Systematically assessing the competence level of digital evidence handling

Odin Heitmann[1,2] and Katrin Franke[2]

[1] The National Criminal Investigation Service, Postboks 2094 Vika, 0125 Oslo, Norway

[2] Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway
odin.heitmann@politiet.no

Abstract. Norway is among the most digitalized countries in the world. For example, more than 91% of the citizens use mobile phones, and even more than 98% have access to the Internet. Hence, almost all kinds of criminal cases investigated by the Norwegian police include digital evidence. Within the police organization, various roles and responsibilities exist, ranging from first responders arriving and securing crime scenes, to police investigators, analysts, forensic scientists, and prosecutors. They will all need to handle digital evidence according to their work tasks. Available skilled personnel with education in digital forensics accounted for only 2% of the available personnel in 2018. To assess the skill level of first responders in securing digital evidence at crime scenes, derive knowledge needs and recommend adequate training, we conducted a large-scale field study. This paper presents our methodology in detail, comprising i) a theoretical competency assessment and ii) a practical test. Our findings indicate deficiencies in the examination phase of digital evidence, and there are indications that a digital evidence verification system is missing before the evidence is presented in court. Further findings are discussed in this paper before we propose several activities for decision makers to implement and to improve digital competence and digital understanding for personnel in law enforcement agencies.

Keywords: Digital investigation, police, digital forensics, criminal investigation, digital competence, investigative competence

1. Introduction

Technology surrounds us in every aspect of our daily life. Each and one of us leave behind a digital footprint in the form of data every time we visit web sites or send messages online [1]. This is a potential gold mine for law enforcement agencies as it can either support or refute a hypothesis[1] in an ongoing investigation. Furthermore, each time we use the Internet there is a chance of unintentionally leaving information behind. This passive digital footprint can include our current internet protocol (IP) ad-

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

dress and what software is in use. Even a passive digital footprint can be what an investigator needs to identify a suspect, rendering it important. There is an abundance of digital information available for law enforcement, but an important question is how ready and capable relevant authorities are to utilize the possibilities that exist.

The remainder of this paper is structured as follows. Section 2 gives a background within the field of criminal investigation and digital forensics in Norway. Bloom's taxonomy of learning objectives is then briefly explained before the research approach used to develop a theoretical competency assessment and a practical test for experimentation is presented in section 3. In section 4, we present and discuss the findings from the experiments conducted. Finally, we conclude in section 5 where we propose several activities and future work on a systemic level to support decision-makers to implement and improve digital competence and digital understanding for personnel in law enforcement agencies and other establishments.

2. Background

2.1. Criminal investigation and digital investigation

The Norwegian Criminal Procedure Act [3] states that the purpose of an investigation is to gather necessary information to decide the issue of indictment, to serve as a preparation for the court's consideration of the issue of criminal liability and, possibly, the question of the determination of reaction. The purpose is also to avert or stop criminal offences or to execute punishment and other reactions.

To fulfil the requirements of the Criminal Procedure Act §226 it is common to seek answers to the basic questions known as '5WH', defined by (Stelfox, 2013) and referred to by Årnes [4]. '5WH' defines the objectives of an investigation as determining ***Who*** was involved, ***Where*** did it happen, ***What*** happened, ***When*** did it happen, ***Why*** did it happen and ***How*** did it happen. Answers to these questions can be imperative to conduct a proper investigation. Digital investigation in its purest form can be viewed as conducting traditional investigation, but with electronic data and information – digital evidence.

2.2. History of digital forensics in Norway

The first Computer Crime Unit (CCU) in Norway was created in 1995, and the first computer crime class was held in 1996 by the Norwegian Police University College (PHS) in collaboration with the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime. In 2004 the first academic digital forensics course was approved. The requirements for this course included the students having achieved a basic computer technical education provided by the Norwegian Networked University (NNU), a now defunct university [5].

The findings from working groups' reports in 2012 and 2017 show that the focus on digital investigation has changed, improving the situation. In 2017 a working group tasked by the Norwegian Police Directorate (POD) wrote about capacity and competence needs of the Norwegian police for the next ten years to come. On the topic of

computer crime, they stated that "anyone who is going to work with the police's core tasks must therefore have a basic understanding of how computers, computer systems, and computer networks function" [6].

Updated curriculum, with increased focus on digital investigation, further support the observation that digital investigation is becoming more relevant and accepted. Police students graduating from PHS before 2011 did not have any mandatory curriculum which included digital evidence. They could, at the end of the semester, choose a specialization course for digital evidence worth five credits. Police students graduating in 2015 had digital evidence the last year of the education as one of several subjects in the module 'Investigation' for a total of twelve credits [7]. The latest change in curriculum was for police students graduating in 2019. They were taught a module called 'Digital Policing and Investigating' each year for three years for a total of ten credits.

PHS provides over ten courses related to computer forensics investigation. The courses are divided into modules. Module 1 is mandatory for anyone wanting to pursue the other modules. The target group for module 1 is stated on the PHS website to be «police staff in the Nordic countries whose main task is or will be handling and investigating digital evidence». After module 1 is passed, it is possible to specialize in different fields within computer forensics, for example 'Network Forensics and Cybercrime'. There is also a post graduate study for investigation. The module gives 15 credits, and the participants are employees who have, or are intended to have, investigation as their primary work task. After graduating from the course, the students should have knowledge about digital evidence in an investigation, and they should be able to safeguard digital evidence on a crime scene. They should also be able to acquire digital evidence on the Internet [8].

2.3. Digital forensics process model and process model for investigation

The digital forensics process model is a normative presentation of the distinct phases in a digital forensics investigation. It consists of five consecutive and iterative phases, and is based on the same principles which adhere to a traditional physical forensics investigation process. The process normally starts with an incident or a crime, and the consecutive phases are *Identification*, *Collection*, *Examination*, *Analysis* and *Presentation*. Based on the crime a hypothesis, or multiple hypotheses, are created which leads to an investigation [4].

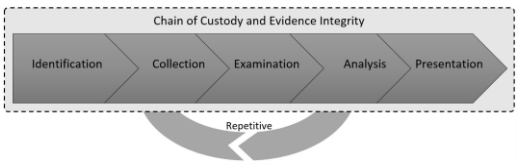

Fig. 1. The Digital Forensics Process illustrated by Flaglien [4]

The digital forensics process model can be used as an executive framework for digital forensics investigation. However, as it is designed for a superior level aimed at digital forensics, and due to the absence of a *continuous evaluati*on of hypotheses,

the digital forensics process model may not be suitable for illustrating the detailed workflow in a *criminal* investigation. Andersen [9] has developed an investigation process model designed to be applied in situations where a systematic examination is performed. The objectives of an investigation, as outlined in section 2.1, will benefit from using a systematic approach to answer the questions related to 5WH. Andersen's model is flexible and can also be used for any incident response situations by minor adjustments in the phases.

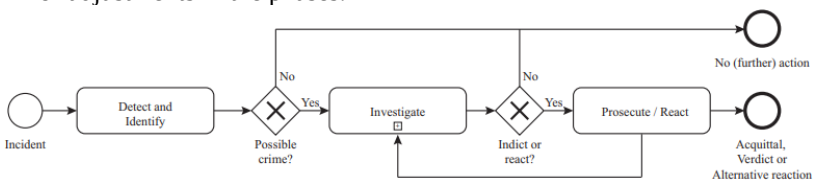

Fig. 2. Criminal case model [9]

As with the digital forensics process model, Andersen's model includes an incident or event that leads to at least one hypothesis. After this the two models are different. While the digital forensics process model goes directly to identification of evidence, the criminal case model, after having determined a possible crime has occurred, starts with the Investigate phase. The first object in the Investigate phase is *formulating hypotheses*. Based on the hypotheses formulated, relevant data sources who can evaluate the hypotheses must be *identified and located*. After information needs are identified, the next main phase is collection and the processing of data. The collection and processing phase of data will not be discussed further.

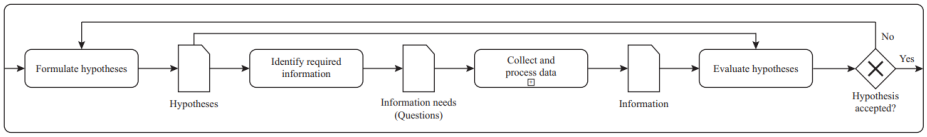

Fig. 3. Criminal investigation model [9]

2.4. Bloom's taxonomy of learning objectives

Taxonomy is the scientific process of classifying things and arranging them into groups. Learning objectives is what the learner is expected to know and understand after going through a learning process. Benjamin S. Bloom and a group of psychologists created several educational objectives in 1953, where they divided learning into six distinct levels. The levels were knowledge, comprehension, application, analysis, synthesis, and evaluation. Bloom's original taxonomy scheme were revised by Anderson and Krathwohl in 2001. The revised scheme was less strict, and the levels were changed from nouns to verbs [10].

The six levels in the revised scheme are illustrated in Fig. 5. Gogus [10] refers to Krathwol (2002) in that the scheme is hierarchically cumulative; in order to climb the pyramid, one must first master the level below. Each level is increasingly more complex in skill and/or ability.

In the illustration the three lowest levels are green, whereas the top three levels are red. This is done purely to illustrate which levels are within the scope of this paper. The levels 'remembering' and 'understanding' are relevant for the survey presented and discussed in section 3. The three lowest levels must be seen in correlation with the practical test covered in section 3. All definitions of the terms are made by Anderson and Krathwohl (2001) as presented by Gogus [10].

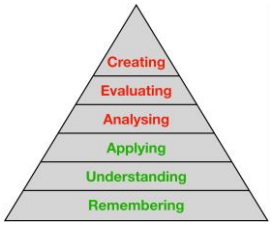

Fig. 4. Bloom's taxonomy of learning, six levels

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

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

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

3. Methodology

3.1. Research approach

Digital investigation competency in the Norwegian police is a specific and narrow area of research, and to our knowledge there has not been conducted any in-depth research on this field. However, there has been drafted reports about the field from various authors and organizations, for example the European Union Agency for Law Enforcement

Training (CEPOL) and Norwegian working groups [2]. Due to limited previous research within the field, written reports were used as support for the background of the field in Norway.

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

3.2. Theoretical competency assessment

To research how competent the respondents perceived themselves, in regards to several topics within digital investigation, a survey with both open and closed questions was used. Most of the questions used were open-ended questions to allow the respondent to provide brief answers instead of choosing from a predefined list.

The first set of questions were about demography and education within information security. These questions were used to be able to conduct a deeper and more comprehensive analysis. The respondents were also asked if they had any accounts on social media or if they owned a smart phone. The idea behind these questions was to see if there was a correlation between having a social media account and a smartphone, and the perceived competence when asked to acquire data from said items. They were then asked for the number of potential digital evidence in the last three criminal cases they had worked on. This provided an indication of the extent of digital evidence in criminal cases.

The next part of the survey was a varied range of scenarios where the respondents were asked to assess how competent they assessed themselves using an ordinal scale from *Not competent at all* to *Very competent*. The set of scenarios was identical, but the respondents were asked to assess their own competence based on three different prerequisites. The prerequisites were based on the subsequent processes from Andersen's process model for criminal investigation, as shown in fig. 3. The prerequisite for the first set of scenarios was to receive a complaint and write a police report. Using Andersen's investigation process model the police officer receiving a complaint must have a certain set of skills to be able to properly formulate hypotheses to identify the required information. The second prerequisite for the set of scenarios was for conducting initial investigative steps while the last prerequisite was the handling of digital evidence.

The last part of the survey was focused on testimony in court. The respondents were asked if they had testified in court about digital evidence, and those who had were asked to describe how confident they were and if their testimony was questioned by the members of the court. Using an open-ended question, the respondents who had given more

than one testimony were asked to briefly describe how they felt when they gave their testimonies. The open-ended question was used to let the respondents describe in their own words how they experienced the testifying. Finally, they were asked if someone else verified their findings before giving their testimony.

The survey was sent out to all police educated employees in the police districts Øst, Trøndelag and Møre og Romsdal. The police districts were chosen due to their variation in size. Approximately 2200 individuals received the survey, and 97 respondents completed the survey.

3.3. Practical test

In addition to the perceived competence, we wanted to develop a proof of concept for a certification that each investigator who will conduct digital investigation must pass. The practical test could also be relevant as a tool to ensure other key personnel, e.g., managers, have a minimum set of skills and knowledge within digital investigation. It could also be used to ensure a common baseline of digital competence across various agencies and even between public and private companies.

The structure of the test was based on both the digital forensics process model, fig. 1, and Andersen's process model for investigation, fig. 3. The first topic is *hypotheses*, which after an incident or event has occurred, is the first phase in Andersen's model. The next topic is *the identification of digital evidence.* This phase is the next in Andersen's model, and the first in the traditional digital forensics process model. The final topic in the practical test was *acquisition of data,* which is the subsequent phase of both models. Admittedly, it is within the same phase in Andersen's model, but in this phase, acquisition comes naturally after the actual identification.

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

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

In the last question in topic 2, the participants were presented with a scenario that contained limited information. They were then asked to identify what potential digital evidence could be present, and what information could be extracted from the digital evidence. The identification part of the question could be used to assess the participants

skills and knowledge to the *remembering* level in Bloom's taxonomy, while the second part of the question could be used to assess the next level, namely *understanding.* The participants could provide up to six different pieces of digital evidence and the corresponding potential information contained within.

The last topic the participants were tested on was acquisition of digital evidence. The main content of this topic required the participants to conduct actual acquisition of various social media accounts which had been created in advance. The purpose of these exercises was to assess the *application* level in Bloom's taxonomy. They were also asked theoretical questions to assess the level of skills and knowledge for both the *remembering* and *understanding* level. In the first part of this topic, the participants were asked open-ended questions about assorted topics within digital investigation. They were asked to name acquisition methods of data from the Internet which could be accessed through a web browser. Furthermore, they were tasked to describe what the Order of Volatility[2] is. Lastly, they were asked to list pros and cons of activating flight mode on a phone after it is seized, and pros and cons of conducting live forensics on a computer.

The next part of this topic was related to the practical handling of digital evidence. Presented with five diverse types of digital evidence, e.g., an Apple iPhone X with a known lock code, they were asked in what order they would handle the evidence. They could choose from a predefined list containing alternatives both forensically correct and incorrect. After each evidence item, there was an open-ended question asking the respondents why they chose to handle the evidence in the order they did.

After being provided with the username and password to three different social media accounts, namely Gmail, Facebook and Instagram, the participants were asked to acquire the accounts using a defined method. If several people across the country try to access an online account within a brief time frame, the content provider may have security measures in place that eventually prevent access to the account. To give the participants a real opportunity to complete the test, even if they experienced problems accessing the account due to the above-mentioned security measures, a Word-document containing already acquired content was attached to the question. The participants were asked if they managed to successfully download the content from the account. In addition to the answer alternatives 'yes' and 'no', they could also answer that they encountered technical difficulties and had to use the content provided in the Word-document instead. Using this practical approach, the participants' *application*-level skills could be assessed.

Those who answered that they managed to acquire the content from the account or had encountered technical difficulties and had to resort to the Word-document, were asked theoretical questions only answerable by examining the acquired content. As the practical test was intended to be a proof of concept of digital competency certification, it was unnatural to omit the examination part. To assess what method the participants would use to acquire a video from YouTube, they were provided with an Uniform Resource Locator (URL) to a video and asked to explain how they would acquire the

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

video. In the next question they were asked to explain how they would acquire a forum post from a given forum thread. The answers could be used to assess the *application* level of their skills and knowledge.

The participants were presented with a picture containing Exchangeable image file format data (EXIF data). They were then asked which two specific EXIF data fields were contained in the image. Lastly, they were asked which tool/method they used to identify and examine the EXIF fields. The answers could also be used to assess the *application* level of their skills and knowledge.

Using an e-mail address provided in the questionnaire, the participants were asked to describe which step(s) they could perform to find out who the owner of the e-mail address was. Regardless of what they answered, a prerequisite in the following question was that they had sent a request to the content provider, asking for basic subscriber information. The content provider had then returned an IP address belonging to an Internet Service Provider (ISP). The participants were asked what their next step would be. Again, regardless of what they answered, they were given a prerequisite where the ISP had returned a name and address of the person who had the IP address at the time. They were also informed that several people lived at the address.

The participants were asked which assessment(s) they should make before they directed suspicion at, or arrested, the person who had the IP address. The intention behind these questions was to assess how the participants approached the situation, and how they evaluated the information they were given.

A total of nine people were invited to take the practical test, and six people completed it. Out of the nine people invited, two were known to not be proficient in digital investigation. These two were invited to see how they managed to solve the tasks without having any digital investigation experience.

4. Results and discussion

4.1. Theoretical competency assessment results

Over half of the respondents (59,6%) graduated in 2011 or before. 26,3% graduated between 2012-2016, and the rest (11,1%) graduated in 2017 or later. As presented in section 2, this means that over half the respondents did not have any mandatory curriculum which included digital evidence during their bachelor education at PHS. Furthermore, almost half of the respondents (47,9%) answered that they had been employed ten years or more by the Norwegian Police. After working as a police officer for ten years, one is most likely looked upon as an experienced senior.

Around four out of ten respondents (39,6%) had attended training or courses in digital investigation after graduating from PHS. Informal training with a colleague was the delivery method of one or more of these training sessions for half the respondents. A purely practical approach has also been used on several occasions. The most common delivery method, however, is combining theoretical lesson(s) with a practical approach.

Over 90% answered that they had an account on Facebook, Facebook Messenger, and/or Snapchat. Seven out of ten (70,8%) had a Google account, and at least seven out of ten (76%) had an Instagram account. Fewer of the respondents had accounts on the

more communication-based platforms. 29 of the respondents (30,2%) had an account on Telegram, and 19 (19,8%) had an account on Signal. Based on the answers from the respondents, it can be argued that the majority are familiar with the social media platforms Facebook, Messenger and Snapchat. Arguably, the majority have the possibility to acquire their own accounts for testing purposes, and after acquisition, review content with which they are familiar. The answers also indicate that communication platforms like Signal and Discord are not as widely used by police officers as the other social media platforms are.

Almost every respondent (98%) answered that they own a smart phone. This high number indicates most police officers have a smart phone, and it can therefore be expected they are familiar with basic use concepts like turning the device on and off, enabling flight mode, entering a pass code, and navigating the menu on the device. It should be mentioned that there are large variations between different operating systems, for example Android and iOS. This might influence the degree of familiarity with an operating system, depending on the operating system the user is normally using.

Inspired by an online test where you can see how good you are at determining if a link or an attachment in an e-mail is legitimate or not[3], the respondents were asked how skilled they rated themselves to determine if a link or an attachment is safe to open or not. The skill level used an ordinal scale ranging from very poor to very good. 95% of the respondents assessed their competency to determine if a link or an attachment in an e-mail is safe to open or not to be fair or better. Only 5% assessed their competence to be poor or very poor. A report from the US communication company Verizon [11] found that 30% of phishing messages gets opened by targeted users, internal threat actors, in the public sector, and 12% of those users click on the malicious attachment or link and thereby compromise their credentials. If the numbers from Verizon's report are correct and representative, the answers from the respondents in the survey can indicate they are either more competent than the average, or that they assess their competency to be higher than it is.

Table 1. Self-assessment on competency to determine if a link or an attachment is safe

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

To give an assessment of possible indications from the results from the set of scenario-based questions a color scheme was applied. If the respondents assess they do not have competence or that they have very little competence, this can indicate major deficiency in their digital competence.

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

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

Fig. 5. Color scheme competency assessment

Based on results from the respondent's self-assessment of their competence in the six scenarios, each scenario indicates there are deficiencies when receiving a complaint and writing a police report and when tasked to perform initial digital investigation steps. The two scenarios that stand out with indications of major deficiencies are Distributed Denial of Service (DDoS) attacks and sextortion via e-mail. The scenarios which involved distribution of a nude picture using a mobile application, online bank fraud, marketplace fraud and identify theft had an average indication of deficiencies in the competency level. The most prominent answer marked with the corresponding color from fig. 5.

Table 2. Self-assessed competency, initial investigative steps, sextortion

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

Based on the results from the self-assessment of knowledge and skills related to assorted topics related to digital investigation, as shown in table 3, there is a clear indication of deficiencies in most of the listed skills and knowledge among the respondents. Except for the question about finding an ISP based on an IP-address, the alternative which got the most individual answers were either *No knowledge/skills at all*, or *Very little knowledge/skills*. This indicates there is a need for further training and for raising competency within the listed topics and concepts.

Table 3. Self-assessed competency, technology, and concepts from digital investigation

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

Out of 97 respondents, 27 (27,8%) answered they have given testimony in court about digital evidence. The respondents who had given testimony were asked if someone else had verified their findings before they gave their testimony. Out of 25 respondents, 14 (56%) had not verified their findings with some else before they gave their testimony. Nine respondents (36%) had verified the findings with a colleague from a computer crime unit, while two respondents (8%) had verified the findings with a colleague who did not work within a computer crime unit.

Table 4. Verification of findings by others before giving testimony

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

Peer review of digital evidence is essential to reduce the risk of miscarriage of justice. Even though the results from the survey has too few respondents to be conclusive, it is concerning that over 50% of the respondents did not verify their findings with someone else before they testified. Further research is recommended to examine the extent of the use of digital evidence with potentially low or even incorrect evidential value and its potential impact on the rule of law. Furthermore, implementation of peer review requirements for digital evidence before it is presented in court should be considered. This is discussed further in section 5.

4.2. Practical test results

The practical test was designed to fulfil three main purposes. First, assessing the participants' ability to solve different tasks commonly encountered by experienced investigators during their daily work. Three different scenarios were created to assess a variation of competencies. Secondly, assessing the different competency levels in accordance with the levels of Bloom's taxonomy as presented in section 2. Thirdly, reflecting the structure of the digital forensics and investigation process models as presented in section 2. It is worth emphasizing that the purpose of the practical test is to serve as a proof of concept for a certification process aimed at personell who will be performing digital investigation. It has not yet been tested on a large cohort, with further research and development being necessary.

The first part of the test was focused on initial investigative steps and the formulation of hypotheses. The participants were presented with three different scenarios containing various amounts of information, and they were tasked to formulate which hypothesis/hypotheses they could make from the information. In the first scenario, the participants provided at least four hypotheses. In the next two scenarios, the participants provided at least three hypotheses. The initial digital investigative steps they suggested had some variations, but also several similarities between them.

The next part was related to the identification of digital evidence. The participants were presented a list of items, and they were tasked to select the items they thought might contain digital evidence. When the test was designed, items which did not meet the criteria for being digital evidence were purposely added. Årnes [4] has defined digital evidence as "any digital data that contains reliable information which can support or refute a hypothesis of an incident or crime". The items in the test which fell outside this definition were notepad, camera lens, newspaper, plant, drugs, analog watch, water bottle, clothes, and power cable. Tasked with identifying items containing potential digital evidence, the participants correctly selected all the right items, except for one participant who did not select the headphones. In addition to selecting the correct items, several participants also selected other items which clearly do not contain potential digital evidence, e.g., a newspaper and a notepad. It is unclear if they selected those items because of an unclear question, or because they believed that newspapers and notepads contain digital data.

Finally, the participants were assessed on the acquisition of digital evidence. In the first part, the participants were asked open-ended questions about assorted topics within digital investigation. These theoretical questions were used to assess the level of skills and knowledge for both the remembering and understanding level. When asked how they would acquire data from the Internet, 'screenshot' was the most frequent listed method.

The next part within acquisition was related to practical handling of digital evidence. Presented with five distinct types of digital evidence, they were asked in what order they would handle the evidence.

When faced with an older MacBook Pro with a known username and password, the highest ranked approach by the participants was to consider their own competence (5/6) before calling a colleague from a computer crime unit for assistance (3/6). As seen in

Table 5, there were variations in how the participants would handle the MacBook Pro from the second action onward. The option no-one chose is marked in red.

Table 5. Practical test: Handling of an older MacBook Pro, known username and password

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

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

Those who managed to acquire the account, or reported that they had technical difficulties, were asked questions from the acquired data. The participants provided correct answers to all but two questions. One participant answered the serial number instead of the model's name for the device. One participant answered 'None' when asked which application the Facebook account was associated with. The questions asked assessed the participants on several things, and on distinct levels of Bloom's taxonomy of learning pyramid. They had to utilize what they remembered and understood about each of the three social media platforms, and master that knowledge, to apply it to an actual acquisition. When asked what the MD5 hash value[4] of the profile picture in the Instagram acquisition was, the participants had to remember what an MD5 hash value is, and they had to understand how an MD5 hash value is created. Finally, they had to have enough knowledge and understanding to create said hash value using the profile picture.

Application is the highest level of Bloom's taxonomy that will be covered in this paper. There were also questions which required the use of additional knowledge and skills from digital investigation. When asked what encryption tool the account user had searched for, they had to have sufficient knowledge about encryption tools to recognize that TrueCrypt had been searched for. This is knowledge on the lowest level, the remembering level.

[4] A hash value is a checksum which can be used to verify data integrity

Table 6. Practical test: Results from questions based on examination of acquired data

Google acquisition			
Question	**Correct answer**	**No. of correct answers**	**Source file**
What brand is the device used when creating the Google account?	*Huawei*	3	*Device-390666881794171690 9.html*
Which model name is the device?	*CLT-L29*	2	*Device-390666881794171690 9.html*
What is the IMEI for the device?	*866264047026922*	3	*Device-390666881794171690 9.html*
The account user has searched for an encryption tool - which tool?	*Truecrypt*	3	*My Activity.html*

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

When tasked with prioritizing the order in which various digital evidence should be handled, the respondents' approach varied largely. The options of documenting the evidence with a photo and considering one's own competence were among the alternatives that were chosen most frequently. The results of this assignment indicate that a uniform approach towards the handling of digital evidence may be advisable. An implementation of an overall standard operating procedure (SOP) for digital investigation methodology should be considered. The practical acquisitions were completed by four of six participants.

5. Conclusion

Findings from the theoretical competency assessment indicates that the survey can be used to discern deficiencies in knowledge and skills within technology and digital investigation. In our study the assessment indicated deficiencies in relation to all technology and concepts presented. The answers also indicate major deficiencies in the competency in live data forensics. With user-friendly encryption tools easily available, initial digital investigation on live evidence may be considered a task the average police officer should be able to perform.

The theoretical competency assessment should be further developed, both substantively and on a more suitable platform than used in our study. It could also be further refined to cover the needs of competency assessments in other law enforcement agencies and private companies.

Another finding was that over half of the respondents who have testified in court, presenting digital evidence, did not verify their findings with someone else before they testified. Digital evidence being presented without verifying its evidential value may indicate a systemic weakness in the Norwegian police procedures. This weakness may, in the utmost consequence, lead to miscarriage of justice if digital evidence of low, or even incorrect, evidential value are presented in court without verification.

The findings from the practical test revealed a lack of a uniform approach to the handling of digital evidence. These findings advocate the possible need for an overall SOP

for digital investigation methodology along with improved training and competence building in the field.

Additionally, the practical test should be further developed. A fully developed practical test may, in combination with training and competence enhancing measures, be used as a certification process where relevant personnel can demonstrate and assess their skills and competency.

References

1. TechTerms Digital Footprint Definition. Available at: https://techterms.com/definition/digital_footprint, last accessed 2019/02/10.
2. O. Heitmann, “Digital investigation: The malnourished child in the Norwegian police family?”, Master thesis, Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, 2019. [Online]. Retrieved from: http://hdl.handle.net/11250/2617759
3. Lov om rettergangsmåten i straffesaker (Straffeprosessloven), 1981. [Online]. Retrieved from: https://lovdata.no/dokument/NL/lov/1981-05-22-25
4. A. Årnes, “Digital forensics”, fall 2016 edn, NTNU, Gjøvik, Norway
5. M. Gjerde, “Victims of success? Knowledge discovery amongst digital forensic investigators in the Norwegian police districts”, Master thesis, University College, Dublin, 2007.
6. Lystad et al., “Politi- og lensmannsetatens kapasitets- og kompetansebehov de kommende ti-årene”, Politidirektoratet, Oslo, 2017. [Online]. Retrieved from: https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/bemanning-ressurser-og-dekningsgrad/bemanning-og-dekningsgrad/politi--og-lensmannsetatens-kapasitets--og-kompetansebehov-de-kommende-ti-arene.pdf
7. Politihøgskolen, “Fagplan for Bachelorstudiet BIII Studieåret 2014/2015”, 2014. [Online] Retrieved from: https://www.phs.no/Documents/5_Studenter/Fagplaner/Fagplan%20B3%202014-2015.pdf
8. Politihøgskolen, “Studieplan videreutdanning i etterforskning”, 2017. [Online] Retrieved from: www.phs.no/Documents/2_Studietilbud/3_EVU/Studieplan%20Videreutdanning%20i%20etterforskning%20VEF.pdf?epslanguage=no
9. S. Andersen, “Technical Report: A preliminary Process Model for Investigation”, 2019. [Online]. Retrieved from: https://doi.org/10.31235/osf.io/z4wma
10. A. Gogus, “Bloom’s Taxonomy of Learning Objectives”, pp. 469-473, 2012
11. 2019 Data Breach Investigations Report. Available at: https://enterprise.verizon.com/resources/reports/dbir/, last accessed 2019/05/18