identified the mail address as important can be explained by a potential weakness in the scenario, where the scenario background information stated that the identification of the suspect already was performed by the NCIS. The participants could by this be led to believe that the mail address evidence could be dropped as important evidence.

Nevertheless, one participant still identified the evidence as important despite the scenario background information, stated that s/he did so because s/he wanted user/subscriber information from the mail provider of the activity of the address. Therefore, not identifying the mail address could qualify as a potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence due to lack of knowledge on basic mail tracing (see chapter 3.3.4.2 and 2.1.4).

However, given the potential opening for misinterpretation of the scenario background information, I will not classify this as a potential occurrence.

#### 5.1.2.3 Illegal images

100 % of the participants identified the illegal pictures as important. However, there were some inconsistencies on how the images were evaluated and weighed.

For an easier overview, the discussion on the illegal images are divided into 3 parts; the illegal images found on the mobile phone and on the computer, the illegal images found in the browser history, and general comments from the participants part.

The mobile phone and computer illegal images artefact was introduced into the scenario to test if the participants would trust the findings of the automated analysis and if they would question the location of the images residing in a cache, by this recognising that the images had a low technical quality (see chapter 2.1.4 and 3.3.4.2).

The illegal images found on the suspects mobile phone and computer were assigned the same evidential level of value from the participants. 43 % of the participants assigned a high evidential value on the illegal images recreated from the mobile phone of the suspect, and 43 % on the illegal images found on the suspect's computer. The reasoning for doing so was purely judicial; the images were illegal, and found on the suspects mobile phone, indicating that no real evaluation of the technical quality were performed.

Some of these participants questioned the presented file paths where the illegal images were found and wanted more information on the degree of intent and needed active participation from the suspect with regards to saving the illegal images. The participants stated however that this was due to lack of what was described as "technical competence" on their behalf, and the lack of conclusions from the DFD in the technical report. This statement indicates clearly a lack of knowledge and competence; by the participants own comment alone.

There were participants that gave the illegal images found on the mobile phone and computer of the suspect a high evidential value that did not question the technical evidential quality of the evidence, and therefore could qualify as a potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence due to lack of knowledge and competence on the importance of caching (see chapter 2.1.4 and 3.3.4.2).

The browser history artefact was inserted into the scenario to test if the participants would question the location of the images, and the process used to acquire the images.

29 % of the participants gave the 1500 illegal images from the browser history a high evidential value, and the stated reasons for this was that it showed the suspects interest in illegal sexualized images of children, and would strengthen the other evidence in the investigation, in other words purely judicial reasoning. There were participants that gave the illegal images from the browser history found on the suspect computer a high evidential value, that did not question or argue the technical evidential quality of the evidence. This indicated that the participants did not question the technical quality of the evidence, and a lack in knowledge and competence in digital forensic principles as well as browser forensics and caching (see chapter 2.1.3, 2.1.4 and 3.3.4.2), and therefore this could qualify as a potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence.

One of these participants recognized the pictures from the browser history as being collected from the internet one year after the suspect last used the computer but chose to give them a high evidential value. The participant was clear on the fact that the internet is dynamic, and that the images could have changed since the suspect visited the web pages. The participant stated that as long as this fact was clearly stated to the court, and how this evidence was procured online, then the members of court would be able to evaluate and weigh this evidence in court. Even if this reasoning legally could be correct, the prosecutor could by presenting these images risk inducing evidence into the court which could be difficult to evaluate without some knowledge and competence on digital forensics and the internet. Presenting evidence of such low technical quality into a court which evaluate evidence by the free evidence evaluation principle could confuse the court and the evidence may get assigned a higher value than it would deserve and could by this produce an error of justice.

#### 5.1.2.4 Browser history

36 % of the participants gave the browser history from the suspect computer containing 1500 visits to web pages with supposedly child abuse material a high evidential value, and all of them stated they did so because the browser history supported and strengthened the rest of the evidence in the investigation, and showed conscious intent towards child abuse material.

The browser history artefact was introduced into the scenario to test if the participants would question the lack of an audit trail, and of internet caching (see chapter 2.1.3, 2.1.4 and 3.3.4.2).

As one of the participants stated:

*"You do not just wander into 1500 web pages containing child abuse material."*

There were participants that gave the browser history alone, without clarification and verification on the suspect being a victim of a computer virus or hacking, a high evidential value. This could qualify as a potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence, due to the indicated lack of knowledge and competence on digital forensic principles and the pitfalls of internet caching (see chapter 2.1.3, 2.1.4 and 3.3.4.2).

#### 5.1.2.5 Antivirus search

73 % of the participants assigned a high evidential value to the performed anti-virus search with a negative result, and the majority of these did so because the negative search result indicated that there were no viruses on the suspect's computer, and that this fact would weaken the suspect's statement and credibility.

The antivirus search artefact was introduced into the scenario to test if the participants questioned the result of the search due to time passed and the use of only one tool, without any proper audit trail (see chapter 2.1.3, 2.1.4 and 3.3.4.2).

The search had been performed one year ago at the time of the arrest and came out negative. Due to the time passed since the first anti-virus search, some of these participants wanted another search performed, preferable by more than one tool.

There was however participants that gave the evidence a high evidential value, and who did not question the search, by this indicating lack of knowledge and competence of basic digital forensic principles and the function of antivirus and malware and qualify as a

potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence.

#### 5.1.2.6 Missing Messenger chat

Only 21 % of the participants identified the missing Messenger chat application on the suspects mobile phone as being an important evidence, which clearly indicate a lack of knowledge and competence in the pitfalls of automation without verification among the participants (see chapter 2.1.4). This evidence could be considered to be crucial to evaluate the suspect's lack of intent and guilt, and not being able to discover the importance of this could result in the wrong conclusions being made.

The missing Messenger artefact was introduced into the scenario as an indicator for knowledge and competence on automation; inflexibility and verification (see chapter 2.1.4 and 3.3.4.2).

The only participant that gave the evidence a high evidential value did so because the missing Messenger chat on the suspects mobile phone weakened the suspects statement and credibility, which actually would be the opposite result of the intended scenario result. So even if the participant identified the artefact and the importance, the reasoning behind the choice could amplify the original low value of the evidence, and elevate the value to high. The reasoning indicated that even if the artefact was identified, it was not understood, and by this indicating lack of knowledge of digital evidence and forensics.

There was only one participant without post graduate studies in digital investigation and forensics that identified this as important evidence, and the low percentage of participants identifying the evidence in itself could qualify as a potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence, as stated in the introduction of chapter 5.1.2.

#### 5.1.3 Scenario 3

Scenario 3 simulated a situation where the prosecutor is at home on off-hours prosecutor duty a late Friday night, and receives a phone call from the Police Operations Centre regarding a 16-year old girl, victim of weekly sexual abuse who is planning to commit suicide and the following need for the prosecutor to quickly issue a warrant or not.

In scenario 3 the IP address artefact and the IP GEO search artefact were introduced to test if the participants would question the competence of the police Emergency operator, the competence of the chat moderator and 3<sup>rd</sup> party information, and the technical quality of the IP-search (see chapter 2.1.4 and 3.3.4.3).

None of the participants would issue a warrant directly.

However, 43 % of the participants would issue a warrant if the Police Operations Centre confirmed that the IP search was correct. In the scenario the Police Operations Centre also trusted the IP GEO search, and would therefore not question the IP search and address location they themselves had been a part of performing. Therefore, the participants that would issue the warrant on the basis of the Police Operations Centre confirming the correctness of the IP search could qualify as a potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence, by this showing a lack of knowledge and competence in IP tracing and digital forensic principles (see chapter 2.1.3, 2.1.4 and 3.3.4.3).



#### 5.1.4 Summary

In the scenarios there were several identified potential occurrences of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence, and the reasons for this were lack of knowledge and competence on digital forensic principles and on the implications of digital artefacts (see chapters 5.1.1, 5.1.2, and 5.1.3).

As some of the participants openly stated, they did not have the technical competence to fully understand digital evidence, and that they have had no training with regards to digital evidence. This is supported by the findings of the study, where there are indications of lack of competence influencing quality of the evidence evaluation. There were also examples of participants asking the right questions objectively, and by this would order new investigative steps performed, that would lead to the faulty digital evidence being corrected.

An interesting observation made when the participants were evaluating digital evidence in the scenarios, was that some of the participants did not evaluate the technical quality of the presented evidence and thus evaluated the evidential value purely through what it could prove or enlighten of the unanswered questions the investigation without considering the technical evidential value. This was also commented on by one of the participants, which stated that the prosecutor would perform a judicial evaluation of the evidence, and that it would be almost impossible for a prosecutor to evaluate technical value of digital evidence. The majority of the participants of the study clearly stated a trust in both automated forensic tool results and digital evidence presented by a DFD. Even if fewer of the participants stated they always trusted digital evidence presented by police officer or detectives, very few actually did question this in the scenarios. This indicates that as the comment above states, that the prosecutor for the most trusts the quality of the evidence they are presented with. One of the participants commented that while s/he was evaluating the scenarios with the digital evidence, s/he suspected that police prosecutors in general probably could take this kind of digital evidence evaluation a bit lightly.

This would also imply that the police officers and DFDs would need to be extraordinarily careful to follow the digital forensic principles when working and handling digital evidence and have the utmost focus on quality both regarding the digital evidence and how reports are written. If not, there would be a strong risk of inducting evidence of low technical quality into the courts, possible risking errors of justice.

The technical report was a format that many of the participants felt gave a decreased accessibility to the presented evidence, and it made the digital evidence difficult to understand and by this made it difficult to ask the right questions. Even if the technical report in this study was introduced with errors and lack of oversight, the participants were often confused by the report format, and the way evidence was presented. This was also an observation made during the interviews, which could coincide with the prosecutors' daily work of perceiving and interpreting textual language (see chapter 2.2.5). This could imply that the reports presenting evidence need to also describe the findings even more textual perfect, or the prosecutors will need to increase their competence on presentation of technology. The DFD need to teach to write better reports, and the prosecutor need to teach to better understand digital evidence.

Another observation which also was commented on by the participants was use of overall assessment of evidence together with digital evidence of different quality, which also is

supported by Norwegian Supreme Court rulings (see chapter 2.2.2). In the scenarios there were examples of low-quality evidence, in some cases also incorrect, which were compiled into an overall assessment of evidence which ended with the multiple low evidence together being evaluated as high (see chapter 4.3.4). This observation, if seen together with the principle of free evidence admissibility and free evidence evaluation (see chapter 2.2.2 and 2.2.4), could open for a potential for error of justice if there is a lack of knowledge and competence among the prosecutors and the judiciary.

The potential occurrences of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence were discussed, and the result could indicate that the competence of the police prosecutor needs to increase when evaluating digital evidence and artefacts; if not the prosecutor will lose some of the function as a guarantor of the rule of law, and this could lead to errors of justice.

## 5.2 Which of these occurrences may be identified as potential fallacies due to lack of knowledge and competence of digital forensics principles?

All of the 14 participants interviewed in this study had a Master of Laws degree, together with the obligatory start-up study for all new prosecutors in the Norwegian Police Service (7).

However, 2 of the participants had in addition to the Master of Laws degree, post graduate studies in digital investigation and digital forensics from the Norwegian Police University College (42).

To identify if there were any potential fallacies introduced, each potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence identified in chapter 5.1 were discussed and compared to the answers given by the participants with post graduate studies in digital investigation and digital forensics.

Potential differences in the quality of evidence evaluation and weighing of digital evidence between the participants with post graduate studies in digital investigation and digital forensics and those without, could then indicate if fallacies due to lack of knowledge and competence of digital forensics principles were introduced into the evidence evaluation process.

The potential differences are presented as undersection, where each undersection represents a potential occurrence.

### 5.2.1 The phone activity timeline from the suspect's mobile phone

**The 1<sup>st</sup>** potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence was identified in chapter 5.1.1, scenario 1, the phone activity timeline table from the suspect's mobile phone. Here some of the participants gave the evidence a high evidential value, and did not question the technical quality of the evidence (for full discussion see chapter 5.1.1.1).

One of the artefacts inserted into the scenario was the timeline from the automated analysis tool, and it was inserted to check if the participants would question the findings (see chapter 3.3.4.1 and 2.1.4). The time skew was another of the inserted scenario artefacts made to confuse and test the participants' competence, and not recognizing this

would be an indication of lack of knowledge and competence of digital evidence and digital forensic principles. To request further verification would introduce unnecessary time consuming digital forensic work to the criminal investigation, which is in conflict with what the attorney general has stated as quality, (see chapter 2.3.2).

The participants with post graduate studies in digital investigation and digital forensics were among the 29 % that assigned the phone activity timeline table from the suspect's mobile phone with a low evidential value. The participants with post graduate studies in digital investigation and forensics stated they did so because an automated analysis not necessarily would produce the required evidential completeness of the evidence, and that a closer manual examination of the application database would be needed. They did not question the competence of the person that analysed the digital evidence, even though this person was a fictive non-technical police officer, but they did question the quality of the evidence.

The participants with post graduate studies in digital investigation and digital forensics recognized the low technological quality of the timeline table and were not confused by the inserted time skew, and their reasoning for doing so were sound and in compliance with digital forensics principles and knowledge.

This mark a difference in the given answers and reasoning between the participants with and without post graduate studies in digital investigation and digital forensics, which indicate the presence of a potential fallacy due to lack of knowledge and competence in digital evidence and digital forensics principles.

### 5.2.2 The manual analysis of the GPS unit

**The 2<sup>nd</sup>** potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence was identified in chapter 5.1.1, scenario 1, and the manual analysis of the GPS unit (for full discussion see chapter 5.1.1.2).

The participants with post graduate studies in digital investigation and forensics assigned the evidence a low evidential value, and also clearly stated that the GPS unit was only manually analysed without documenting how this was performed, and that there would be no way of telling how the GPS unit registered data, with reference to the completeness and reliability of the evidence.

The participants with post graduate studies in digital investigation and digital forensics recognized the low technological quality of the GPS evidence and questioned the competence of the police officer, and their reasoning for doing so were sound and in compliance with digital forensics principles and knowledge of digital forensics.

This mark a difference in the given answers and reasoning between the participants with and without post graduate studies in digital investigation and digital forensics, which indicate the presence of a potential fallacy due to lack of knowledge and competence in digital evidence and digital forensics principles.

### 5.2.3 The missing identification of digital evidence

**The 3<sup>rd</sup>** potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence was identified in chapter 5.1.2.

This part is a more general finding, due to not being connected to a specific evidence. Not all participants identified all the digital evidence as important, which in itself would indicate a lack of knowledge and competence in digital evidence. A person would not identify something if s/he did not know what to look for. By not identifying all digital evidence, these participants showed that they did not possess the necessary knowledge and competence on digital evidence, and on how the different digital evidence may have importance or not. Lacking this knowledge may have led the participants to the fallacy of trusting that evidence produced without testing how the data was recorded, or if the analysis changed some of the data, would be reliable.

The participants with post graduate studies in digital investigation and forensics did identify all of the digital evidence. The participants with post graduate studies in digital investigation and digital forensics recognized and identified all of the digital evidence, and their reasoning for doing so were sound and in compliance knowledge of digital evidence.

This mark a difference in the given answers and reasoning between the participants with and without post graduate studies in digital investigation and digital forensics, which indicate the presence of a potential fallacy due to lack of knowledge and competence on digital evidence.

#### 5.2.4 The mismatching checksums of the suspects computer

**The 4<sup>th</sup>** potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence was identified in chapter 5.1.2, the mismatching checksum of the image file of the suspects computer (for full discussion see chapter 5.1.2.1).

All of the participants which identified the mismatching checksums gave this a high evidential value because the image file should not have been used as evidence without proper verification, and not because it had a high value as evidence in the investigation. The participants with post graduate studies in digital investigation and forensics were among these participants.

The participants with post graduate studies in digital investigation and digital forensics recognized the mismatching checksums and questioned the quality of the image file. Their reasoning for doing so were sound, and in compliance with digital forensics principles, digital evidence integrity and knowledge of digital forensics.

This mark a difference in the given answers and reasoning between the participants with and without post graduate studies in digital investigation and digital forensics, which indicate the presence of a potential fallacy due to lack of knowledge and competence in digital evidence and digital forensics principles.

#### 5.2.5 The illegal images

**The 5<sup>th</sup>** potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence was identified in chapter 5.1.2, the illegal images from the suspects mobile phone, computer and browser history (for full discussion see chapter 5.1.2.3).

100 % of the participants identified the illegal pictures as important, but evaluated and weighed the images differently. There were participants that gave the illegal images found on the mobile phone and computer of the suspect high evidential values, and the

illegal images from the browser history found on the suspect computer that did not question the technical quality of the evidence, high evidential value.

The participants with post graduate studies in digital investigation and forensics assigned a low evidential value to the images, recognizing that the file paths of the images pointed to a cache, and that this fact did not have to derive from an active action by the suspect. These participants also recognized that Facebook was mentioned in the file path concerning the illegal images on the mobile phone, and that this fact would have to be investigated further, especially seen in light of the missing Messenger chat application, which the file path could be a part of. The participants also stated that the file paths of the images could coincide with the statement given by the accused.

They also stated that this evidence was pure nonsense because these images resided on internet. They also questioned the legality of indicting the suspect on the basis of this evidence at all, due to internet being dynamic and by this not a constant factor, it would not be possible to say if these images were the same as on the time of the suspect supposedly visited these web pages.

The participants with post graduate studies in digital investigation and digital forensics recognized that the images residing in caches and questioned the quality of the forensic analysis. Their reasoning for doing so were sound, and in compliance with digital forensics principles, digital evidence integrity, and knowledge of digital forensics.

This mark a difference in the given answers and reasoning between the participants with and without post graduate studies in digital investigation and digital forensics, which indicate the presence of a potential fallacy due to lack of knowledge and competence in digital evidence and digital forensics principles.

With regards to the illegal images from the browser history, and the lack of quality of this digital evidence, one of the participants with post graduate studies in digital investigation and forensics commented on how aware the prosecutor really had to be when choosing which digital evidence to present to court. The court could often know far less about the technical evidential quality of digital evidence than the prosecutor, and it could be easy to introduce errors that would not be argued by the court, even if they had a low evidential value.

#### 5.2.6 The browser history from the suspects computer

**The 6<sup>th</sup>** potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence was identified in chapter 5.1.2, the browser history from the suspects computer (for full discussion see chapter 5.1.2.4).

The participants with post graduate studies in digital investigation and forensics stated that this evidence only showed an activity into web pages that contained child abuse material, but the fact it were 1500 visited web pages was interesting. However, they wanted more clarification, especially concerning the suspects statement of being victim of a potential virus-infected computer, because these facts alone could coincide with the suspect's statement.

The participants with post graduate studies in digital investigation and digital forensics recognized that the images residing in caches and questioned the quality of the forensic analysis. Their reasoning for doing so were sound, and in compliance with digital forensics principles, digital evidence integrity, and knowledge of digital forensics.

This mark a difference in the given answers and reasoning between the participants with and without post graduate studies in digital investigation and digital forensics, which indicate the presence of a potential fallacy due to lack of knowledge and competence in digital evidence and digital forensics principles.

### 5.2.7 The performed anti-virus search on the suspects computer

**The 7<sup>th</sup>** potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence was identified in chapter 5.1.2, the negative anti-virus search performed on the suspect's computer (for full discussion see chapter 5.1.2.5).

The participants with post graduate studies in digital forensics stated that this evidence had a low evidential value, due to the time that had passed since the search was performed, and because there might have been a new virus at the time of the search that had not yet been implemented in the databases of the search tools.

The participants with post graduate studies in digital investigation and digital forensics recognized that the performed antivirus search lacked in quality. Their reasoning for doing so were sound and in compliance with digital forensics principles, digital evidence integrity, and knowledge of digital forensics.

This mark a difference in the given answers and reasoning between the participants with and without post graduate studies in digital investigation and digital forensics, which indicate the presence of a potential fallacy due to lack of knowledge and competence in digital evidence and digital forensics principles.

### 5.2.8 The missing Messenger chat on the suspects mobile phone

**The 8<sup>th</sup>** potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence was identified in chapter 5.1.2, the missing Messenger chat on the suspects mobile phone (for full discussion see chapter 5.1.2.6).

The participants with post graduate studies in digital forensics identified this evidence, and they assigned this evidence to a low evidential value. The reasoning for doing this based on automated forensic tools were being made to handle the volume cases, but that the evidence still would need further verification for the last percentage of completeness and credibility, especially regarding false negatives. They stated that it would be possible to find databases on the phone that the automated analysis tools not necessarily parsed and interpreted, and the fact that remnants of a Messenger application could not be found in the automated analysis actually did not mean much. It only meant that this tool did not find any traces of it, and there could be several reasons for this. The participants wanted a deep manual analysis of the phone, where specific manual searches after the Messenger application database were performed, because there could be databases residing in the phone the tool did not find.

The participants with post graduate studies in digital investigation and digital forensics recognized that the missing Messenger lacked in quality. Their reasoning for doing so were sound, and in compliance with digital forensics principles, digital evidence integrity and knowledge of digital forensics.

This mark a difference in the given answers and reasoning between the participants with and without post graduate studies in digital investigation and digital forensics, which

indicate the presence of a potential fallacy due to lack of knowledge and competence in digital evidence and digital forensics principles.

### 5.2.9 The IP search from scenario 3

**The 9<sup>th</sup>** potential occurrence of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence was identified in chapter 5.1.3, scenario 3, the IP GEO search and the request for a warrant (for full discussion see chapter 5.1.3).

The participants with post graduate studies in digital investigation and forensics would not issue a warrant without a proper user / subscriber request to the internet service provider who runs the IP address, by this identifying the address of the subscriber of the IP address at that specific time. They stated that an IP GEO search would not point to the correct address.

The participants with post graduate studies in digital investigation and digital forensics recognized that the performed IP search lacked in quality. Their reasoning for doing so were sound, and in compliance with digital forensics principles, digital evidence integrity, and knowledge of digital forensics.

This mark a difference in the given answers and reasoning between the participants with and without post graduate studies in digital investigation and digital forensics, which indicate the presence of a potential fallacy due to lack of knowledge and competence in digital evidence and digital forensics principles.

### 5.2.10 Summary

Throughout the different scenarios, the participants with post graduate studies in digital investigation and forensics evaluated and weighed the digital evidence in compliance with the technical quality of the evidence, also in all of the potential occurrences listed in chapter 5.1, as shown in undersections 5.2.1 through 5.2.9.

There were also other participants who managed to evaluate and weigh the digital evidence in compliance with the technical quality of the evidence, but not as consistently as the participants with post graduate studies in digital investigation and forensics, who were able to solve the scenarios without any deviating from best practice.

This difference was not only seen in the answers the participants gave, but also in the reasoning behind their decisions. The participants with post graduate studies in digital investigation and forensics gave reasoning which were in compliance with digital forensic best practice and principles, while the participants without post graduate studies in digital investigation and forensics often gave only judicial reasoning.

Potential bias was also identified in the interviews, where it was commented on that the suspect in his statement stated that he claimed to not remember seeing any illegal images, and that this would not be correct, because if the suspect ever had seen an illegal sexualized image of a child, he would not forget it. Due to the scope of the thesis, this was not discussed further.

The difference in evaluation and weighing of the digital evidence between the participants with post graduate studies in digital investigation and forensics and other participants were discussed. The result may indicate that these were potential occurrences of fallacies due to lack of knowledge and competence of digital forensics principles among the

participants. The marked difference between participants with or without post graduate studies in digital forensics was not only seen in the answers the participants gave, but also in the reasoning behind their decisions. The participants with post graduate studies in digital investigation and forensics gave reasoning which were in compliance with digital forensic best practice and principles, while the participants without post graduate studies in digital investigation and forensics often gave only judicial reasoning.

## 5.3 What are the consequences if these fallacies occur, and how can they be mitigated?

### 5.3.1 Consequences

*"Failing to provide lawyers and judges with sufficient education in digital evidence can result in serious miscarriages of justice and disruption of the legal system".*

As clearly stated by Barbara Endicott-Popovsky and Aaron Alva in the Journal of Digital Evidence (43), the consequences of poor understanding and legal ignorance of digital forensics could lead to grave errors of justice, as in the case of; State of Connecticut v. Julie Amero in 2004.

In this case, the substitute-teacher Julie Amero was found guilty on four counts of risk to a child, with a possibility of a 40-year sentence, on the basis of incorrectly evaluated digital evidence. The lack of technical knowledge among the different members of court, including the prosecutor, led to the digital evidence being misinterpreted.

Even though the fictive suspect in the fictive scenarios of this study risked far less severe sentences than Julie Amero, the results from the digital evidence evaluations and interviews show that errors of justice potentially could have been a result in the scenarios as well.

As Asbjørn Rachlew states; "An insidious trait of the errors of justice is that they can be made by the participants of the judicial chain, participants that in spite of the error, still believe the result of the criminal case to be correct." (3) p.5.

There were also other observations made during the interviews, and one of these was that the participants on several occasions commented that identified evidence would support the other evidence in the investigation in an overall evidence assessment, even if the identified evidence had a low evidential value and a low technical quality. This was also commented on even when the evidence in question was incorrect but perceived by the participants as having a high or low evidential value. It was also mentioned that if you looked at the fictive scenario investigations as a whole, you would see that the evidence resided everywhere, and in totally different parts. Some evidence could be found in the browser history, some on the phone, and so on. This would strengthen the evidence in an overall assessment of the evidence. Another participant commented that as long as the evidential facts were clearly stated to the court, then the members of court would be able to weigh and assess this evidence in court, even if the evidence had a low quality.

This way of judicial reasoning is widely used when evaluating traditional evidence where there is free evidence admission like in Norway and would rarely be problematic if all members of court fully understood the judicial implications and quality of the evidence at hand.



With this judicial reasoning in mind, imagine a courtroom consisting of potentially members not fully understanding the judicial implications of the digital evidence at hand. In such a situation, the members of court may not discover when incorrect or evidence with low quality are presented as a part of an overall evidence assessment, ending up with a situation where multiple incorrect digital evidence of low quality seen together are being perceived as evidence of high value. Such a situation could also potentially result in errors of justice.

This potential was supported by a comment from one of the participants, stating that the court probably would not care much about where in the file structure the illegal images were found, but that the defence attorney might have. The participant would not have made a problem of the file paths if it was not argued by the defence attorney. This was commented with regards to this being an old case, and that the efficiency of the investigation also was of importance.

One of the participants suspected that police prosecutors in general probably could take this kind of digital evidence evaluation a bit lightly. This became clear for the participant now as s/he was set to evaluate digital evidence in the scenarios. This can also be a sign of the *Hawthorne effect* (see chapter 3.3.5), where the participant performs better or differently due to the participation in the research study.

One of the participants with post graduate studies in digital investigation and digital forensics stated that the technical report in scenario 2 could produce a serious possibility of error of justice, and that this case should have been dismissed a year ago.

### 5.3.2 Mitigation

When examining different factors that could mitigate digital evidence being poorly evaluated, several elements should be considered.

71 % of the participants had gotten training or additional competence on digital evidence since joining the Norwegian police service, while 29 % had not. However, only 14 % of the participants had anything more than informal exchange of knowledge between colleagues.

The participants were asked if they could mention some of the hindrances that they felt were working against them when it came to evidence evaluation, and also on which factors they thought could improve the process of evaluating digital evidence.

Not having enough basic knowledge about digital evidence was the main hindrance they mentioned, and that more competence was needed.

The basic competency level of a prosecutor consists of a Master of Laws degree, and the obligatory 105 hours of start-up course delivered by the Norwegian Police University College. None of these study plans include training or basic knowledge on digital evidence. Digital evidence and cyber related prosecution work should be considered implemented into the study plans of these studies.

When looking at the post graduate studies at the Police University College, there are 50 studies meant for the investigative detective, where of 10 studies on different topics and levels are within digital investigation or digital forensics. For the prosecutor there are only 3 studies, and that includes the obligatory 105 hours start-up course. None of the studies include digital investigation or digital forensics for the prosecutor. The

prosecutors are however free to apply for all of the 50 studies meant for the investigative detective.

There would however be understandable if these courses meant for the investigative detective could be perceived as less interesting for the prosecutor, than a specific study course on digital evidence made by prosecutors, for prosecutors.

When asked about their competence on digital evidence, several of the participants mentioned the difficulty of getting approval for applying for post graduate studies at the Norwegian Police University College due to case backlogs and time pressure as hindrances for undertaking such post graduate studies.

The Norwegian Police University College should however consider setting up a post graduate study course on digital evidence directed at the prosecutor specifically. To work around the challenge of time pressure due to case backlogs it would be cost efficient to set this up as an online study.

Alternatively, a specific obligatory yearly training (OÅO) for the prosecutor specifically could be implemented, just as OÅO for the investigative detective and investigative detective leader are set up in the Norwegian Police Service today.

The US justice department released in 2007, more than 12 years ago, a guide on digital evidence for the prosecutor. A similar guide should be considered implemented in Norway also.

The technical reports and the cooperation with the DFD were also stated to be of importance for the quality of the evidence evaluation. Some of the participants felt that if the police reports were too technical, and by this too complex, it would be easy to overlook digital evidence, and thus lose the necessary logic needed for the evidence evaluation. The factor of digital evidence being poorly explained or understood in the police report could lead to the prosecutors not understanding the evidence they were set to evaluate.

The prosecutors also wanted more conclusions on the evidential value included from the DFD that wrote the report, but this may be due to the lack of competence of the prosecutors.

However, an arrangement where the quality and lay out of the technical reports should however be considered evaluated by the digital forensic community in Norway. The participants wanted an increased use of visualization of the digital evidence when presented to the prosecutor and the members of court and mentioned the possibility of implementing an obligatory DFD-to-prosecutor walk through of digital evidence during the investigation.

If one were to include the role of the DFD, an obligatory peer review of the quality of the technical reports and the quality of the digital evidence presented could also be implemented. In addition to this, an increased awareness of the pitfalls automation without verification could bring into the production of digital evidence throughout the Norwegian Police Service.

Mitigation on an organizational level could include increased digital forensic specialization of the police prosecutors, where every digital policing district unit in the Norwegian police service would be assigned their own prosecutor. In addition to prosecuting the most complex criminal cases involving digital evidence, these specialized prosecutors could

also advice other prosecutors in the police districts on digital evidence evaluation, by this increasing the level of knowledge on digital evidence over time among prosecutors.

## 6 Conclusions

By combining theory from law, digital forensics, and investigation methodology – and by creating and simulating real-life evidence evaluation scenarios, and obtaining information on evidence evaluation through interviewing case study participants, fallacies introduced in to the prosecutor process of evaluating and weighing digital evidence in compliance with the technical quality of the evidence were identified:

### 6.1 Digital evidence were not evaluated and weighed in compliance with the technical quality of the evidence

In the scenarios there were several identified potential occurrences of digital evidence not being evaluated and weighed in compliance with the technical quality of the evidence, and the reasons for this were lack of knowledge and competence on digital forensic principles and on the implications of digital artefacts.

The participants did not have the technical competence to fully understand digital evidence, and that they have had no training with regards to digital evidence. This is supported by the findings of the study, where there are indications of lack of competence influencing quality of the evidence evaluation.

The competence of the police prosecutor needs to increase when evaluating digital evidence and artefacts; if not the prosecutor will lose some of the function as a guarantor of the rule of law, and this could lead to errors of justice.

This would also imply that the police officers and DFDs would need to be extraordinarily careful to follow the digital forensic principles when working and handling digital evidence, and have the utmost focus on quality both regarding the digital evidence and how reports are written. If not, there would be a strong risk of inducting evidence of low technical quality into the courts, possible risking errors of justice.

The technical report was a format that many of the participants felt gave a decreased accessibility to the presented evidence, and it made the digital evidence difficult to understand and by this made it difficult to ask the right questions. This could imply that the reports presenting evidence need to also describe the findings even more textual perfect, or the prosecutors will need to increase their competence on presentation of technology. We need to teach the DFD to write better reports, and to teach the prosecutor to better understand digital evidence.

Another observation which also was commented on by the participants was the use of overall assessment of evidence together with digital evidence of different quality. In the scenarios there were examples of low quality evidence, in some cases also incorrect, which were compiled into an overall assessment of evidence which ended with the multiple low evidence together being evaluated as high This seen together with the principle of free evidence admissibility and free evidence evaluation could open up for a potential for error of justice if there is a lack of knowledge and competence among the prosecutors and the judiciary.

## 6.2 Fallacies due to lack of knowledge and competence were identified

Throughout the different scenarios, the participants with post graduate studies in digital investigation and forensics evaluated and weighed the digital evidence in compliance with the technical quality of the evidence and best digital forensics practice.

There were also other participants who managed to evaluate and weigh the digital evidence in compliance with the technical quality of the evidence, but not as consistently as the participants with post graduate studies in digital investigation and forensics, who were able to solve the scenarios without any deviating from best practice.

This difference was not only seen in the answers the participants gave, but also in the reasoning behind their decisions. The participants with post graduate studies in digital investigation and forensics gave reasoning which were in compliance with digital forensic best practice and principles, while the participants without post graduate studies in digital investigation and forensics often gave only judicial reasoning for their answers.

## 6.3 Consequences and Mitigation

The consequences of fallacies being introduced into the evaluation process of digital evidence could lead to poorer quality of the criminal cases, and wrong conclusions being made, which could pose a threat to the rule of law.

Some prosecutors openly stated that they did not have the technical competence to fully understand digital evidence, and that they have had no training with regards to digital evidence.

As a short term countermeasure, the implementation of a specific obligatory yearly training (OÅO) for the prosecutor, where digital and cyber related evidence and the potential pitfalls of automation without verification were discussed, could potentially help increase the awareness and mitigate the threat to the rule of law.

A national guide on digital evidence for the prosecutor should also be considered implemented.

Of long term countermeasures, the implementation of knowledge on digital and cyber related evidence and on the challenges these evidence present to the evidence evaluation, should be considered implemented into the study plans of the Norwegian Master of Law degree and the obligatory 105-hours start-up course at the Norwegian Police University College.

The Norwegian Police University College should also consider setting up a post graduate study course on digital evidence aimed at the prosecutor specifically. To work around the challenge of time pressure due to case backlogs it would be cost efficient to set this up as an online study.

The recommendations of the Norwegian prosecution analysis report - "*Påtaleanalysen*" – on a systematic competence build up for the police prosecutor should be implemented.

An obligatory peer review of the quality of technical reports and the digital evidence, together with an increased use of visualization of the digital evidence when presented to the prosecutor were sought after by the prosecutors in the study. An obligatory DFD-to-

prosecutor walk through of digital evidence before the evidence evaluation could also be implemented.

Police officers and DFDs would need to be extraordinarily careful to follow the digital forensic principles when working and handling digital evidence, and have the utmost focus on quality both regarding the digital evidence and how reports are written. If not, there would be a strong risk of inducting evidence of low technical quality into the courts.

## 7 Future work

The scope of this thesis has been limited to having a technical focus. On the basis of the findings in this study, there are some elements that could be subject for further research:

Even though I have had legal education at the Norwegian Police University College, and have worked for years in the Norwegian Police Service, my legal competence is limited.

A study with a judicial focus on evidence evaluation with regard to the role of the prosecutor and the judiciary could bring further insight into the evidence evaluation process.

## References

1. Erlandsen TE. Verification of commercial automation in mobile forensics. [Specialized project - research assignment]. In press 2017.
2. Sunde N, Sunde IM. Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation 2017.
3. Rachlew A, Universitetet i Oslo Det juridiske f. Justisfeil ved politiets etterforskning : noen eksempler og forskningsbaserte mottiltak. Oslo: Det juridiske fakultet, Universitetet i Oslo; 2009.
4. Påtaleinstruksen.
5. Lov av 22. Mai 1981 om rettergangsmåten i straffesaker (Straffeprosessloven), (1981).
6. Myhrer T-G. Kvalitet i etterforskningen - Særlig om påtaleansvarliges rolle og betydning. 2015;1.
7. Politihøgskolen. studietilbud/etter--og-videreutdanning/utdanninger/juristutdanninger/obligatorisk-utdanning-for-nye-politijurister1/ 2019 [Available from: <https://www.phs.no/studietilbud/etter--og-videreutdanning/utdanninger/juristutdanninger/obligatorisk-utdanning-for-nye-politijurister1/>].
8. Bergen Ui. Studietilbud, master i rettsvitenskap 2019 [Available from: <https://www.uib.no/studier/MAJUR>].
9. Fredriksen S. Innføring i straffeprosess. Oslo: Gyldendal akademisk; 2006.
10. Bjerknes OT, Fahsing IA, Bergum U. Etterforskning : prinsipper, metoder og praksis. Bergen: Fagbokforl.; 2018.
11. Andersen S. Technical report: A preliminary Process Model for Investigation. 2019.
12. Henseler H, van Loenhout S. Educating judges, prosecutors and lawyers in the use of digital forensic experts. Digital Investigation. 2018;24(S):S76-S82.
13. Årnes A. Digital forensics. Hoboken, NJ: Wiley; 2018.
14. Carrier B. File system forensic analysis. Upper Saddle River, N.J: Addison-Wesley; 2005.
15. ACPO. Good Practice Guide for Digital Evidence. 2012.
16. Casey E. The increasing need for automation and validation in digital forensics. Digital Investigation. 2011;7(3):103-4.
17. Endicott-Popovsky B, Horowitz DJ. Unintended Consequences: Digital Evidence in Our Legal System. IEEE Security & Privacy. 2012;10(2):80-3.



18. Shaw A, Browne A. A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. *Digital Investigation*. 2013;10(2):116-28.
19. James JI, Gladyshev P. Challenges with Automation in Digital Forensic Investigations. 2013.
20. Horsman G. Tool testing and reliability issues in the field of digital forensics. *Digital Investigation* 2019. p. 163-75.
21. Guo Y, Slay J, Beckett J. Validation and verification of computer forensic software tools—Searching Function. *Digital Investigation*. 2009;6(S):S12-S22.
22. Casey E. The broadening horizons of digital investigation. *Digital Investigation*. 2017;21:1-2.
23. Daniel L, Daniel L. Web and Browser Caching-Chapter 31. *Internet History: Elsevier Inc.*; 2012. p. 213-8.
24. Sukwong O, Kim HS, Hoe JC. Commercial Antivirus Software Effectiveness: An Empirical Study. *Computer*. 2011;44(3):63-70.
25. Hadlund M-A, Jebens SE, Aarli R. *Bevis i straffesaker : utvalgte emner*. Oslo: Gyldendal juridisk; 2015.
26. Smith FC, Kenneally EE. Electronic evidence and digital forensics testimony in court. 2008. p. 103-32.
27. Kolflaath E. *Bevisbedømmelse i praksis*. Bergen: Fagbokforl.; 2013.
28. Hatlem R. *Kvaliteten på etterforskningen*. Oslo: Politihøgskolen, 2000; 2000. p. s. 81-106.
29. *Politiinstruksen, (1990)*.
30. *Politi-loven, (1995)*.
31. Bjerknes OT, Williksen E. *Politirapport*. 3. utgave 2012 ed: Forlaget Vett & Viten; 2012.
32. Kolflaath E. *Språk og argumentasjon - med eksempler fra juss*. Bergen: Fagbokforl.; 2004.
33. Casey E. Clearly conveying digital forensic results. *Digital Investigation*. 2018;24:1-3.
34. Casey E. The knowledge management gap in digital investigations. *Digital Investigation*. 2018;27:1-2.
35. Casey E. Differentiating the phases of digital investigations. *Digital Investigation*. 2016;19:A1-A3.
36. Casey E. Editorial - A smörgåsbord of digital evidence. *Digital Investigation*. 2017;23:1-2.
37. Casey E, Geradts Z, Nikkel B. Transdisciplinary strategies for digital investigation challenges. *Digital Investigation*. 2018;25:1-4.

38. Justice USDo. Digital evidence in the courtroom: A guide to law enforcement and the prosecutor. 2007.
39. Riksadvokaten. Kvalitetskrav til straffesaksbehandlingen i politiet og ved statsadvokatembetene mv. (Kvalitetsrundskrivet) nr. 3 / 2018. 2018.
40. Forst B. Errors of Justice : Nature, Sources and Remedies. Cambridge: Cambridge University Press; 2003.
41. Leedy PD, Ormrod JE. Practical research : planning and design. 11th ed. ed. Boston: Pearson; 2015.
42. Politihøgskolen. NCFI - Nordic Computer Forensic Investigator 2019 [Available from: <https://www.phs.no/studietilbud/etter--og-videreutdanning/utdanninger/etterforskning-og-kriminalteknikk/>].
43. Aaron A, Barbara E-P. Digital Evidence Education in Schools of Law. Journal of Digital Forensics, Security and Law. 2012;7(2):75-88.



# Appendices

**Appendix 1:** Verification of commercial automation in mobile forensics

**Appendix 2:** Informasjonsskriv

**Appendix 3:** Intervjuguide

**Appendix 4:** SCENARIO 1

**Appendix 5:** SCENARIO 1 - digitale spor

**Appendix 6:** SCENARIO 2

**Appendix 7:** SCENARIO 2 - Avhør

**Appendix 8:** SCENARIO 2 - analyserapport

**Appendix 9:** SCENARIO 2 - Bilderapport

**Appendix 10:** SCENARIO 3

**Appendix 11:** SCENARIO SPØRRESKJEMA

Appendix 1:

# Verification of commercial automation in mobile forensics



Tom Erik Erlandsen  
IMT4125 - NTNU  
01.06.2017

## Abstract

*The use of commercial automated forensic tools in mobile phone forensics are widespread. Because of later years' massive growth in digital evidence the automatically generated results from such tools are often reviewed by detectives without digital forensic knowledge, as digital investigators are being a hard-pressed commodity. This paper presents an empirical study that explores to what degree one commercial automated mobile forensic tool parse out and verify information from some of the most popular instant messaging smartphone applications in use today. The results of the study indicate that without further manual verification of output from an automated analysis, we risk missing out on potential evidential data, with the possible treat this could pose to the rule of law.*

# Table of contents

Abstract .....	1
1. Introduction .....	3
2. Related work .....	5
3. Method .....	11
3.1. Device setup: .....	11
3.2. Application setup:.....	12
3.3. Creation of user activity: .....	13
3.4. Mobile forensic tool: .....	14
3.5. Extraction procedure: .....	16
3.5.1. UFED extraction method Android – device A:.....	16
3.5.2. UFED extraction method iOS – device B:.....	16
3.6. Examination:.....	17
3.6.1. Automated analysis:.....	17
3.6.2. Manual analysis: .....	18
4. Results .....	18
4.1. Android.....	18
4.1.1. Facebook Messenger.....	18
4.1.2. Skype .....	19
4.1.3. WhatsApp .....	19
4.1.4. Kik .....	19
4.1.5. Snapchat.....	20
4.1.6. Viber .....	20
4.1.7. Instagram .....	20
4.2. iOS.....	21
4.2.1. Facebook Messenger.....	21
4.2.2. Skype .....	21
4.2.3. WhatsApp .....	21
4.2.4. Kik .....	21
4.2.5. Snapchat.....	22
4.2.6. Viber .....	22
4.2.7. Instagram .....	22
4.3. Summary .....	22
5. Discussion / Conclusion .....	23
6. Future work .....	25
List of references.....	26
Appendices.....	27

# 1. Introduction

The number of smartphone users in the world is forecast to precede 2.87 billion by 2020 (1), and with the increase in popularity of instant messaging applications on these devices, the estimated number of users of such applications are already over 2 billion globally (2).

With such massive numbers of users, devices and applications, an almost unimaginable number of instant messages are being generated and stored digitally on smartphones every day, and digital evidence from these devices are playing an increasingly important role in combatting crime all over the world. Due to the popularity of the smartphone, and the rapid evolving technology for these devices, the capabilities of the smartphone has closed the distance in performance to traditional computers for the normal user, often making smartphones the preferred digital device in daily use.

At the same time have the total growth in digital evidence pressed the need for some sort of automation of the digital forensic process (3). This has led to a larger portion of digital evidence being processed through commercial automated forensic tools, and the automatically tool generated reports often being reviewed by detectives without digital forensic training or background, saving both vital initial investigation time and digital forensic resources (4).

Even though automation of the digital forensic process may be the key in solving the challenges concerning the growth in digital evidence, we also need to uncover the potential challenges to verification when automating digital forensic analysis, and what effects this can have if not mitigated properly (5,6,7).

For better understanding the effects of automation, this report presents an empirical study that test the result of forensic automation and verification on smartphones with instant messaging applications installed without any post tool verification performed by a digital investigator, thereby studying the potential differences between automated tool results, manual analysis, and the documented user activity.

Any potential differences in output would then illustrate the risk of what an investigative service could be missing out on in an investigation, if the automated forensic tool results were reviewed by a detective without digital forensic knowledge, compared to a digital investigator.

So, to build on this, a research question was stated:



***"Will there be any deviations in the results from commercial automated mobile forensic tool analysis of instant messaging applications on smartphones versus manual analysis and verification?"***

This led to the research hypothesis:

***"There will not be any deviations in the result from commercial automated mobile forensic tool analysis versus manual analysis and verification."***

By identifying the independent variable as the analysis, the mediating variable as the level of verification, and the dependent variable as the analysis result, differentiating the level of verification by running automated and manual verification on the extracted images of test devices, the researcher would be able to measure the potential difference in effect on the analysis result, by this rejecting the no-deviancy hypothesis or not.

To present the limitations of the study, I needed to address the digital forensic process. This process can best be described as the way a digital investigation is structured, and include all steps performed. Anders Flaglien presents this process the following way (8, p. 28):

*"The digital forensic process supports a structured and sound investigation of digital evidence from any device capable of storing or processing data and information in a digital form".* Flaglien split the process into 5 steps:

#### **Identification – Collection – Examination – Analysis - Presentation**

These steps describe the identification of potential evidence sources, collection of these by forensic copying, the examination and pre-processing of collected data, analysing the data to identify important information, and then present the evidence in a report and / or in court. Even if this process can appear to be linear, it can be repetitive, depending on the findings during the process. This meaning the process can be rolled back to a previous step, and repeated, if new evidence is found during an investigation. The thought behind this is that by following the structure of the digital forensic process, good evidence integrity will be ensured.

This study seen in context of this framework, will limit itself to the analysis part of the digital forensic process, where the extracted and examined dataset from a smartphone are being run through an automated forensic tool analysis. There is no focus on access control, so test devices utilised in this study have not had this feature turned on. The study will also limit itself to the created user content of the instant messaging applications installed on the test devices, this being instant chat messages, picture and video attachments, and calls made through the applications. The study also only focused on the communication functions of the applications, not other potential features like

friend stories, feeds and so on. The study will not provide detailed description or mapping of artefacts or file paths from the instant messaging applications, or fully discuss deep decoding and/or interpretation of these artefacts. The study focuses on potential differences between findings obtained by automated tool analysis, actual user activity, and low level manual digital forensic interpretation of the tool created forensic image from a digital investigator. All recorded timestamps in the user activity documentation are recorded in dd/mm/yyyy hh:mm, so any time skew measured in seconds between smartphone, application, and recorded user activity will not be controlled for.

I organised this paper in the following way: In the **related work** section, some related work within the scope of my study are presented and reviewed, mainly concerning automation in digital forensics. In the **methods** section the synopsis of the study, the process concerning the setup of smartphones and instant messaging applications, the creation of user activity and the documentation of this, and the procedures and examinations performed, are presented. In the **results** section, the results of the automated forensic analysis are presented, and then compared against the documented user activity and the manual forensic analysis, which is reviewed and concluded on in the **discussion / conclusion** section. Some suggested future work based upon experiences made from this study are presented in the **future work** section.

## 2. Related work

Automated commercial forensic tools have been used in digital forensics for many years, but the output of these has traditionally been analysed by the digital investigator, reducing and interpreting the result further before presenting the output to detectives for reviewing, by this maximising investigative result and ensuring good forensic quality. The reason for choosing this approach has been that some findings from an automated analysis normally would need further tuning to be fully understandable for a detective with little or no digital forensic knowledge. Some forensic artefacts presented in an automated analysis report can have no obvious links to what the detectives are trying to uncover, making judging the potential evidential value of findings difficult (4,6).

However, with the growth in digital evidence, large datasets are making an impact on digital forensics, creating investigation backlogs, forcing the digital forensics community to seek out solutions to this problem. There are those who have advocated for mitigating this growth in digital evidence by implementing a triage solution (4,9-11).

Shaw and Brown point to the pros and cons of the triage approach (12). They define a triage in digital forensics as *"the practice of eliminating digital devices from the process*

*of forensic analysis, or simply prioritising the order in which devices are forensically examined, via administrative and/or technical means”.*

They present two different traditional approaches to triage, administrative- and technical triage. They describe the administrative triage as the process where cases or digital devices that are being considered for forensic examination, are measured against criteria set for examination. These criteria can be the seriousness of the crime investigated, or the level of likeliness that the digital device contains evidence based on tactical information. The digital evidence is then either rejected, or accepted for examination. Administrative triage can also involve the prioritisation of in which order cases and /or digital evidence are to be examined. The technical triage involves the use of commercial forensic triage tools, where these tools focuses on allocated files and other easily found artefacts on the digital evidence. An approach to a technical triage could then be to review the output these automated tools generate, trying to identify evidence. If something of potential evidential value is found, the digital device is accepted for full forensic examination.

Shaw and Brown however state that there are clear risks associated with personnel without digital forensic experience reviewing artefacts that might contain information without any clear links between the artefact and the evidence, and that examining such artefacts requires a high degree of digital forensics know-how (12). Their paper further present the primary concern of a triage to be that evidential data can be overlooked, or that the technical triage can be conducted by personnel with insufficient training or competence, hence potentially missing out on evidence. The counter-argument presented is that by performing full forensic examinations in all cases and on all digital evidence, the investigation backlogs would present a greater risk to the quality of an investigation than to perform a triage, due to the extended casework time frames such an approach would represent. The paper also discuss a solution to the problem of triage versus full examination, where they present an alternative to triage, which they refer to as “enhanced previewing”, where the digital evidence are being previewed in a forensically sound manner.

Mislan, Casey and Kessler addresses the need for on-scene triage of mobile devices to overcome the potential hindrances that the growing backlogs will have on investigations created by the increasing number of mobile devices submitted for analysis (13). They claim both more effective methods and tools are needed to solve this problem, and that there are limited existing tools and methods for performing on-scene triage work. The tools for performing such on-scene triage inspections of smartphones are often just rugged versions of automated mobile forensic tools. They also state that there are risks

that on-scene inspections only would give logical data, due to the nature of the tools and triage techniques used when performing on-scene triages.

Performing a technical triage of digital evidence in mobile forensics would then often normally either mean manually interacting with the evidence in original, which would change the integrity of the evidence, or connecting the smartphone to some sort of mobile on-scene triage unit, and browse through the logical volumes presented on the triage unit. This on-scene triage approach would still be dependent of the triage tool having programmed version support to be able to parse out applications. It would also require the smartphone to be turned on and open, since turning it on only for the sake of a triage would change the integrity of the evidence unnecessary. This approach would also either require a digital investigator on-scene to conduct the triage, or the triage would have to be performed by first-line police officers on-scene normally without digital forensic experience. With digital investigators already being a hard-pressed resource, and first-line police officers normally having inadequate training for performing a digital forensic triage at this level, this may present itself as a non-viable solution for most police services (4). Digital investigators are often organised in centralised forensic units, and the factor of geographical distances alone could rule out on-scene triages for all crime scenes, all the time the digital investigator then would be away from the digital forensics lab, further increasing the digital forensic backlogs. Hitchcock, Le-Khac and Scanlon points to the training of first-line personnel as a possible solution. They presented a model for digital field triage, where first-line personnel would receive basic digital forensic training (11). The personnel would not be dedicated to digital forensics, but would be able to conduct digital forensic triages, thereby relieving the digital investigators on-scene.

Others again point to automation as a necessary implementation in the digital forensic process, seeking big data solutions to mitigate the risk of backlogs. The Netherlands has put this automation into system, and since 2010 automated large parts of their initial processing of datasets. Van Baar, Van Beek and Van Eijk from the Netherlands Forensics Institute presents this concept in the article "*Digital Forensics as a Service: A game changer*" (4). In this concept, the digital investigator creates forensic copies of digital devices, and then copies them to a central storage, where the images are being processed automatically by multiple tools. The results can then be queried, reduced and analysed by detectives by logging on to the system. If any information of interest is found, they can then contact a digital investigator for further scrutiny of the evidence. This article reports this system to have reduced case backlogs, and freed up digital investigators. The article reports that detectives also have increased their technical understanding over time with this approach, further freeing time for the digital

investigators to conduct research. Good communication between the detectives and the digital investigators are mentioned as a prerequisite for this system to function properly.

With these different models for mitigating backlogs being dependent on increased resources of some sort, bringing the evidence into the lab and performing an acquisition of the mobile device with an automated mobile forensic tool, and then present an automated tool generated report of the findings for review to the analyst or detective without any further processing or scrutiny from the digital investigators part, would then often be the preferred and easier choice. This solution can be seen as a similar approach to the problem as the Dutch implementation of automation - digital forensics as a service, and the enhanced previewing presented by Shaw and Browne (3,12). The use of a commercial automated mobile forensic tool for both acquisition and report generating without further involvement from the digital investigator could thus be considered to be both automation and a sort of triage, where the detective would be the one reducing and triaging the digital evidence. This approach would be freeing time for the digital investigator, and at the same time satisfying strict time frames in criminal cases, giving the detectives and analysts material to work with faster.

With the growing need for automation to deal with the increase in evidence sources and huge datasets, an increased need for verification present itself.

Verification is defined by Guo, Slay and Beckett as a confirmation of validation with laboratory tools, techniques and procedures (14). Friheim states that the verification of tools when introducing automated interpretation of data is important, but due to rapid changing artefacts and applications, tool verification also should include comparison of the outcome of tools and the verification of results. He points further to the importance of using tools that uses different underlying engines when verifying and comparing forensic tools, and advocating that due to the transparency of open source tools, these can be of importance when performing dual tool verification (15).

Potential lack of competent manual verification of output from commercial forensic tools can affect the result of an investigation, by overlooking evidence not found by the automated analysis, and not uncovering false positives or incorrect interpretations (5). This would especially come to play in countries with no strong restrictions on the admissibility of digital evidence in court, like in the Norwegian legal system. The basic principle of free evidence admissibility is a central principle in the Norwegian legal system, where evidence rarely is dismissed, but evidence credibility is taken into the total consideration of evidence during the court proceedings (16-18). Under these circumstances, you could risk that mobile digital evidence that were imaged by a digital investigator, got reviewed by a detective without digital forensic experience, which again

could present the findings to the court as evidence without other verification than what the commercial automated mobile forensic tool had support for.

With regards to digital forensic tools and admissibility of digital evidence, Carrier addressed in 2002 the Daubert Test, used in connection with the judging the reliability of scientific evidence in United States courts, such as the output of a digital forensic tool (19). He mentions two categories of tests for ensuring that the tool produces viable results. The first category tests for false negatives, in other words tests that ensures that the tool produces all the available data from the input. The second category tests for false positives, tests that validates that the tool does not introduce new data. Carrier further introduces a preferred method for tool testing, the open method, where specific requirements for different digital forensic tools are set, and then tested. Carrier also advocate for the use of open source tools for testing.

James and Gladyshev discusses the challenges of automation in digital forensic investigations, and states that to approach the challenges of missed evidence due to automated processing of evidence, we need to know how good these automated digital forensic tools work (20). They also bring forward concerns of the trained digital investigator relying on highly automated tools over time may cause deterioration of knowledge, and that automated tools also may allow the untrained investigator to appear more knowledgeable. They further state:

*"If it can be assumed that the automation built into these tools is reliable – keyword list search, hash search, etc. – then there are really two challenges that remain: a reliance on the investigator to correctly run the automated tool and a reliance on an investigator, with possibly no knowledge of the data, to interpret the presented information."*

In my experience, most parties in the legal system and in the police service without digital forensics knowledge tend to have the impression that commercial automated mobile forensic tools deliver a complete forensic copy of the mobile device, with all installed applications fully parsed out, as seen on the device. This can potentially lead to wrong conclusions taken in the legal system, and could pose a threat to the credibility of digital evidence (7).

Casey points out concerns that while automated validation is a necessity for coping with the amount of digital evidence, there still will be a need for automated tools to provide the transparency needed for discovering errors and omissions, due to the inflexibility of automation (5). With the constant evolving landscape of new applications, smartphone system updates, and new version releases of applications, there is not possible for an automated mobile forensic tool to support interpretation of all third-party applications at any given time. The challenge of inflexibility has also been recognised by the people

behind the forensic tool Cellebrite, who has presented an implementation of what they call the SQLite wizard to their analysing tool – Physical Analyzer (21). The SQLite wizard is a SQLite database tool integrated into the Physical Analyzer that is meant to let the digital investigator build queries from both supported and non-supported databases, making it possible to perform manual decoding and verification of SQLite databases without exporting the databases out for verification using a third-party tool. That said, SQLite database forensics and queries can be considered being well beyond and above the normal competence level of a detective without extended digital forensic experience (4,22).

This study explores if we need to pay more attention to the inflexibility concerning automation of forensic analysis by measuring if potential decisive pieces of evidence residing in artefacts and databases are being uncovered and verified by automation or not (5).

## 3. Method

The synopsis of the study was set up by two smartphones with Android and iOS operating systems running, with seven of the most popular instant messaging applications on the market today installed, upon where I had created and documented user activity (23,24). The mobile devices were then imaged, processed and analysed with an automated mobile forensic tool. The results of the automatically generated tool analysis were then compared with the documented user activity and a manual forensic analysis of the image, and the findings presented.

The synopsis was constructed to illustrate a mobile device being run through an automated mobile forensic tool with the automated tool report being reviewed by a detective with no knowledge of digital forensics, compared to the result you would get with added manual forensic analysis from a digital investigator. Any potential differences in output would then illustrate potential evidential values we could risk missing out on in an investigation.

To be able to recreate automated analysis results from a commercial mobile forensic tool, an automated mobile forensic tool and smartphones with documented user activity were needed. The focus was on choosing popular, updated and renowned tools, smartphones and applications, for the research to be up to date and relevant.

### 3.1. Device setup:

A setup with two different smartphones was chosen, both with different operating systems from two of the most popular vendors, Apple and Samsung. Both devices were updated with the latest system updates to further ensure relevance of the study.

Test device A:

**Samsung S6 SM-G920F running Android 6.0.1**

Kernel version: 3.10.61-8826787

Build number: MMB29K.G920FXXU5DQB9

Test device B:

**iPhone 6 plus A1524 running iOS 10.3**

Model: MGAH2QN/A

Build number: 14E277



Since neither of the handsets were out-of-the-box new, and had been used for test purposes before, both handsets were updated with the latest system updates, and then a factory reset of both handsets were performed. This left both handsets with a clean installed and updated system environment. Since the research was limited to study automated tool analysis results of instant messaging applications, both handsets were set up with no access control. Both handsets were left with factory default setup.

### 3.2. Application setup:

7 applications were selected based on 4 criteria:

1. The application was available on both App Store and Google Play Store
2. The application had a chat function / instant messaging function
3. The application was one of the most popular used
4. The application had showed up in my investigations one time or another

Facebook own the two most popular messaging applications for smartphones in the world: 1. WhatsApp 700 million users and 2. Facebook Messenger 600 million users. In addition, Facebook also own the picture sharing application Instagram, which has around 600 million active users per December 2016 (23,24). Even if Instagram is defined as a social picture sharing app, it also has a chat function embedded in the application. The photo and video messaging app Snapchat can show a total of 150 million daily users pr June 2016, Skype 300 million users, Kik 200 million users, and Viber 250 million users (23,24). This would make up a total of 2.8 billion users of the different applications, making the selection relevant. With criteria for selecting applications set, the following applications were picked out, and installed on the test devices. All installations and applications were installed with default system setup from application vendor.

Samsung S6 - android 6.0.1:

Application:	Version:
Skype	7.44.0.215/534
Messenger	115.0.0.22.69
Instagram	10.18.0
Snapchat	10.7.1.0
Kik	11.17.0.362
WhatsApp	2.17.146
Viber	6.8.5

**Table 2: List of installed applications with version numbers on test device A.**

IPhone 6 plus - iOS 10.3:

Application:	Version:
Skype	6.34.0.105
Messenger	115.0
Instagram	10.19
Snapchat	10.5.0 Boo
Kik	11.15.0
WhatsApp	2.17.11
Viber	6.8.5

**Table 3: List of installed applications with version numbers on test device B.**

### 3.3. Creation of user activity:

To be able to see the results of an automated analysis, relevant user activity for the forensic tool to analyse were created.

By documenting the creation of user activity, the documentation could have the function of a control group when comparing results later, and Excel was used for recording the user activity. A 3-part system was chosen to solve the documentation problem, where each instant message would consist of 3 parts – the name of the application, a running number and the letter A or B, describing which unit had sent the message. For the application Skype, the structure of a message thread would look like this: Skype A1, Skype B1, Skype A2., and so forth. The timestamp of when the instant message was sent was documented beside the numbered message for the specific application. The "Skype A2" message could then be read as the message was sent with the application Skype, from unit A, message number 2.

To more accurately illustrate normal user behaviour, both pictures and videos were included into the generated user activity. Calls were also generated from the applications if this functionality was present for the specific application. To be able to track the recorded user history for non-text content, the structure of the 3-part system was implemented for these messages. For instance, if the generated message Skype A2 was a picture, the content of the picture would be the text Skype A2. And if the message Skype A2 was a video attachment or a video call, a video of the text Skype A2 would be recorded. If the message Skype A2 was phone call from the application were made, the text Skype A2 would be spoken out loud. This meant that in the case of the instant chat message, video / picture attachment, or phone- or video call, being recovered from a non-expected part of the forensic image, with no obvious link to the application, the message or content could then be traced back to both the specific handset, the specific application, and the specific documented timestamp for comparison. When recording timestamps in the user activity, seconds was not recorded. This because there was no practical way of recording this when creating user activity.

To attempt to account for potential journaling artefacts within the databases of the applications, a minimum of 40 instant messages from each unit was generated, so that the message threads per application would reach a total of 80 messages, by this potentially triggering the journaling artefacts.

### 3.4. Mobile forensic tool:

The choice of automated mobile forensic tool for producing an automated analysis result was decided by the fact that I only had access to one commercial tool on a daily basis – The Universal Forensic Extraction Device (UFED) Touch2 Ultimate and the UFED Physical Analyzer from Cellebrite. The tools from Cellebrite are considered to be market leader, and are distributed in over 200 000 units all over the world. The tools have been voted the forensic4:cast award winner 8 consecutive years up to 2016 by the digital forensic community, also being nominated in the upcoming 2017 vote, for delivering the best mobile forensic software and hardware on the market, so I felt the forced choice of tool would not weaken the study (25). Cellebrite UFED is also my choice of tool in mobile forensics, and I have used it on a daily basis since 2009. My impression of both the tool performance and the frequency of new releases are very good.

At the time of the research, the Cellebrite installations were as follows:

Cellebrite tool:	Version:
UFED Touch 2 Ultimate	6.1 (March 2017)
UFED Physical Analyzer	6.1.6.19 (April 2017)

**Table 4: Installed Cellebrite mobile forensic tools with version number used.**

The Cellebrite tool series are set up with the UFED Touch 2 performing the imaging or extraction of data from the mobile device, while the UFED Physical Analyzer (PA) performs the automated analysis, interpretation and presentation of the data on the image file extracted by the UFED Touch2. The investigator can then generate automated reports from the PA tool (26).

The PA has also built in possibilities for conducting deeper manual analysis of non-supported mobile applications before report generation. The digital investigator can run python scripts against the automated analysis results, and there is also a hex viewer and a SQLite database tool for deeper analysis.

I am also a Cellebrite certified physical analyst, a certification Cellebrite describe as (26):

*"an advanced level certification that certifies participants have gained knowledge and practical skills using UFED Physical Analyzer software conduct advanced analysis on mobile devices, including advanced search and analysis techniques to verify and validate*

*findings. This class will also introduce students how to generate reports on technical findings."*

Me being tool certified by the vendor of the tool, further strengthened my study, minimising the chance of wrong use of the tool, that could lead to the tool potentially reporting false findings. Given the limitations of my study, with the focus of illustrating the result of an automated analysis with no further review from a digital investigator, the implemented tools for manual analysis were not utilised in this study. Both the UFED Touch2 Ultimate and the UFED PA were updated to the latest software version releases at the time of the research, to further add to the strength and relevance of the study.

Both test devices were listed as supported by Cellebrite UFED, and all the selected applications were also listed as supported for the test handsets in the list of supported devices. In addition to the supported device list, Cellebrite also has released lists of which versions of the supported applications that they have verified are supported, cross-checked with the operating system versions of the supported devices (27,28). When I cross-checked the versions of the selected and installed applications, and correlated this to the lists of supported devices and applications from Cellebrite, I was able to make two tables listing which of the applications Cellebrite had verified support for:

Verified supported decoding of applications UFED Physical Analyzer version 6.0 (Jan 2017):

iOS	Verified:	PA	Android	Verified:	PA
Skype	-	--	Skype	-	-
Messenger	-	-	Messenger	-	-
Instagram	Yes	3.07	Instagram	-	-
Snapchat	-	-	Snapchat	-	-
Kik	-	-	Kik	-	-
WhatsApp	-	-	WhatsApp	-	-
Viber	-	.	Viber	-	-

**Table 5: Cellebrite verified decoding of applications UFED Physical Analyzer version 6.0.**

Verified supported decoding of applications UFED Physical Analyzer version 6.2 (May 2017):

iOS	Verified:	PA	Android	Verified:	PA
Skype	-	-	Skype	-	-
Messenger	Yes	-	Messenger	-	-
Instagram	-	-	Instagram	-	-
Snapchat	Yes	3.7	Snapchat	-	-
Kik	Yes	3.5	Kik	-	-
WhatsApp	Yes	-	WhatsApp	Yes	-
Viber	-	-	Viber	-	-

**Table 6: Cellebrite verified decoding of applications UFED Physical Analyzer version 6.2.**

I was not able to find any list over supported applications for PA version 6.1. I only found lists for versions 6.0 and 6.2. The lists from Cellebrite did not further explain any values or interpretations found in the lists, so I found these lists giving me little or no oversight over actual support.

## 3.5. Extraction procedure:

### 3.5.1. UFED extraction method Android – device A:

Cellebrite lists the physical extraction method as available for the test device A – Samsung S6 SM-G920F, and given this extraction method gives us a raw data image of test device A, this method was selected by using the forensic recovery partition option, and imaged the test device A.

Cellebrite list out an explanation of what a physical extraction with UFED Touch 2 is (26):

*"Physical Extraction- For devices supported in this category, the Cellebrite UFED 4PC/Touch Ultimate will use advanced methods to extract a physical image of the flash memory or address range of a device, including unallocated space. Unlike conventional logical extraction processes, the physical extraction method bypasses the phone's operating system, acquiring the data directly from the phone's internal flash memory. Unallocated space may contain access to deleted items such as SMS, Call logs, Phonebook entries, Pictures, and Video. Support for data types automatically decoded are marked for each device. Additional decoding for new content types will be constantly updated with each new UFED 4PC/Touch Ultimate release. Search tools built into the UFED Physical Analyzer tool can be used to manually search for content types such as SMS messages, for devices not yet supported for automatic decoding (see 'find' feature in UFED 4PC/Ultimate manual)."*

### 3.5.2. UFED extraction method iOS – device B:

It was not possible to extract the raw physical data image from the test device B due to the encrypted secure boot chain of iOS devices (29). This meant there was not any possibility for extracting the physical image of the iPhone test device.

The UFED Touch 2 Ultimate presented the following options for extraction data from the open access iPhone 6 plus:

#### **7.1.1.1 Logical extraction:**

The Cellebrite UFED Touch 2 manual describes this as a quick extraction method that supports most mobile devices. The artefacts that can be extracted from a source unit ranges from call logs, phone contacts, SMS, calendar events, multimedia files (images,

video, audio) and application data. They also explain that the range of extracted data can differentiate depending on the version and model of the source unit. In most cases, there will not be possible to perform a logical extraction on locked units (26,30).

#### **7.1.1.2 File system extraction:**

The Cellebrite UFED Touch 2 manual describe this extraction as collection of files from the source unit memory, and that the file system can contain hidden system files that will not be visible in a logical extraction. They state that the user can get access to all files residing in memory, including images, videos, databases, system files and logs, and that most of the applications store their data in databases (26,30).

#### **7.1.1.3 FULL file system extraction (CAIS):**

This option of extracting what Cellebrite defines as the full filesystem was only available through Cellebrite Advanced Investigative Services (CAIS). It is not clear what Cellebrite state is the difference between a file system and a full file system extraction, other than "further filesystem access" was given when choosing the full file system extraction. In addition to the full filesystem option, CAIS also provide unlocking and extraction of some iPhone and iPad models, in addition to unlocking and decrypted physical extraction of a range of Samsung models. To use this service the investigator have to fill out an online form, and request details about this service. The use of this service also includes in many cases to send the digital evidence to the Cellebrite lab (26,30). With the full iOS filesystem extraction method being a part of this service, I did not have this option available.

The best option for extracting data from the iPhone was then first to use the file system extraction method, and then further adding a logical extraction, combining the 2 extractions into a "Multi-project extraction" using the UFED PA, seeing both extractions as one. These extraction methods were selected, and the acquisition and extraction was performed.

### **3.6. Examination:**

#### **3.6.1. Automated analysis:**

For the automated analysis of the two test devices, I used the UFED Physical Analyzer v. 6.1.6.19 (PA).

The PA was executed, and the multi-project opened from the combining of extractions. When opening the extractions, the PA runs parsers against the extraction, eventually presenting the extractions in a easy to use graphical user interface (GUI). Within this GUI the investigator can search for evidence, and select files of interest. The investigator can

then generate reports, either selecting the total extraction or selected parts of the extraction. The PA then automatically write out a report on the selected content. Due to the scope of this study, fully automated reports without any investigator interaction were generated. These reports were then opened, and results extracted and compared to the recorded user activity.

### 3.6.2. Manual analysis:

When conducting the manual analysis, I used the open source tools "Autopsy" version 4.0.0 and "DB Browser for SQLite" version 3.9.1. I also used the tool HexEdit version 4.0 (31-33).

Even if the focus was not on using open source third-party applications only, but to research the difference in output with or without digital investigator interaction illustrating automation with or without further digital investigator interpretation, open source tools were used to strengthen the study. The UFED PA was not used for other purposes than source database comparison between the open source tools and the UFED PA. The analysis was conducted by opening the source extractions from UFED in Autopsy, and then exporting the application SQLite databases out for further SQLite queries with DB Browser for SQLite. The findings were then exported into Excel for comparison with the automated results and the recorded user activity. Pictures and videos was manually searched for, when not located through the chats.

Potential findings of images / videos / audio in original was not included in the exported Excel findings, but a file path to the image / video was provided if a link to the chat threads could be made.

## 4. Results

### 4.1. Android

#### 4.1.1. Facebook Messenger

##### **7.1.1.4 Automated results:**

No results from the automated analysis.

##### **7.1.1.5 Manual results:**

The manual analysis was able to recreate all the instant messages from querying the SQLite database *USERDATA/Root/data/com.facebook.orca/databases/threads\_db2*, but was not able to connect attached media files to the chat.

## 4.1.2.Skype

### **7.1.1.6 Automated results:**

All chat messages parsed out, but no media attachments. Calls made from application was found in call history.

### **7.1.1.7 Manual results:**

The analysis parsed out the chat messages by extracting the *main.db* database found in *USERDATA/Root/data/com.skype.raider/files/live#3ab8277146e7b08f58/*, and it was scrutinized in DB browser for SQLite. The analysis was not able to recreate media attachments. Calls made from application was found in the call history.

## 4.1.3.WhatsApp

### **7.1.1.8 Automated results:**

All chat messages parsed out with correct timestamps and multimedia attachments. Calls found in call history, and there was possible to differentiate between calls and video calls.

### **7.1.1.9 Manual results:**

The manual analysis parsed out all chat messages with correct timestamps and multimedia attachments. Calls found in call history tab, and there was possible to differentiate between calls and video calls.

Chat messages was parsed out from: *USERDATA/Root/data/com.whatsapp/databases/msgstore.db*, and scrutinized with Autopsy and DB SQLite browser. The media files were parsed from *USERDATA/Root/media/0/Media/WhatsApp\_Images/Sent/* and videos from *USERDATA/Root/media/0/Media/WhatsApp\_Video/*. It was possible to link the media files to the chat thread.

## 4.1.4.Kik

### **7.1.1.10 Automated results:**

All chat messages parsed and images from chat parsed out. Videos were not parsed out by the automated analysis, only showing thumbnails of the videos.

### **7.1.1.11 Manual results:**

The manual analysis was able to recreate the chat messages by parsing out the information from */Root/data/kik.android/databases/7788e857-15f1-4361-81a1-7ad95f1e6bd3.kikDatabase.db* using DB browser for SQLite. The analysis linked videos to the chat by locating the filenames of the videos from



the <content\_id> in the messages table. The videos were then located in *USERDATA/Root/media/0/Kik/<filename>*. This was not done by the automated analysis.

#### 4.1.5.Snapchat

##### **7.1.1.12 Automated results:**

The automated results recovered a lot more traces of snapchats than the manual analysis did, mostly showing timestamps and partly user contact, but no content. Of the recreated user content that was readable, the analysis found chat message snap b 38 sendt as chat with correct timestamp.

##### **7.1.1.13 Manual results:**

The manual analysis recreated a total of 7 messages, but no content except for the snap b 38 chat. This was exported out the database from:

*USERDATA/Root/data/com.snapchat.android./databases/tcspahn.db*, and scrutinized with DB browser.

#### 4.1.6.Viber

##### **7.1.1.14 Automated results:**

The automated analysis parsed out all chat messages and all image media attachments, but only presented image thumbnails of the videos in the chat thread. All timestamps correct. Calls made from application was found in call history tab, but it was not possible to differentiate between calls and video calls.

##### **7.1.1.15 Manual results:**

The manual analysis showed the same result as the automated by extracting the viber\_messages database from *USERDATA/Root/data/com.viber.voip/databases/*, and in addition it managed to recreate videos and link them to the chat by parsing out the <extra\_uri> from the database <messages> from the table with the filename of the video found in *USERDATA/Root/media/0/viber/media/Viber Videos/<filename from extra uri field>*. This was not done by the automated analysis.

#### 4.1.7.Instagram

##### **7.1.1.16 Automated results:**

No results from the automated analysis.

##### **7.1.1.17 Manual results:**

The analysis recreated 20 of the chat messages by exporting the database from *USERDATA/root/data/com.instagram.android/direct.db*, and scrutinizing it with Autopsy and DB SQLite browser. This was messages A31 to B40, meaning the first 30 messages did not get parsed out.

The analysis also linked picture A32 and video A35 to the chat, and locating the media files in */data7user/0/com.instagram.android/cache/original\_images/<direct\_temp\_video>* and *<direct\_temp\_photo>*. The message insta A1 was located when the *direct.db-journal* database was scrutinized with hex editor, but this was not recorded as a find due to difficulties interpreting the file information, possible due to journaling overwrite artefacts within the *direct.db-journal*.

## 4.2. iOS

### 4.2.1. Facebook Messenger

No results from both automated and manual analysis.

### 4.2.2. Skype

No results from both automated and manual analysis.

### 4.2.3. WhatsApp

#### **7.1.1.18 Automated results:**

All chat messages parsed out with correct timestamps and multimedia attachments. Calls found in call history tab, and there was possible to differentiate between calls and video.

#### **7.1.1.19 Manual results:**

All chat messages parsed out with correct timestamps and multimedia attachments. Calls found in call history tab, and there was possible to differentiate between calls and video.

Chat messages parsed out from: */Applications/group.net.whatsapp.WhatsApp.shared/ChatStorage.sqlite*, and scrutinized with Autopsy and DB SQLite browser. The media files were parsed from */Applications/net.whatsapp.WhatsApp/Library/Media/*. It was possible to link the media files to the chat thread.

### 4.2.4. Kik

#### **7.1.1.20 Automated results:**

All the chat messages including multimedia attachments were parsed out with correct timestamps. Calls made from the application were found in the call history tab.

#### **7.1.1.21 Manual results:**

All the chat messages including multimedia attachments were parsed out with correct timestamps. Calls made from the application were found in the **call *history.db***. The database used for parsing out the information was located in:

`/Applications/group.com.kik.chat/cores/private/ae2ebe137a16412da455c9f2d3130d29/kik.sqlite`, and scrutinized with Autopsy and DB SQLite browser.

The multimedia files were found in `/Applications/group.com.kik.chat/cores/private/ae2ebe137a16412da455c9f2d3130d29/content_manager/data_cache/<filename>`, and linked to the chat thread.

#### **4.2.5.Snapchat**

No results from both automated and manual analysis.

#### **4.2.6.Viber**

#### **7.1.1.22 Automated results:**

All the chat messages were parsed out with correct timestamps. Multimedia attachments that were sent from device B were not recovered by the tool, all other multimedia attachments were recovered. Calls made from the application were recovered from the call history tab, but it was not possible to see if the call was a video call or not.

#### **7.1.1.23 Manual results:**

Same results as automated. The analysis was performed by extracting the ***Contacts.data*** database from `/Applications/group.viber.share.container/`, and scrutinized with Autopsy and DB SQLite browser.

#### **4.2.7.Instagram**

No results from both automated and manual analysis.

### **4.3. Summary**

Apart from snapchat, the manual analysis parsed out more complete result than the automated analysis. The automated analysis did not parse out any results from Messenger or Instagram, while the manual analysis parsed out the complete chat thread from Messenger, and a partial chat thread from Instagram from the Android device. The media attachments were not parsed completely by the manual analysis. Android was parsed put significantly better than iOS, with the tool parsing out only 4 of 7 iOS applications. This can be explained with Cellebrite not being able to extract a physical image due to the encrypted boot chain of iOS devices (29), as opposed to the Android system. Of all recorded timestamps, the analysis found 24 errors. All the errors were within 1 minute of the recorded timestamp. Of the

timestamps that were documented from the datasets with seconds, all the errors were within seconds of the timestamp changing minute.

## 5. Discussion / Conclusion

The focus of this study was to test the effects of commercial automation and verification on smartphones, by differentiating the level of automation and verification added to the analysis.

There were substantial deviances in the results from the automated mobile forensic tool analysis versus the manual analysis and verification, with more and better results being presented by the manual analysis, thereby rejecting the no-deviancy hypothesis.

No false positives were discovered in the recovered chat messages, timestamps or media attachments. The 1-minute timestamp errors can be explained with natural time skew between devices and the recording computer, and human error /delay.

There were however discovered some false negatives by the manual analysis. In the case potential decisive information resided in just these chat messages that were not parsed out, the investigation could miss important information that could have affected the final product of an investigation. Manually parsing out the test devices was quite labour intensive, and took a lot of time. If every digital evidence was to be parsed out manually, the complexity of this process alone would increase the chance of wrong interpretations, so automation in digital forensics is a necessity to cope with large datasets. Automation should however be implemented with the knowledge that commercial automated mobile forensic tools, with or without manual verification, do not parse out all content residing in a smartphone. This knowledge needs to be taken into consideration when organising digital forensic work, and when previewing and reviewing digital evidence.

To identify potential biases that could affected the outcome of the study, I will state that I have been using Cellebrite tools since 2009, and is certified as a Cellebrite certified physical analyst - CCPA - by Cellebrite with this tool. I have also attended Cellebrite sponsored user forums, and have an overall good experience from using the tool. This can however also strengthen the study, mitigating the risk for wrong use of the tool. When addressing the potential weaknesses of the study, none of the test devices was out-of-the-box new smartphones, making it possible that earlier traces of user activity could be present. This would especially apply to android due to the Physical extraction performed on the android Samsung test device A. This was mitigated by the structure of the messages. Only one commercial mobile forensic tool was tested, and adding more tools would have strengthened the study. I attempted mitigating this by ensuring that the mobile forensic tool software was fully updated with the latest system and tool releases, strengthening the relevance of the tool. My level of knowledge on manual analysis of artefacts and

databases within Android and iOS devices could also affected the outcome of the study, if the knowledge level was inadequate. The limitations of the study however stated that deep decoding of databases would not be discussed, and my experience with mobile forensics include decoding artefacts from iOS and Android mobile devices.

With automation used without manual verification like illustrated in this study, there would not be any possibility for rolling back steps in the digital forensic process, repeating the steps necessary for parsing out potential new discovered traces. The use of automated analysis tools in digital forensics are a necessity and of very good use. The automated tools cannot be seen as a challenge in itself, but rather the use of automation without verification. Few if any digital forensic tools can interpret every digital artefact, and automating the digital forensic process without proper verification, has risks that need to be taken into consideration when organising digital forensic work.

## 6. Future work

Makeev, Timofeev, Afonin and Gubanov argue for the low-level forensic analysis of SQLite databases (22), due to the popularity of SQLite databases both for iOS and Android devices, and multiple instant messaging applications. They mention that forensic analysis of SQLite databases often consists of only reviewing the database file in a database browser. In their article, they also examine the features write ahead log (db.wal), free lists and unallocated space of the SQLite database engine. Carving and recovering deleted SQLite databases from unallocated space on a mobile device will not be possible due to the use of MMC memory in these devices, but all is not lost. A SQLite database consists of pages of fixed size, and the size of these pages are specified in the header of the file. Some of these pages stores data, and others are unused. The unused pages of these databases are stored in free lists, and when information is deleted from the database, pages are put into these free lists, ready for reusing. In other words, there can be deleted information to be found inside of these free lists if the database vacuum service is not activated.

They also discuss the forensic value of the WAL file, the write-ahead-log. This file can be seen with the naming convention <database name>.db-wal. This file has a kind of opposite journaling function, that stores new changes to the SQLite database before they are written, protecting the main database. The database will read from the write ahead log instead of using the main database until the changes are written to the main database automatically when the WAL reaches its pre-set roll-over limit, default 1000 pages. Due to the potential size of the WAL, the write ahead log can contain huge amounts of potential important information, and should be forensically scrutinized as standard.

I would propose that future work study the possibilities of verifying if the different journaling databases are being parsed out by automated mobile forensic tools, and / or recovering free lists.

Future work should also implement verification of the output from the SQLite tool implemented in the UFED Physical Analyzer, and those of other commercial mobile forensic tools on the market.

## List of references

1. <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>
2. Darren Quick, Kim-Kwang Raymond Choo, Impacts of increasing volume of digital forensic data: A survey and future research challenges, *Digital Investigation*, Volume 11, Issue 4, December 2014, Pages 273-294
3. Van Baar R.B, Van Beek H.M.A, Van Eijk E.J. Digital Forensics as a Service, *Digital Investigation* 11, (2014), pp. 54-62
4. Casey E, editorial, *Digital Investigation*, Volume 7, Issues 3-4, April 2011, Pages 103-104
5. James J, Gladyshev P. Challenges with Automation in Digital Forensic Investigations. 2013, arXiv:1303.4498v1[cs.CY]
6. Endicott-Popovsky B, Horowitz D.J. Unintended Consequences: Digital Evidence in Our Legal System. *IEEE Security & Privacy*, March-April 2012, Vol.10(2), pp.80-83
7. Årnes A. *Digital Forensics*, 2015, pp. 43-67
8. Lillis D, Becker B, O'Sullivan T, Scanlon M. Current Challenges and Future Research Areas for Digital Forensic Investigation, <https://arxiv.org/abs/1604.03850>
9. Darren Quick, Kim-Kwang Raymond Choo, Impacts of increasing volume of digital forensic data: A survey and future research challenges, *Digital Investigation*, Volume 11, Issue 4, December 2014, Pages 273-294
10. Ben Hitchcock, Nhien-An Le-Khac, Mark Scanlon, Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists, *Digital Investigation*, Volume 16, Supplement, 29 March 2016, Pages S75-S85
11. Shaw A, Browne A, A practical and robust approach to coping with large volumes of data submitted for digital forensic examination, *Digital Investigation*, September 2013, Vol.10(2), pp.116-128
12. Mislan R, Casey E, Kessler G. The growing need for on-scene triage of mobile devices, *Digital Investigation*, 2010, Volume 6(3), pp.112-124
13. Yinghua Guo, Jill Slay, Jason Beckett, Validation and verification of computer forensic software tools—Searching Function, *Digital Investigation*, Volume 6, Supplement, September 2009, Pages S12-S22
14. Friheim I. Practical use of dual tool verification in computer forensics. School of Computer Science and Informatics, University College Dublin, 2016. Thesis.
15. Høyesterettsdom. *Rettstidende* 1990, p. 1010. Norwegian.
16. Høyesterettsdom. *Rettstidende* 2002, p. 1744. Norwegian.
17. Høyesterettsdom. *Rettstidende* 1998, p. 1386. Norwegian.
18. Carrier, Brian. Open source digital forensics tools: The legal argument. stake, 2002.
19. James J, Gladyshev P. Challenges with Automation in Digital Forensic Investigations. 2013, arXiv:1303.4498v1[cs.CY]
20. <http://blog.cellebrite.com/blog/category/cellebrite-ufed/>
21. Makeev D, Timofeev N, Afonin O, Gubanov Y. Forensic Analysis of SQLite Databases: Free Lists, Write Ahead Log, Unallocated Space and Carving. *D F I News* 2015 Mar 17.
22. <https://www.statista.com/topics/1523/mobile-messenger-apps/>
23. <http://www.quytech.com/blog/most-popular-messaging-apps-country-wise/>
24. <https://forensic4cast.com/2016/06/forensic-4cast-awards-2016-results/#comment-262278>
25. <https://www.cellebrite.com>
26. [https://my.cellebrite.com/client/app/ui/#/downloads/UFED Supported Devices 6.2 \(May. 2017\)](https://my.cellebrite.com/client/app/ui/#/downloads/UFED_Supported_Devices_6.2_(May_2017))
27. [https://my.cellebrite.com/client/app/ui/#/downloads/UFED Supported Apps 6.0 \(Jan 17\)](https://my.cellebrite.com/client/app/ui/#/downloads/UFED_Supported_Apps_6.0_(Jan_17))
28. [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf)
29. [https://my.cellebrite.com/client/app/ui/#/downloads/UFED Touch2 PDF Manual 6.2 Eng \(May 17\)](https://my.cellebrite.com/client/app/ui/#/downloads/UFED_Touch2_PDF_Manual_6.2_Eng_(May_17))
30. <https://www.sleuthkit.org/autopsy/>
31. <http://sqlitebrowser.org>
32. <http://www.hexedit.com>

## Appendices

Appendix A:	User activity Messenger
Appendix B:	Android Messenger results
Appendix C:	User activity Instagram
Appendix D:	Android Instagram results
Appendix E:	User activity Snapchat
Appendix F:	Android Snapchat results
Appendix G:	User activity Kik
Appendix H:	Android Kik results
Appendix I:	iOS Kik results
Appendix J:	User activity WhatsApp
Appendix K:	Android WhatsApp results
Appendix L:	iOS WhatsApp results
Appendix M:	User activity Skype
Appendix N:	Android Skype results
Appendix O:	User activity Viber
Appendix P:	Android Viber results
Appendix Q:	iOS Viber results



Appendix 2:



## INFORMASJONSSKRIV

Forespørsel om deltakelse i forskningsprosjektet:

### **«Fallacies when evaluating digital evidence among prosecutors in the Norwegian Police Service»**

*Masteroppgave v/ Tom Erik Erlandsen*

#### Formål

Politijuristen har en viktig rolle som en garantist for god kvalitet i etterforskningen. Ettersom digitale bevis i økende grad blir en del av bevisbildet i straffesaker, vil det derfor være interessant å se nærmere på hvordan digitale bevis blir oppfattet og vurdert av politijuristen. Informantene er politijurister i norsk politi.

#### Hvem er ansvarlig for forskningsprosjektet?

Norges teknisk-naturvitenskapelige universitet (NTNU) – ved fakultet for informasjonsteknologi og elektroteknikk (IE), institutt for informasjonssikkerhet og kommunikasjonsteknologi - er ansvarlig for forskningsprosjektet. Politihøgskolen er en samarbeidspartner.

#### Hvorfor får du spørsmål om å delta?

Du får spørsmål om å delta gjennom din rolle som politijurist i norsk politi.

#### Hva innebærer det for deg å delta i studien?

Studien blir gjennomført som en saksstudie. Informantene vil få presentert fiktive scenarier som innbefatter fiktive digitale bevis, som de deretter skal ta stilling til. Etter dette vil det bli stilt utfyllende spørsmål knyttet til vurdering av digitale bevis, hvor svarene blir registrert på et spørreskjema av intervjuer. Sakstudien vil gjennomføres som et enkeltvis intervju med hver informant, og varigheten vil være fra 30 minutter til 1 time pr. deltaker. Intervjuene vil ikke bli tatt opp på lyd, og verken navn, alder, kjønn, erfaring eller arbeidssted vil bli registrert eller kommentert, ut over at informanten er ansatt som politijurist i norsk politi.

#### Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Dersom du kan tenke deg å delta i studien, så kan du ta kontakt med meg på tlf. 924 10 257 (*Tom Erik Erlandsen*). Min veileder er professor Katrin Franke, NTNU, tlf.902 15 425, og Rune Nordvik ved Politihøgskolen, tlf. 952 01 803.

#### Personvern

Ingen personopplysninger om deltakerne vil bli registrert, og det vil heller ikke bli gitt beskrivelser av person eller arbeid i intervjudataene. Informantene vil dermed være

fullstendig anonymisert. Alt av innsamlet materiale blir slettet når forskningsprosjektet er ferdigstilt.

### Godkjenninger

Det er innhentet godkjenning til å gjennomføre studien fra politimesteren i informantenes politidistrikter. Godkjenningen ligger vedlagt.

*Med hilsen*

*Tom Erik Erlandsen*

# INTERVJUGUIDE:

## Formalia

Intervjuer informerer informanten om faktorer ved forskningen, personvern og samtykke. Samtidig overleveres kopi av informasjonsskrivet til informanten. Deretter spørres det etter muntlig samtykke, som registreres på svarskjemaet av intervjuer.

## Innledning

Forklare fremgangsmåten for studien. Informanten anmodes om å svare sannferdig, og om å vurdere informasjonen som blir fremlagt som en ekte sak.

Informanten får overlevert 3 scenario av ulik karakter, ett og ett. Noen av scenarioene kan inneholde rapporter som presenterer opplysninger i det enkelte scenario. Etter hvert scenario vil intervjuer stille 2 spørsmål, som registreres ved at intervjuer noterer ned svarene på svarskjemaet. Etter at alle 3 scenario er gjennomgått, stilles det ytterligere 20 spørsmål fra spørreskjema. Intervjuer registrerer svarene ved å notere disse ned på svarskjemaet.

## Scenario 1

Legge frem og presentere scenario for informanten.

Deretter legge frem rapport om digitale spor.

Har informanten spørsmål til scenario eller rapporter som blir fremlagt, så besvares disse etter mal – svar til scenario 1.

Intervjuer stiller deretter spørsmål til scenario, og notere svarene på svarskjemaet.

## Scenario 2

Legge frem scenario og presentere scenario for informanten.

Deretter legge frem analyserapport, bilderapport og avhør.

Har informanten spørsmål til scenario eller rapporter som blir fremlagt, så besvares disse etter mal – svar til scenario 2.

Intervjuer stiller deretter spørsmål til scenario, og notere svarene på svarskjemaet.

## Scenario 3

Legge frem og presentere scenario 3 for informanten. Scenarioet presenteres muntlig for å spille inn rollen påtalejuristen har som jourhavende.

Intervjuer stiller spørsmål til scenario, å notere svarene på svarskjemaet.

## Spørreskjema

Informanten får overlevert kopi av spørreskjema.

Intervjuer stiller spørsmål fra spørreskjemaet, og notere svarene på svarskjemaet.

## Avslutning

Informanten spørres om han / hun har noen spørsmål eller kommentarer til gjennomføringen. Hvis kommentarer, så registreres disse på svarskjema.

Appendix 4:

# SCENARIO 1:

---

«Påkjørsel i gangfelt, veitrafikkloven §3»

## Bakgrunnsinformasjon:

Tirsdag 2. april 2019 kl. 16:09 kjørte Marte Kirkemo til jobb i sin eldre BMW. På vei gjennom sentrum av Lillevik, like ved Lillevik Jernbanestasjon, så kjørte Marte Kirkemo på Peder Ås, med den følge at Peder Ås fikk påvist 2 alvorlige brudd i høyre ben. Marte Kirkemo ringte med en gang til 113 for å tilkalle ambulanse.

## Rapport om veitrafikkuhell ga følgende faktaopplysninger:

Fartsbegrensningen på stedet for ulykken var skiltet til 50 km/t, tettbebygd strøk.

Vær- og føreforhold var gode, tørr / bar vei, 15 grader pluss.

Ingen bremsespor i asfalten.

Lysforholdene var gode, daglys.

Ikke blendende sollys / lavt lys.

Ingen spesielle forhold ved kjøretøyet. Det var ikke installert hands-free system for telefon i bilen.

Godt merket og skiltet fotgjengerfelt.

Ingen utslag eller mistanke om ruskjøring, og siktede hadde gyldig førerkort for klasse B.

## Vitneopplysninger:

**Vitnet 1** forklarte at han ikke hadde observert selve ulykken, men at han kom til stedet like etterpå. Han bistod med å ta vare på Peder Ås som hadde store smerter fram til ambulansen ankom. Vitnet forklarte videre at det ikke var noen stor overraskelse at nettopp Marte Kirkemo var involvert i en slik påkjørsel. Det var en kjent sak i Lillevik at Marte Kirkemo var aktiv på Snapchat, også når hun kjørte bil. Det hadde han selv også tidligere observert, både ved at han har mottatt meldinger på Snapchat fra siktede, og at han hadde sett at hun hadde fiklet med telefonen når hun kjørte ved tidligere anledninger. Hun hadde ofte lagt ut videoer av at hun kjørte på Snap-storyen sin.

**Vitnet 2** forklarte at farten hadde vært lav, han anslo farten å være ca. 40-50 km/t. Han forklarte videre at fornærmede ble påkjørt midt i gangfeltet, og at bilen ikke senket farten eller forsøkte noen unna manøver før påkjørselen. Det kunne se ut som om føreren av bilen rett og slett ikke så fornærmede i det han gikk over gangfeltet, og kjørte på Peder Ås som om skulle ha vært «usynlig». Han kunne ikke se om siktede var opptatt med mobiltelefonbruk på eller like før ulykkestidspunktet, men at det i alle fall ville ha forklart hvorfor bilen ikke forsøkte å bremse eller foreta en unna-manøver.

Med bakgrunn i vitneopplysningene fra vitnet 1, ble mobiltelefonen til siktede tatt i beslag av patruljen på stedet.

#### Avhør av siktede:

Siktede forklarte at hun kom kjørende gjennom sentrum i Lillevik. Da siktede kjørte forbi fotgjengerfeltet ved Lillevik jernbanestasjon så traff siktede noe eller noen.

Siktede forsto ikke med en gang hva som hadde skjedd. Personen har kommet fra siktedes venstre side og ut i veien fra jernbanestasjonen. Personen treffer panseret og siktede bråbremset. Personen rullet da ned foran bilen.

I forkant av dette så er siktede obs på denne strekningen ettersom det har vært ulykker her før. Siktede holdt fartsgrensen som er på 50 km/t på strekningen.

Siktede har ikke brukt rusmidler under eller forut for kjøringen. Siktede går ikke på noen medisiner. Siktede har heller ikke brukt mobiltelefonen som hun kan huske under kjøreturen.

Før siktede traff personen så oppfattet hun ikke at det var noen personer på vei ut i veien.

#### Informasjon:

De objektive vilkårene i § 3 ansees å være bevist.

## Egenrapport – digitale spor

---

I forbindelse med trafikkulykken ble det innhentet og sikret digitale spor.

På grunnlag av vitneopplysninger fra vitne 1 om siktedes mobilbruk, ble siktedes mobiltelefon beslaglagt.

Mobiltelefonen ble transportert til avsnitt for digitalt politiarbeid, og ble der sikret med dataverktøyet Cellebrite UFED Touch 2, og deretter analysert med analyseprogrammet Cellebrite Physical Analyzer. Resultatet ble deretter oversendt rapportskriver for innholdsanalyse, ved hjelp av dataverktøyet UFED Reader.

Analysen av mobiltelefonen viste at siktede hadde ringt til 113 for å varsle om ulykken 02.02.2019 kl. 16:09:58.

Analysen viste også at i tidsrommet fra kl. 16:06:15 til siktedes anrop til 113 kl. 16:09:58 var det registrert 9 aktiviteter på siktedes mobiltelefon. 7 forskjellige Snapchat brukere var fordelt på disse 9 aktivitetene:

Nr:	Inn / ut:	Tid:	Sender:	Mottaker:	Beskrivelse:
1	Ut	02.02.2019 kl. 16:06:15	MarteKirkemo	Linda30	Snapchat
2	Ut	02.02.2019 kl. 16:06:17	MarteKirkemo	Anja20	Snapchat
3	Ut	02.02.2019 kl. 16:06:19	MarteKirkemo	LissiK	Snapchat
4	Ut	02.02.2019 kl. 16:06:32	MarteKirkemo	TuridÅs	Snapchat
5	Inn	02.02.2019 kl. 16:06:50	TuridÅs	MarteKirkemo	Snapchat
6	Ut	02.02.2019 kl. 16:07:53	MarteKirkemo	Guro36	Snapchat
7	Ut	02.02.2019 kl. 16:08:24	MarteKirkemo	StineK	Snapchat
8	Inn	02.02.2019 kl. 16:08:25	Anja20	MarteKirkemo	Snapchat
9	Ut	02.02.2019 kl. 16:09:48	MarteKirkemo	HeleneK	Snapchat
10	Ut	02.02.2019 kl. 16:09:58	Marte Kirkemo	113	Oppringing

Tabellen over viser aktiviteten på siktedes mobiltelefon de siste 4 minuttene før hun ringte 113.

Det ble sendt meldinger ved bruk av applikasjonen "Snapchat" til forskjellige mottakere, og det ble mottatt 2 meldinger i samme applikasjon. Den siste meldingen på "Snapchat" ble sendt kl. 16:09:48, altså 10 sekunder før siktede ringte 113. Dette viser at siktede har vært aktiv på telefonen i tiden forut for påkjørselen.

På grunn av bevisverdien tidspunktet for oppringningen til 113 hadde, så ble det innhentet teledata fra TELENOR for å bekrefte dette tidspunktet. Datasettet fra TELENOR viste at Marte Kirkemo hadde ringt 113 kl. 16:09:46 UTC + 1, noe som bekrefter at mobiltelefonen til

Marte Kirkemo sine tids- og datainnstillinger er riktige med et 12 sekunders avvik, og dermed er korrekte.

Det ble også sikret video fra kameraovervåking fra Lillevik jernbanestasjon, og videoen viste at Peder Ås ble påkjørt i det han befant seg i midt i gangfeltet, og det var ingen tegn til at bilen forsøkte unna manøver eller oppbremsing.

En GPS fra bilen til siktede ble manuelt gjennomgått på stedet, og ved omregning kunne man fastslå at gjennomsnittsfarten på kjøreturen hadde vært 46 km/t.

*Svein Storeby*

*Politibetjent 2*

*Lillevik lensmannskontor*



## SCENARIO 2:

---

«Seksualisert chat / overgrepsmateriale»

### Bakgrunnsinformasjon:

*Gjennom etterforskningen av en alvorlig overgrepssak tidlig i 2018, så fant KRIPOS en SKYPE chatlogg på den siktedes PC. Via IP sporing klarte KRIPOS å identifisere flere som hadde vært delaktig i å chatte med unge jenter via SKYPE, men som ikke var involvert i overgrepssaken de etterforsket. Innholdet i chattene hadde et seksuelt innhold. KRIPOS opprettet derfor saker på alle de identifiserte fra den aktuelle chatloggen. En av disse, Peder Ås, hadde bopelsadresse i ditt politidistrikt, og KRIPOS oversendte derfor saken til ditt distrikt.*

*Peder Ås er tidligere straffedømt for å ha chattet seksuelt med jenter under 16 år for noen år tilbake.*

*I en aksjon like etter at saken fra KRIPOS ble mottatt i 2018, ble Peder ÅS pågrepet og avhørt, og hans mobiltelefon og datamaskin beslaglagt og sikret.*

*På grunn av stor sakstilgang så har saken hatt liggetid i nærmere 1 år siden pågripelsen og det innledende avhøret. I denne tiden ble det også byttet hovedetterforsker og jurist på saken. I forbindelse med en restanseaksjon året etter ble det din oppgave å påtaleavgjøre saken. Saken ble derfor prioritert, og speilfilene fra beslaget ble funnet frem, og deretter analysert.*

Appendix 7:

## SCENARIO 2

### AVHØR

Siktete - Pågripelsestidspunktet:

*Siktete erkjenner å være den eneste som har tilgang til sitt eget nett så vidt han vet om. Nettverket er passordbeskyttet, og siktete har ikke gitt ut dette passordet til noen. Han nektet å ha chattet med unge jenter, og iallefall med seksuelt innhold. Han har ikke noe ulovlig materiale på datamaskinen eller mobiltelefonen sin. Siktete ble løslatt etter avhør.*

Siktete – 1 år etter pågripelsen, oppfølgingsavhør etter analysen av beslaget:

*I avhør nr. 2 nekter han fortsatt straffeskyld, både for seksualisert chat og besittelse av ulovlig SOMB materiale. Han hevder han ikke har noe ulovlig SOMB materiale, verken på mobiltelefonen eller datamaskinen sin.*

*Om bildene på telefonen forklarer siktete at det er mulig han fått tilsendt noen bilder som kan ha vært ulovlige på mobiltelefonen, men i så fall ble disse slettet i det han så hva det var han fikk tilsendt. Siktete kan ikke huske hvem det var som kan ha sendt ham disse bildene, eller når det var, men at de i så fall ble sendt via Messenger, Snapchat eller Kik, men husker ikke mer omkring dette.*

*Siktetes bekrefter at hans mailadresse er: [peder.ås@mail.xx](mailto:peder.ås@mail.xx)*

*Siktete forklarte at det kun er han som har tilgang til nettverket, datamaskinen og telefonen, og at alle 3 er satt opp med et passord kun han har tilgang til. Så om det er overgrepsmateriale på hans datamaskin, IP sporing som peker til ham, så må han vært utsatt for hacking eller et virus, som igjen har lastet ned overgrepsmaterialet, og chattet med unge jenter i hans navn.*

# SCENARIO 2

## ANALYSERAPPORT

### OPPSUMMERING

Det ble funnet totalt 1504 bilder som viser SOMB på siktedes datamaskin, i hans netthistorikk, og på hans mobiltelefon. Det ble også funnet 1220 chattelinjer med seksuelt innhold fra SKYPE hvor siktede chatter med unge jenter fra 13 til 17 år. Det ble ikke funnet tegn på at siktede har fått tilsendt SOMB bilder på mobiltelefonen eller til datamaskinen. Det ble heller ikke funnet virus / malware på siktedes datamaskin.

### DATASIKRING

I forbindelse med sak, ble beslag 2018/xxx-1 og 2 sikret.

Beslag 2018/xxx-1 ble sikret ved at datamaskinens harddisk ble skrudd ut, og deretter sikret ved å lage en speilkopi av harddisken ved hjelp av dataverktøyet EnCase Imager.

Beslag 2018/xxx-2, mobiltelefonen til siktede, ble sikret ved hjelp av dataverktøyet Cellebrite UFED Touch 2 Ultimate.

Nr:	Alg:	Sjekksum original:	Sjekksum speilfil:
1	MD5	a34744edade35cd83f684eb88eea2a87	5bd942a58139fc8d93ba4a8dae13b036
2	MD5	5c96768ac698c354c8c4693e37c9515d	5c96768ac698c354c8c4693e37c9515d

Figur 1. Viser oversikt over sjekksummer

Sjekksummene på speilfilene stemte overens med sjekksummene til originalbeslaget, og integriteten til beslaget er dermed godkjent, se figur 1.

Speilkopiene ble lagret på politiets server.

Speilkopi av harddisken fra datamaskinen ble deretter analysert. Netthistorikken ble gjenskapt ved hjelp av dataverktøyet Internet Evidence Finder, og bildematerialet ble gjennomgått ved bruk av dataverktøyet Griffeye Analyze.

Speilkopi av mobiltelefonen ble analysert ved bruk av Cellebrite Physical Analyzer.

## INTERNETTHISTORIKK

### *Datamaskin*

Internetthistorikken ble eksportert ut ved hjelp av dataverktøyet Internet Evidence Finder, og det ble funnet over 1500 nettadresser som pekte til nettsteder som inneholdt overgrepbilder av barn, viser til bilderapport – bilde nr. 1 til 12.

### *Mobiltelefon*

Internetthistorikken ble analysert ved bruk av Cellebrite Physical Analyzer, og det ble ikke funnet netthistorikk av interesse for saken.

## CHAT

### *Datamaskin*

Det ble funnet og gjenskapt chat-historikk fra applikasjonen SKYPE på datamaskinen til siktede, som sammenfaller med chatloggen KRIPOS fant. Totalt 1220 linjer med chattelogger fra SKYPE ble gjenskapt:

Nr:	Tid:	Fra:	Til:	Melding:
1	03.03.2018 21:23:10	PeDå	Jente13	«Seksuelt innhold»
2	03.03.2018 21:23:46	Jente13	PeDå	«Seksuelt innhold»
3	03.03.2018 21:23:57	PeDå	Jente13	«Seksuelt innhold»
4	03.03.2018 21:24:10	PeDå	Jente13	«Seksuelt innhold»
5	03.03.2018 21:26:34	Jente13	PeDå	«Seksuelt innhold»

+ 1215 linjer til

KRIPOS identifiserte SKYPE brukeren «PeDå» som Peder Ås, registrert hos SKYPE under mailadressen:

[peder.ås@mail.xx](mailto:peder.ås@mail.xx)

Denne mailadressen tilhører siktede, og er gjenfunnet og registrert flere steder både på mobiltelefonen og datamaskinen til siktede.

### *Mobiltelefon*

Det ble ikke funnet Messenger meldinger på mobiltelefonen til siktede.

Det ble funnet Kik og Snapchat meldinger, men ingen spor av at siktede har fått tilsendt ulovlige bilder via disse applikasjonene, eller logger som omhandlet seksuelt innhold på siktedes mobiltelefon.

## BILDER

Det ble funnet totalt 1504 ulovlige SOMB bilder. 2 SOMB bilder på siktedes mobiltelefon, og 1502 SOMB bilder på siktedes datamaskin.

### Mobiltelefon

Det ble funnet 2 ulovlige bilder som viste SOMB på siktedes mobiltelefon, viser forøvrig til bilderapport, bilde nr. 15 og 16.

Bildene ble funnet i filstien:

```
USERDATA(ExtX)/Root/data/com.facebook.orca./cache/image/v2.ols100.1/95/<filnavn>
```

### Datamaskin

I filstrukturen på beslaget ble det funnet 2 ulovlige SOMB bilder i filstrukturen på siktedes datamaskin.

Bildene lå i følgende filsti:

```
C:\Users\Azz\AppData\Local\Mozilla\Firefox\Profiles\VGKB1F2.default\cache2
```

Internetthistorikken viste over 1500 adresser (URL) som pekte til overgrepbilder av barn.

For å få frem internetthistorikken ble dataverktøyet Internet Evidence Finder brukt.

Internetthistorikken ble deretter eksportert ut til et eget dokument, som ble overført til en ren nyinstallasjon av Linux, som var oppsatt med anonymt internett. Etterforsker og dataetterforsker gikk deretter gjennom internetthistorikken ved å gå til nettadressene de forskjellige URL`ene pekte til, og deretter dokumentere overgrep bildene som lå der ved ta skjermbilder.

### VIDEO

Det ble ikke funnet videofiler av interesse på verken mobiltelefonen eller datamaskinen til siktede.

### SØK ETTER VIRUS / MALWARE

Det ble rutinemessig søkt etter virus på datamaskinen ved bruk av anti-virus verktøy like etter sikringen av datamaskinen ved pågripelsestidspunktet, og det ble ikke funnet virus eller tegn på at siktedes datamaskin har vært utsatt for hacking.

Dataetterforsker

Sverre Kirkemo

Appendix 9:

## Bilderapport – siktedes PC:

*Representativt utvalg av overgrepbilder fra siktedes PC – hentet fra internetthistorikk og filstruktur - totalt 1504 bilder.*

1. Fra datamaskin, netthistorikk, URL: <https://XXXX./PTHC/9yo/11548>

Bilde:



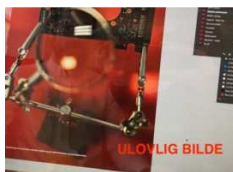
2. Fra datamaskin, netthistorikk, URL: <https://XXXX./PTHC/11yo/23687>

Bilde:



3. Fra datamaskin, netthistorikk, URL: <https://XXXX./PTHC/12yo/36587>

Bilde:



4. Fra datamaskin, netthistorikk, URL: <https://XXXX./PTHC/7yo/78943>

Bilde:



5. Fra datamaskin, netthistorikk, URL: <https://XXXX//young/988775>

Bilde:



6. Fra datamaskin, netthistorikk, URL: <https://XXXX//young/78655>

Bilde:



7. Fra datamaskin, netthistorikk, URL: <https://XXXX//young/93425>

Bilde:



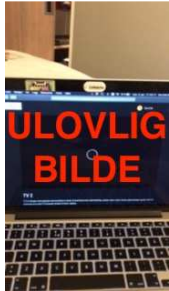
8. Fra datamaskin, netthistorikk, URL: <https://XXXX//young/3212375>

Bilde:



9. Fra datamaskin, netthistorikk, URL: <https://XXXX//young/94565>

Bilde:



10. Fra datamaskin, netthistorikk, URL: <https://XXXX//young/733345>

Bilde:



11. Fra datamaskin, netthistorikk, URL: <https://XXXX//young/222175>

Bilde:



12. Fra datamaskin, netthistorikk, URL: <https://XXXX//young/703395>

Bilde:





13. Fra datamaskin, filsti :

C:\Users\Azz\AppData\Local\Mozilla\Firefox\Profiles\VGKB1F2.default\cache2

Bilde:



14. Fra datamaskin, filsti :

C:\Users\Azz\AppData\Local\Mozilla\Firefox\Profiles\VGKB1F2.default\cache2

Bilde:



15. Fra mobiltelefon, filsti :

USERDATA(ExtX)/Root/data/com.facebook.orca./cache/image/v2.ols100.1/95/BrEb  
mKi-zIYBNa9nWA4K7j4wgTE.cnt

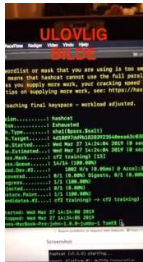
Bilde:



16. Fra mobiltelefon, filsti :

USERDATA(ExtX)/Root/data/com.facebook.orca./cache/image/v2.ols100.1/95/KhCrIk  
o-sIUNBw4lpASk6saXC.cnt

Bilde:



## SCENARIO 3:

---

### «Jourhavende»

#### Bakgrunnsinformasjon:

Politiets nødsentral 112 i Lillevik ble fredag 12.04.2019 kl. 2200 oppringt fra Peder Ås, teknisk ansvarlig ved MAYDAY-chat.no, en chat-tjeneste for ungdom som trenger noen å snakke med. Chattetjenesten spesialiserer seg på seksuelle overgrep. MAYDAY-chat har i utgangspunktet taushetsplikt, men Peder Ås følte likevel at fare for tap av liv og helse nå var så stor at han måtte varsle.

Peder forklarte at han tirsdag kveld kl. 2035 hadde hatt en samtale på chat med en ung jente som hevdet å være 16 år. Hun forklarte at hun nesten daglig var utsatt for seksuelle overgrep av sin far, og at dette hadde pågått i over 8 år. Overgrepene startet først "uskyldig", men hadde nå gått over i voldtekt. Hun hadde på grunn av dette selvmordstanker, og bedrev også alvorlig selvskading. Samtalen mellom Peder Ås og jenta ble avbrutt, men de rakk å avtale med jenta at de skulle snakkes igjen i kveld, fredag 12.04.2019. Peder vurderte allerede tirsdag om han skulle kontakte politiet, men bestemte seg for å vente å se om jenta tok kontakt igjen fredag kveld, og høre hva hun sa da.

Fredag kveld kl. 2105 fikk Peder Ås igjen kontakt med jenta. Hun forklarte da at hennes far var på vei hjem, og at han var beruset. Hun visste at hun kom til å bli utsatt for et overgrep ikveld, da det alltid skjedde når faren hadde drukket. Jenta var svært fortvilet, og virket veldig redd. Hun forklarte at hun hadde tenkt å ta livet sitt etter dette.

Peder Ås vurderte at liv- og helse gikk foran taushetsplikten, og at han uten opphold måtte varsle politiet slik at overgrep og mulig selvmord kunne avverges.

MAYDAY-chat.no har gjennom den tekniske serverløsningen sin mulighet til å se hvilken IP-adresse deltakerne i chatten har, og jenta hadde IP-adresse 192.168.25.1. Ved søk på IP-adressen kunne Peder fastslå at IP-adressen tilhørte en adresse i Lillevik. Peder ringte derfor 112 i Storeby, og ble satt over til 112-sentralen i Lillevik.

Peder forklarte operatøren ved 112 sentralen situasjonen, og sendte over skjermbilder av chatten, sammen med informasjonen om IP-adressen og hvor den pekte til på et kart gjennom et IP-geosøk. Operatøren på sentralen klarte ved hjelp av søk i folkeregisteret å finne korrekt adresse og identifisere de som var registrert på adressen. På adressen var det registrert 2 personer, en jente på 15 år og hennes far på 45 år.

På grunn av sakens alvorlighet ble det vurdert som tidskritisk å gå til umiddelbar pågripelse / ransaking på adressen. Operasjonsleder ved 112 sentralen ringte derfor opp jourhavende jurist for å fremlegge saken, og for å be om beslutning om pågripelse / ransaking på aktuell adresse for å avverge nye overgrep / selvmord.

Appendix 11:

SVARSKJEMA nr: .....

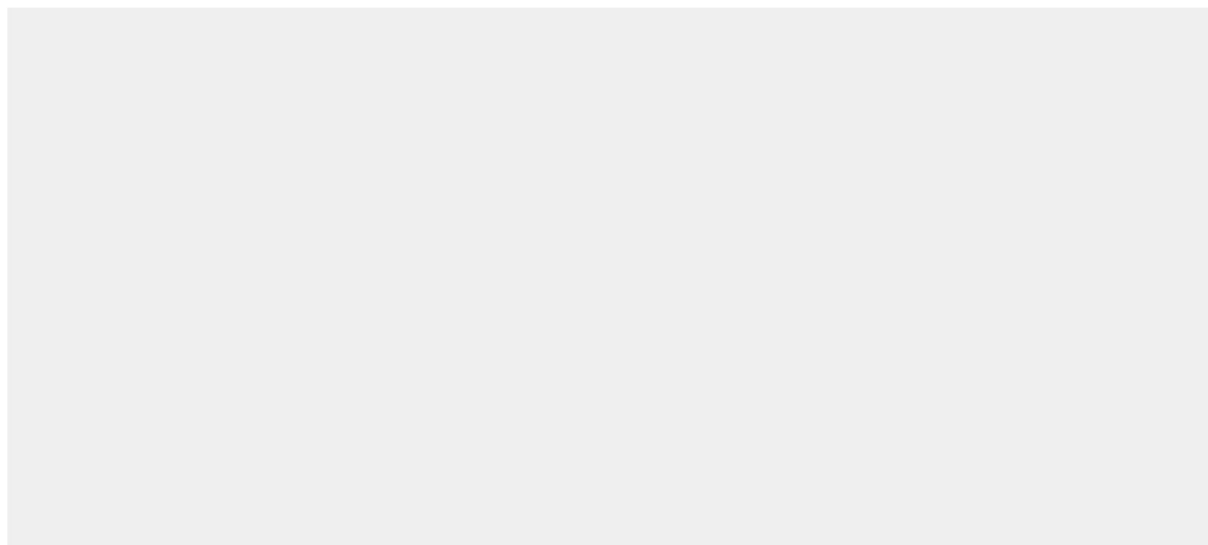
**Samtykke til deltakelse i studien:**

**JA**

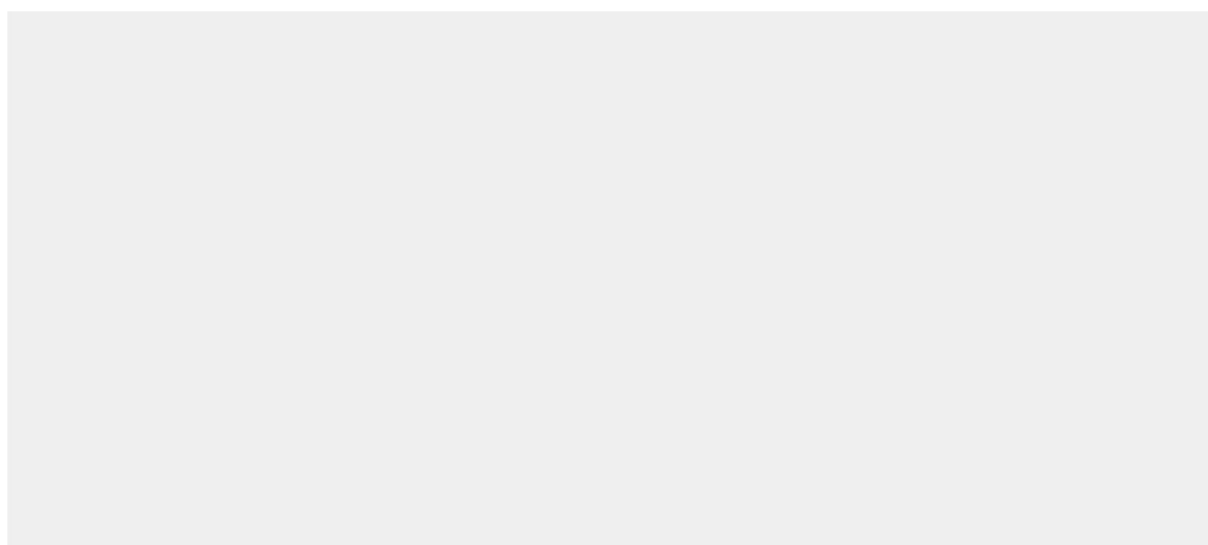
Jeg har fått informasjon om studien, og er villig til å delta:

# SCENARIO 1:

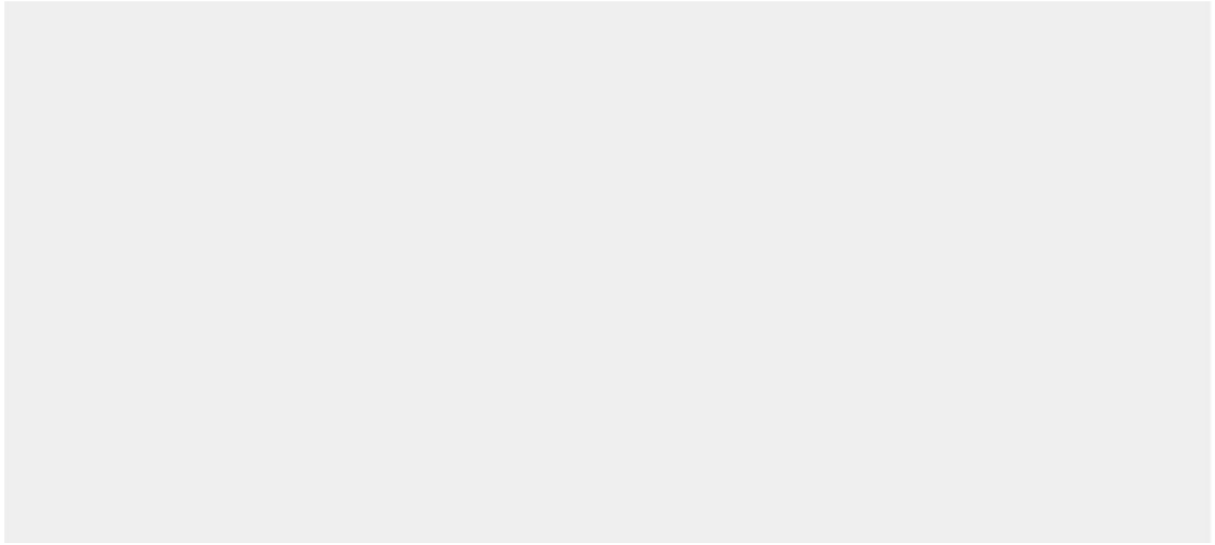
1) Identifisering: Kan du identifisere digitale bevis mener du har betydning for tiltals spørsmålet i denne saken?



2) Bevisvurdering: Hvordan vurderer du de enkelte digitale bevisene? Høy grad, liten grad.

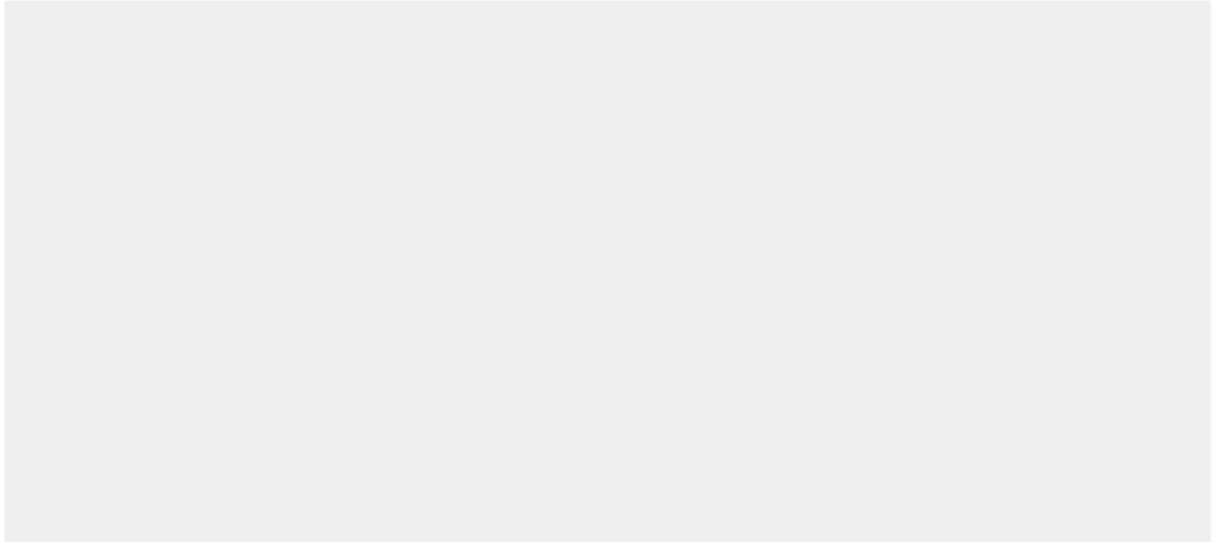


3) Hvorfor?

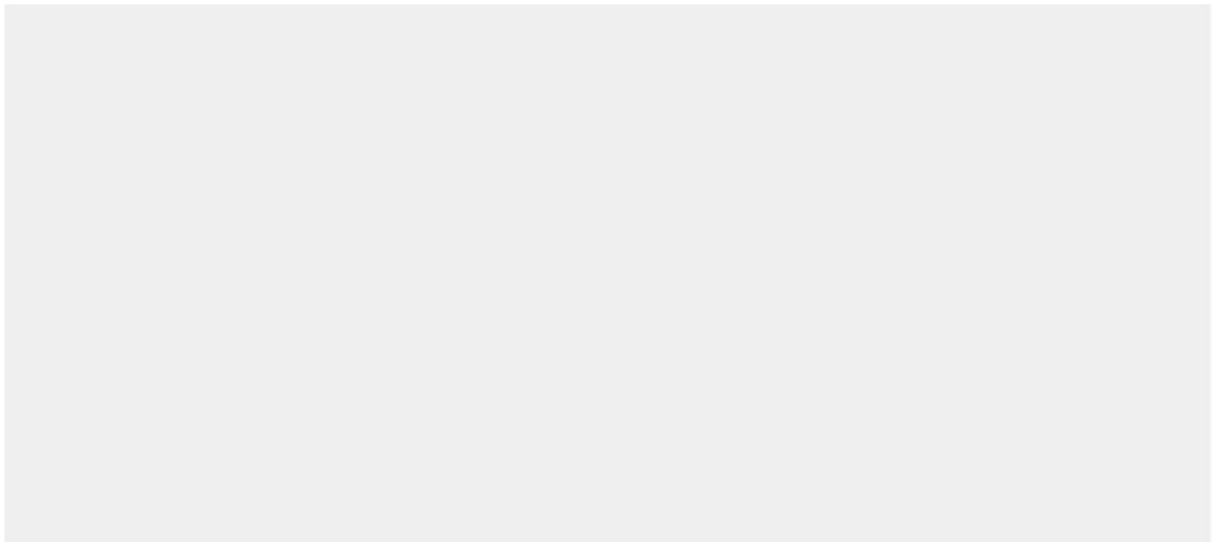


## SCENARIO 2:

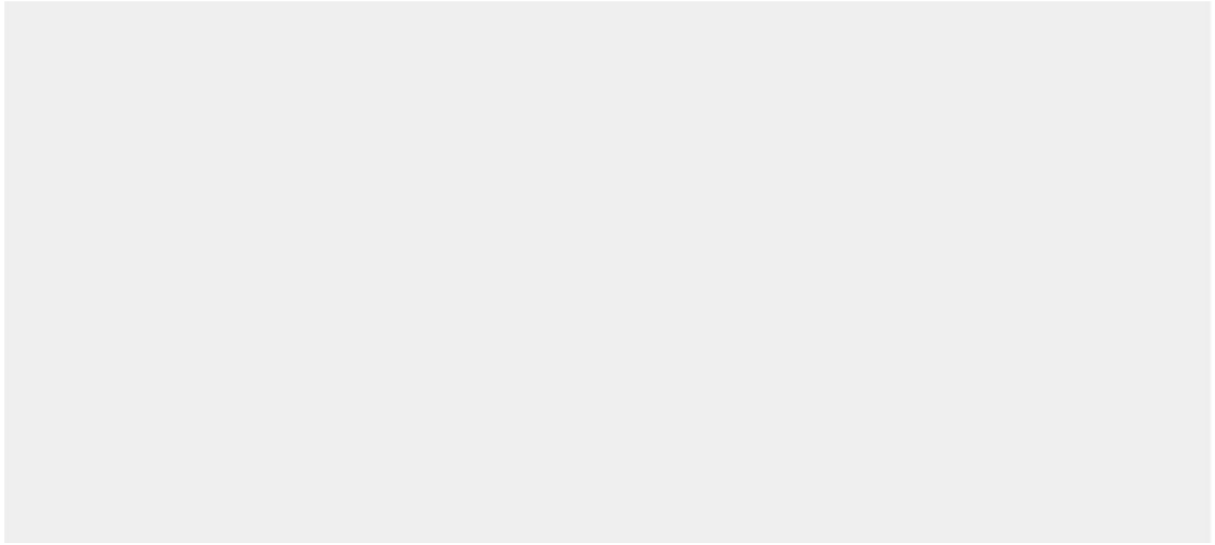
1) Identifisering: Kan du identifisere digitale bevis mener du har betydning for tiltalspørsmålet i denne saken?

A large, empty rectangular box with a light gray background, intended for the user to identify digital evidence relevant to the case.

2) Bevisvurdering: Hvordan vurderer du de enkelte digitale bevisene? Høy grad, liten grad.

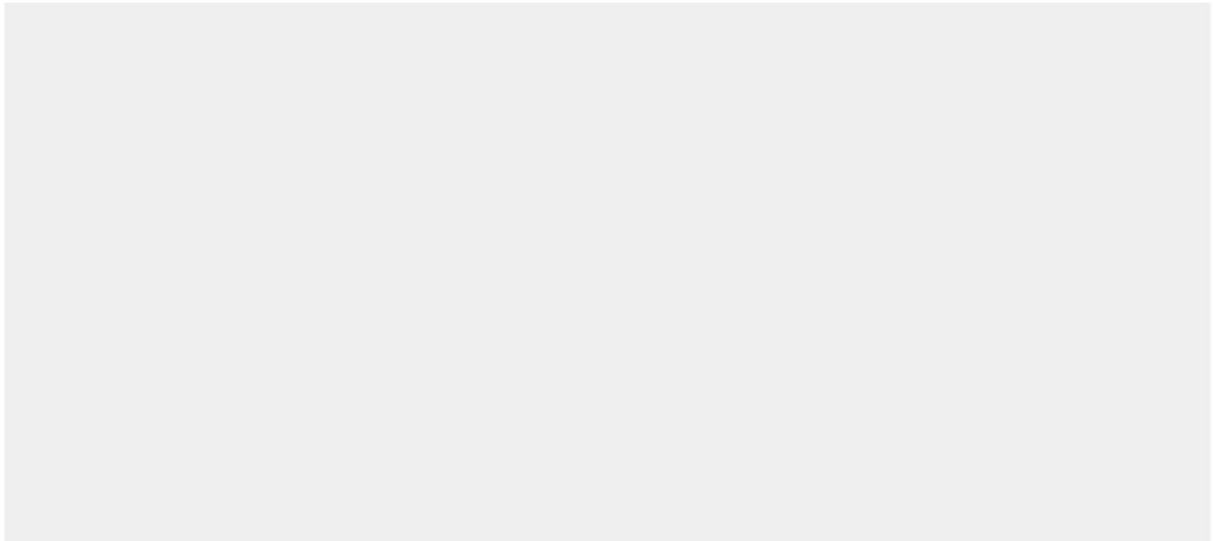
A large, empty rectangular box with a light gray background, intended for the user to evaluate the individual digital pieces of evidence, such as their degree of relevance.

3) Hvorfor?

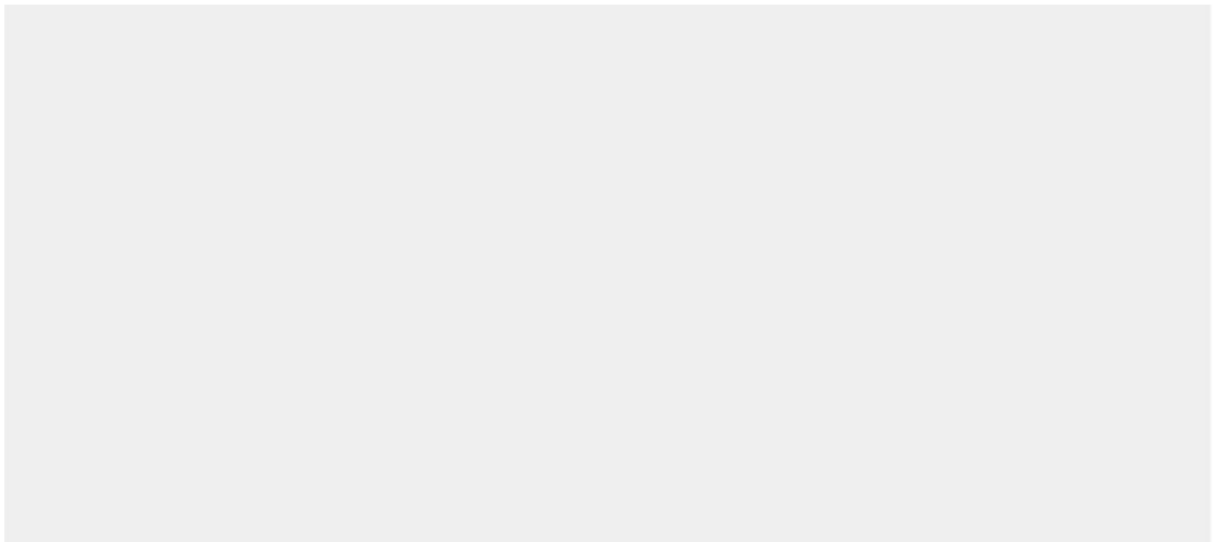


# SCENARIO 3:

1) Vil du utferdige beslutning om pågrepelse og ransaking?



2) Hvorfor? Vurdere, veie.





# Spørreskjema

1) I de tre - 3 - siste straffesakene du har jobbet med, i hvor mange saker bestod bevisbildet av minst ett digitalt spor?

*Digitalt spor: Mobiltelefon, konto på sosiale media, datamaskin, bankutskrift, bompassering, videoovervåkning etc.*

**0      1      2      3      USIKKER**

2) Hva slags digitale spor var til stede i saken(e):

**Mobiltelefon                  Datamaskin                  Lagringsmedium                  Sosiale media**

**E-post                  Videoovervåkning                  Annet**

3) Stoler du på kvaliteten til de digitale bevisene du får presentert i saken fra dataetterforsker?

**JA      NEI      AV OG TIL      VET IKKE**

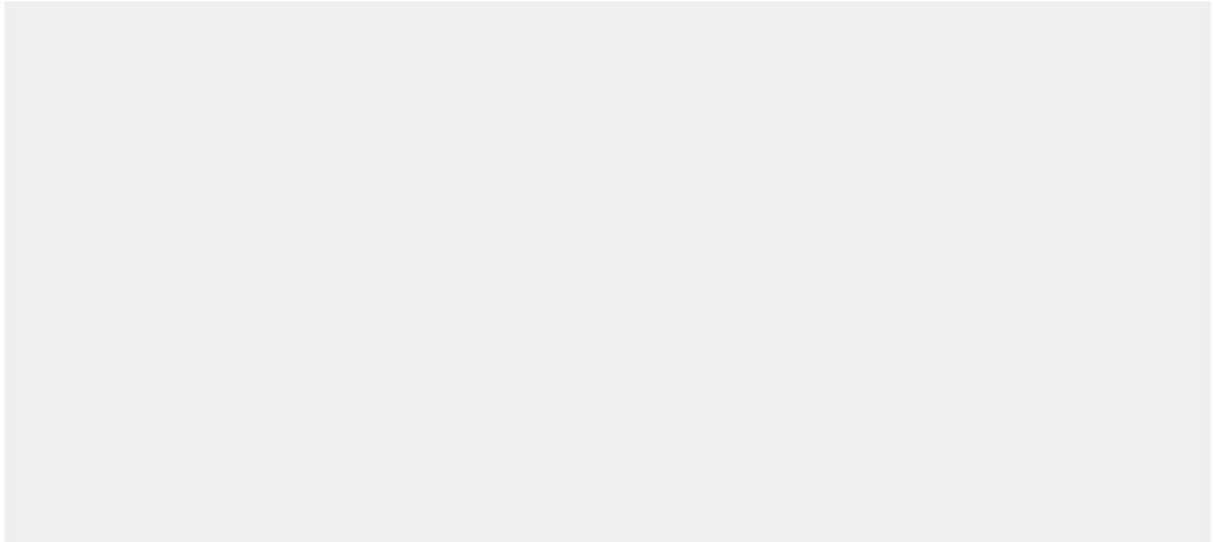
4) Stoler du på kvaliteten til de digitale bevisene du får presentert i saken fra etterforsker / politibetjent?

**JA      NEI      AV OG TIL      VET IKKE**

5) Vurderer du kompetansen på vedkommende som har levert bevismaterialet når det kommer til digitale bevis?

**JA      NEI      AV OG TIL      VET IKKE**

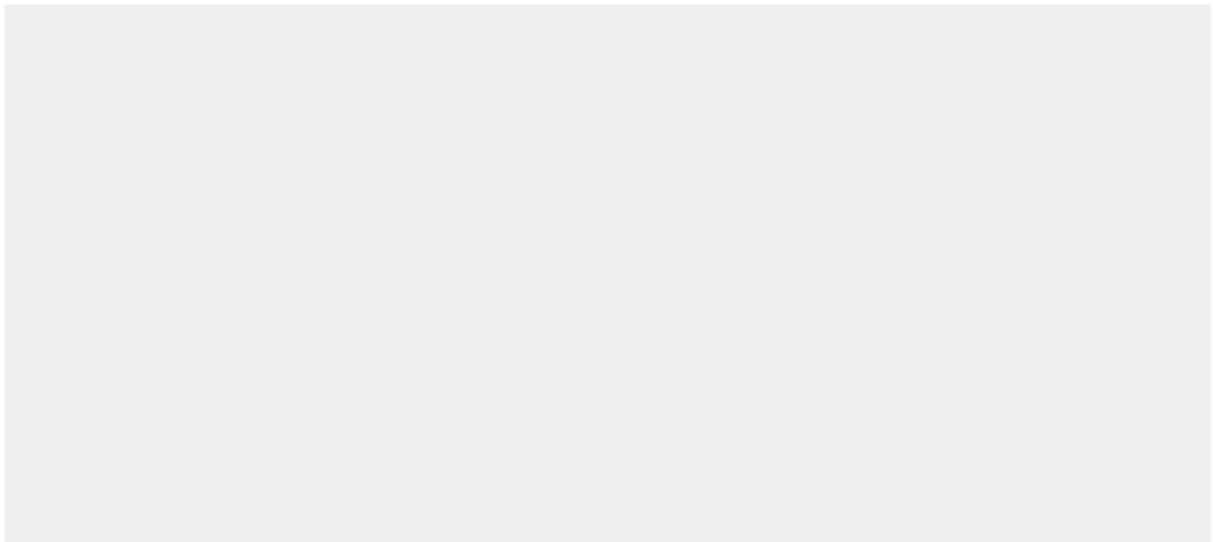
6) Hvordan gjør du dette? (Metode, helhetsvurdering, sunn fornuft, kjennskap. Hva ser du etter?)



7) Vurderer du bevisverdien av digitale bevis? (parameter for kvalitet – RA)

**JA    NEI    AV OG TIL    VET IKKE**

8) Hvordan gjør du dette? (Metode, helhetsvurdering, sunn fornuft. Hva ser du etter?)



9) Stoler du på at de digitale bevisene du får presentert i saken som er produsert av automatiserte dataverktøy er verifiserte?

**JA    NEI    AV OG TIL    VET IKKE**

10) Hvordan vil du vurdere din egen kompetanse til å vurdere kvaliteten på digitale bevis produsert med følgende analyseverktøy:

	Ikke kompetent	Svært lite kompetent	Litt kompetent	Kompetent	Svært kompetent	Har aldri hørt om dette
Griffeye Analyze (bilder/video)						
Internet Evidence Finder (internettrelatert)						
Cellebrite Physical Analyzer/Reader (mobile enheter)						
XRY Reader (mobile enheter)						

11) Hvordan vil du vurdere din egen kompetanse om du får påtaleansvar for en sak som omhandler:

	Ikke kompetent	Veldig lite kompetent	Litt kompetent	Noe kompetent	Kompetent	Svært kompetent
Et firma har anmeldt et tjenestenektangrep (DDoS-angrep) på deres datasystemer						
En ung jente har fått et nakenbilde av seg spredd ved bruk av en mobilapplikasjon						
En mann har fått kontoen sin i nettbanken tømt for penger						
En eldre mann har blitt svindlet på FINN.no						
En kvinne har blitt utsatt for						

identitetstyveri, og noen har bestilt varer på internett i hennes navn						
Ole har mottatt en e-post hvor det står at en hacker har filmet Ole med webkamera når Ole har sett på pornografi. Hackeren truet med å sende videoen til Oles venner og familie hvis Ole ikke betaler 0,1 Bitcoin til en oppgitt adresse						

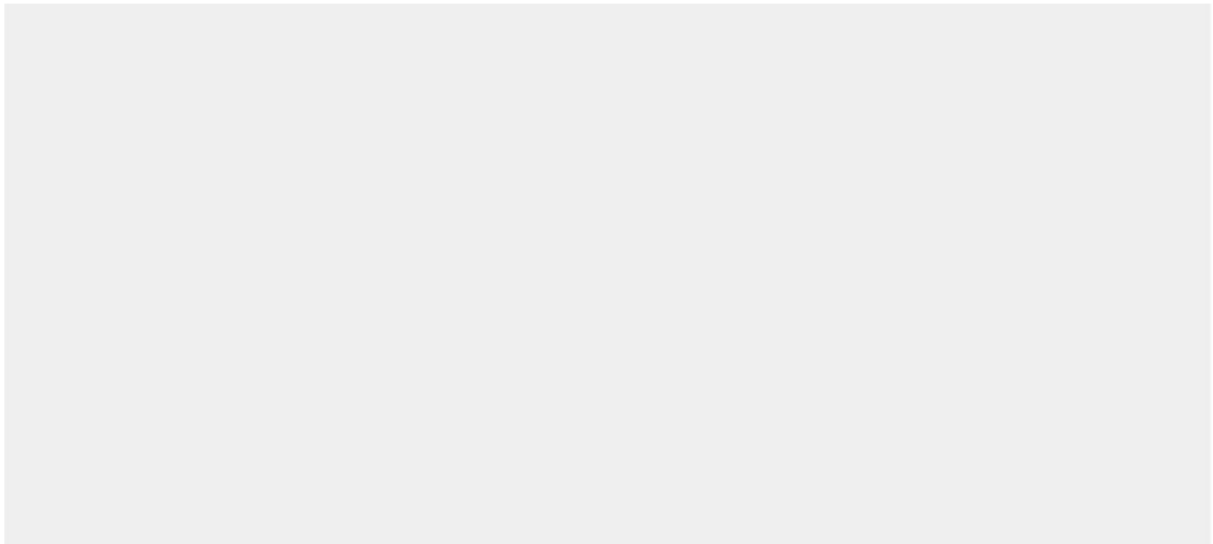
12) Hvordan vil du vurdere din egen kompetanse omkring følgende digitale bevis:

**Kjennskap til teknologi og digital etterforskning:** *Du vil nå bli presentert for forskjellig teknologi og konsepter fra digital etterforskning.*

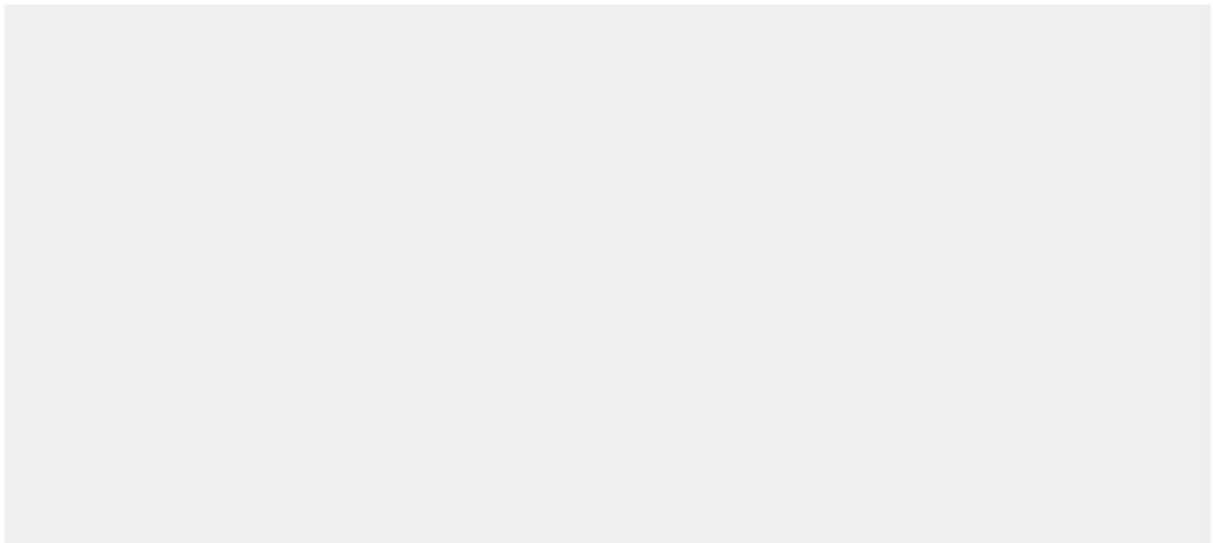
	Ikke kompetent	Veldig lite kompetent	Lite kompetent	Noe kompetent	Mye kompetent	Svært mye kompetent
Sporing av e-post						
Digital valuta som Bitcoin og Ethereum						
Eierskap av konto på sosiale media						
En slettet fil som er gjenskapt						
IP sporing						
Datanettverk og funksjonalitet						
Løsepengevirus (ransomware)						
Hvorfor tidsinnstillinger på beslag kan være viktig						
Utarbeide beslutning om utlevering fra en						

tjenestetilbyder som f.eks Google						
Skadevare (malware)						
Det mørke nettet (dark web)						
Hvordan internett fungerer i teorien						
VPN (virtuelle private nettverk)						

13) Hva mener du kan påvirke deg negativt i din vurdering av digitale bevis?



14) Hva mener du kan hjelpe deg i din vurdering av digitale bevis?



15) Har du opplevd at det har blitt stilt spørsmål om kvaliteten på digitale bevis fra aktørene i retten?

*Rettsens aktører: Dommer, jury, bistandsadvokat, forsvarer*

**Ingen spørsmål**

**Noen få spørsmål**

**Mange spørsmål**

16) Har du hatt kursing/opplæring innenfor digitale bevis etter at du begynte i politiet?

**JA**

**NEI**

**VET IKKE**