Master Thesis

Master Programme in Network Forensics, 60 credits

Is the chain unbroken

- a pilot study of the local police use of IT forensic processes

Thesis in Digital Forensics, 15 credits

Halmstad 2020-06-22
Ove Andersson

HALMSTAD UNIVERSITY

Is the chain unbroken?

- a pilot study of the local police use of IT forensic processes

by

Ove Andersson

Supervisor: Stefan Axelsson

Abstract

This work is done in cooperation with the Halmstad local police. We examine how seized phones are handled throughout the organisation. We investigate where and if there can occur issues with the physical device handling and we also look at how the extractions made on seized phones are analysed and the possible problems with that work.

We have interviewed several employees, both sworn and unsworn staff, we have looked at provided statistics and done thorough background research in this field. The comparison and analysis of the material show that the evidence integrity and the chain of custody stand comparably firm. We do on the other hand see issues with the knowledge level in the IT forensic field, the wish for more training, the lack of knowledge sharing between groups and the risk for missing crucial evidence due to these issues. We also look at some possible ways of meeting the risks mentioned by investigating the newly employed IT case administrators and how that has turned out. At the local police stations, these persons solve issues that needed addressing but were previously neglected due to lack of knowledgeable staff. The suggestions on adding these types of employees address some of the issues with extraction analysis. The paper also proposes some possible solutions to some of the problems mentioned.

Word translations

This work is written in English but is about the Swedish police force in the Halland county. All the interviews have been conducted in Swedish. The translations are made by us. Below is the translations used for some of the concepts used in the thesis.

Gruppchef - Group manager
Beslag - Acquisition
Beslagshantering - Acquisition handling
IT Handläggare - IT case administrators
Grova Brott roteln - serious crimes unit
IT forensik avdelningen - IT forensic unit

Figures

Fig. 1 - *Generic process model after Årnes(2018)*
Fig. 2 - *The number of devices in average per analyst*
Fig. 3 - *The imagined flow of a mobile device from acquisition to prosecution*
Fig. 4 - *Number of errands (crime reports)*
Fig. 5 - *Number of examinations*
Fig. 6 - *Number of units examined per errand*
Fig 7. - The product of errands and examinations

Introduction **5**
Purpose and goal 5
Research questions 6
Limitations and problems with the Research questions 6
Ethical and judicial considerations 7
Background **7**
Initial steps 7
Related Research 9
Forensic processes, are they for real? 9
Organisational dilemmas 12
Conclusions from the background research 14
Research questions 15
Methodology **17**
Results **20**
Introduction 20
Statistics 20
Interview study 23
Talking in the interviews 24
Local police in Varberg 25
IT forensic unit, Analysts 26
serious crimes unit - Investigator 27
serious crimes unit - Case analyst 29
Prosecutor 31
Local Police Falkenberg, Varberg, Group managers 32
Results summary 33
Discussion **35**
Conclusion **39**
Future work **40**
Acknowledgement **41**
Reference **42**
Interviews **44**
Appendix 1 **45**
Appendix2 **46**

Introduction

IT Forensic processes is a vast subpart of the even larger IT forensic research area. IT forensic is usually seen as a mainly technical area. But, doing technical work needs structure and order for the work to run smooth and efficient. Here is where processes and guidelines come in handy. Processes also help to keep the chain of custody intact and make sure the evidence integrity is preserved. How this topic came to be investigated in this thesis is described in the background chapter. The work performed has been conducted during the dreaded covid-19 pandemic, which complicated matters somewhat. The interview study was, on some occasions, done in person. We held the other interviews over the phone and on skype.

The work consists of three major parts. First, we made a thorough background research study of essential pieces of the IT forensic field. The material was somewhat hard to come by since this area is not very well researched. The papers we could find was highly relevant and gave us useful insights into different countries police forces. Second, we analyse the provided statistics and discusses the results of that analysis. Third, an interview study has been conducted. We summarise every interview and present suggestions made by the respondents. We also make an analysis where we compare the answers given by the respondents.

In the thesis, we then discuss the findings that have been presented and finally we conclude the work with a few suggestions for the Hallands police force.

The respondents are all working at the Hallands police force, the majority in Halmstad. They represent different parts of the organisation, according to the initial idea of following an acquisition from the actual seizure of a mobile device to prosecution. The approach contained the assumption that the crime committed (where the phone was seized) was of a graver character, so the evidence gets evaluated by the serious crimes group, which is the investigating unit in our case. All interviews were conducted in the Swedish language. We have done all translations to English.

The major part of the interviews is recorded. We decided not to make transcriptions of the discussions but only to summarise them. The reason for that is time constraints and some technical issues. Each recorded interview is between 45 minutes to over one hour long, and in a few cases, the recording did not even work, so we are just stuck with notes from the occasion. The relevant information and answers are still in the summaries.

Purpose and goal

The work is carried out to investigate whether the Halland police force is employing any IT forensic processes. The main goal is to see if there are any issues with the chain of custody and evidence integrity.

We also want to examine, lest there are no processes in place, whether the extraction of evidence still works and if there might be beneficial to implement any processes in that case.

More generally, we hope that this work will be able to help the local police to identify limitations in today's way of working and collaborating across group borders. We also hope that this report can induce discussions aiming to make the workflows and the investigative processes more streamlined.

Research questions

The developed research question that has guided the work is:

> *"Has the Halland local police an IT forensic process that supports the chain of custody, evidence integrity and is effectively sharing the results and knowledge from the investigative process to relevant colleagues or groups in a correct judicial way?"*

This question is more described in the Background/research question section. As another guide for our work, we set up two hypotheses:

1. Through the studies, we will find holes in the chain of custody (the chain IS broken) or issues with the evidence integrity. We will also find some failures in the handling of the evidence where (hopefully) simple measures can mitigate these problems.
2. The police have significant issues with the number of acquisitions and the features of modern mobile devices.

Limitations and problems with the Research questions

In this work, we need to rely on the respondents' answers exclusively, and we need to trust the statistics that have been provided to us. We also have the distinct disadvantage of not being police staff ourselves, talking about processes and work routines we see this from the outside and do not have the full picture regarding conducting police work and criminal investigations.

Investigating processes is a vast area within an even larger field of IT forensics. We have been limiting the research only to cover the local police view on IT forensics. We also try to focus on mobile device handling and not general IT forensic work. We also considered to include Forensic readiness within the examination of processes, but we decided to exclude that part from the investigation. Forensic readiness is not the focus of this paper, and it is only mentioned once across in this thesis.

This thesis is touching the subject of training of the police officers. Some of the background papers investigate the IT forensic knowledge level of the staff. The fundamental police education that is taking place at the police academies is not either in the scope of this thesis. It would, though, be interesting to evaluate and compare with Norway police training and the possibilities for higher education within the police.

We are also, as is stated, focusing on the local police and how the current work is organised and performed. Another limitation to this is that we are not touching the police reorganisation and what the implications have been, or will be for the local police districts. During our work, we had indications that the work is not performed in the same way all across Sweden, which was one of the thoughts with the reorganisation.

Ethical and judicial considerations

We have decided to keep the respondents anonymous. We also stated at the beginning of every interview that we were not interested in actual persons or cases but were only interested in the work on a meta-level. In conjunction with this statement, no persons or real-life cases are to be mentioned in this thesis unless they are mentioned in the background research or other publications.

We recorded some of the interviews to have as a support for a failing memory. These recordings are to be deleted once this thesis is approved, finished and presented.

When looking at the possible implications of this work, we have been cautious not to disclose anything that might be sensitive. The head of Serious crimes has checked the interview summaries in the report. She approved the use and claimed that most of the methods used are already published on the internet. The individual summaries of the interviews have been approved by the respondents as well. We would not want this work to be used by “the bad guys”, and in accordance, the individual staff members are to stay anonymous, and several persons have checked the text, so it does not contain anything sensitive.

On the other hand, you could argue that the findings could be sensitive in themselves. The wrong persons might exploit the lack of training and the urge for more knowledge among police staff within this field. Even with this argument, we feel that the results are too significant for the police organisation not to consider when planning the future work.

Background

In this section, we are describing the background for the work conducted, covering related research in a summarised literature review and also how the process started. We then explain how the research question, presented above, was formed.

Initial steps

The basis of this work is the initial meeting we had with the serious crimes units group manager, Cecilia Bergsten, at the Halmstad police (Bergsten, 2020). The short discussion we had led to several questions which are partly covered below in this section and more in-depth in the research question section. The concerns that emerged during our discussion are briefly the following:

1. Extracted information from mobile phones differs between extraction methods.
2. Unlocking the phones for extraction is the biggest problem.
3. Extracting data from cloud storage which is mainly a legal issue.
4. Raised concerns regarding the chain of custody and evidence integrity.

When we reviewed the separate points, we soon concluded that the 4:th point of concern was the basis for the other three. With this, we mean that all the different aspects are important but if the chain of custody and the evidence integrity cannot be guaranteed to be intact this will impact the possibility to reach a conviction in court. Evidence must be indisputable and possible to explain intelligibly in a court of law. Below is a more thorough explanation of the different issues discussed.

Examining the points one by one gives the following;

1. Extracted information from mobile phones differs between extraction methods.

- This is a technical issue dependant on the different software/hardware vendors supplying the extraction software/hardware. If we were to examine these issues, we would need access to software that is extraordinarily expensive and is continuously used in the IT forensics unit. We would also need access to data that contains information that is parts of real investigations. The impact of such a study is also somewhat unclear to see. We do not even know how big of a problem it is.

2. Unlocking phones for extraction is the biggest problem.

- This is also a technical issue where the skills of the individual IT forensic, and (if an older phone) the capabilities of the cellular phone password cracking software. There is also newer legislation in place, which might help the IT forensic staff to be able to use more forceful methods to get the passcodes to mobile devices; Riksdagen(2020).

3. Extracting information from cloud storage which is mainly a legal issue.

- The cloud is a constant headache for law enforcement agencies in Sweden and the rest of the world, which research shows, Leukfeldt, R., Veenstra, S., & Stol, W. (2013). The current stance is that - the cloud is untouchable and the only way to handle the phone is to put it in “flight mode” and extract what’s in it when in that mode. The big issue here is legislative.

4. Concerns regarding the chain of custody and evidence integrity

- We discussed the chain of custody and the evidence integrity of digital evidence briefly (Bergsten, 2019). We concluded that if the chain of custody cannot be trusted, all the other points of discussion are affected. I that sense not being able to trust the chain of custody affects the other issues, meaning that the evidence extracted could be unusable in a court of law.

We decided to pursue the concerns raised in point 4. We made plans on working to find background research, study that and then to perform interviews on the matter of how an imagined acquisition is handled throughout the organisation.

We wrote a proposal and presented that to the group managers for the serious crimes group and the IT forensics group. We decided to go along with the research, several persons were appointed respondents, and Cecilia Bergsten agreed to help as the police contact. Some points in our wish list were removed due to judicial, organisational and pandemic reasons.

Related Research

In this section, we analyse the found, hopefully, relevant research. We are first talking generally about the processes, and then we will discuss the organisational dilemmas of cyber policing.

Forensic processes, are they for real?

The forensic method or process is an evergoing evolving work that has been discussed for a long time. The classical physical forensic techniques have been used and evolved over many thousands of years—the digital counterpart for not so long (Årnes, 2018). Several suggestions for a process covering all the part in a forensic investigation has been presented over the years. The ones we have studied show similarities in that they are based on several steps, phases or similar. One example of a generic process model is shown in Fig 1.

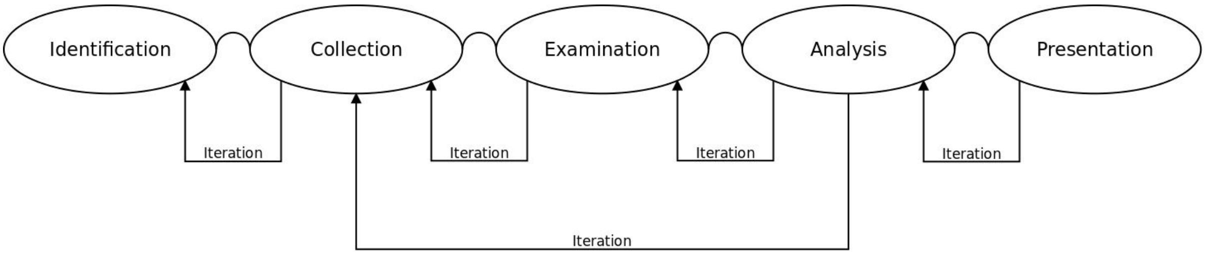

Fig 1. *Generic process model after Årnes(2018)*

In this model, the steps in short consist of:

1. Identification - The initial step where the crime committed is discovered in some way.
2. Collection - The device acquisitions are made.
3. Examination - The phase where the information is extracted and the device specialities are considered.
4. Analysis - the data retrieved is analysed, and the evidence is documented and collected.
5. Presentation - the findings are presented in a way that is possible to understand for non-technical persons.

The process flow goes from left to right. The model allows the investigator to return to a previous step if needed for some reason.

There are numerous process models formed by other researchers. For instance, Goel, M., & Kumar, V. (2019) have created a 7-layer process model. The layers described are:

Layer 1: Prepare and strategise
Layer 2: Crime scene detection
Layer 3: Seizure and preservation
Layer 4: Extraction and acquisition of data
Layer 5: Examination and Analysis
Layer 6: Reporting and documentation
Layer 7: Close the case

We will not go into depth with the different layers but can see that these layers can fit into the "generic" model above. The first layer is regarding the concept of forensic readiness; which is an important concept. The investigative authority needs to be prepared for upcoming criminal activities. This concept is discussed in this particular paper and several other research papers. It is an important area, but we will not cover it in this paper.

The other proposed models' framework can be fit into the generic one in the same manner with a slight adaptation. In the Hunton(2010) paper, he offers a model which should incorporate other parts than only the technology used in an investigation. As he puts it:

"However, investigating cyber-related crime requires a much broader understanding of the wider context specific to a criminal investigation before it can be established just how and what technology is relevant."

This means that IT forensics is only one part, though in many cases an essential or even crucial part, of an entire investigation. The other proposed methods or processes are not in full, concerned with the whole picture but tend to lean heavily on the technical side of IT forensics. A holistic view on the crime investigation where all parts in the investigative work are considered would be a good start. In Carrier, B., & Spafford, E. (2003), the author links the "physical" crime scene with the "digital" crime scene. They are introducing the latter as "a door to another room". They also argue that the investigative principles of both types of crime scenes should adhere to the same kinds of policies in acquiring the evidence, regardless of whether digital or physical.

In Carrier, B., & Spafford, E. (2004), the main focus is on the digital crime scene itself. The authors claim that there are similarities in digital crime scene examinations with physical ditto, and the examinations could be performed similarly in regards to guidelines and documentation. From these presumptions, they have developed their event-based framework. Each event has clear goals and requirements and is divided into five simple phases.

In another research, Adams(2012), the study lean towards the acquisition itself. The goal of the study is to create process maps for all parts in the work to acquire digital evidence from a crime scene. This process is modelled in the Unified Modelling Language, UML, which is primarily used in software development (UML, 2020). The 'ADAM' as the method is named, is claiming to cover the entire workflow when it comes to digital evidence acquisition.

The review above is covering some of the processes and methods studied. But we have not found any evaluations of IT forensic process method that actually used or how well they work. In the Advanced Acquisition Model (ADAM) (Adams, 2012), the author claims the Australian police is using the model. There are papers describing some law enforcement departments which are using parts of models or methods. In the UK, triage, which is a formalised method for prioritising the acquired digital devices and their evidence, is used as a method of diminishing workload for the It forensic staff (Wilson-Kovacs, D., 2019). The problem here is that of getting trained staff to keep using the triage method. Properly using triage makes the backlog and the amount of work for the IT forensic labs lessen by a significant amount. Apart from that, we are not able to find papers covering the use and the following analysis of the gain in using a specific IT forensic model.

On the other hand, the non-use of models can be found in the research, eg. Willits, D., & Nowacki, J. (2016) and Lundström, J & Wirman, J.(2018). The main issue found in these papers is that of the staff not getting proper training, and a more experienced colleague gives the introduction they get. The formalised way of performing the actual forensic craft is taught in a "show and tell" manner and is not formalised or written down. The work in the cybercrime units described is done professionally. The devices are mirrored and extracted in a way that makes the investigators able to analyse and find evidence from the information obtained. This is though done without the support of an IT forensic process method.

Let us move forward and see how the IT forensic evidence is treated given law and keeping the chain of custody intact. The Rethinking Digital Forensics, (Jones, A., & Vidalis, S.,2019), is talking about the digital forensics and a paradox in that a court of law in a common law system, is not usually accepting evidence that is not conforming to the Daubert principle. The Daubert principle - in a very short explanation - states that for a piece of evidence to be accepted in a court of law, it must adhere to the basic scientific rigour such as a published paper, peer-reviewed etc. According to Jones et al., most digital evidence cannot live up to those standards due to how the field of IT is rapidly evolving and usual digital problems like the size of today's storage media and volatility of evidence in, e.g. mobile phones. The research is not in sync with the rapidly evolving world of IT forensic. Jones, A., & Vidalis, S. (2019) continues to discuss other issues such as the possible error rates for extracting tools, and the problem with the output from extractions of mobile devices done with different tools, not giving the same results. The authors argue that since the tools used are proprietary, there is rarely any research done on the reliability and no published possible error rates either. Årnes(2018) suggest that a:

> *"Dual-tool verification can be applied as a means to detect errors from one tool by using another tool to confirm the results."*

This is one way of mitigating this problem which is also mentioned in Jones, Vidalis(2019).

The knowledge among the staff in the IT forensic field is researched in two papers from the Norwegian police academies master programmes. Heitmann(2019) sets up tests where the respondents first get an assignment and then gets to self assess how comfortable they feel with this assignment. The knowledge varies significantly between the respondents. This is described in length. Heitmann also describes several frameworks where different roles in the police force have been assigned the preferred types of competencies that this role should benefit from. This matrix is constructed by the European union competency framework. The (Erlandsen, 2019) is describing the knowledge among prosecutors in Norway within the field of IT forensics. The prosecutors get cases and the assignment to identify the most critical pieces of evidence. Just like they would prepare a case for presentation in court. The tasks were complex, fictive, but realistic cases. They were also interconnected with each other. The prosecutors were well educated, law school and the introductory prosecutor course that is provided to all Norwegian prosecutors.

Both the Heitmann paper and the Erlandsen paper show that the police officers and the prosecutors have shallow knowledge in IT forensic. For instance, only a few of the prosecutors were able to find the planted pitfalls in different cases.

In the Norwegian police academy, IT forensic training has become a prioritised area. The basic police training has courses in different IT forensics areas, but the knowledge is still not widely spread in the organisation

Organisational dilemmas

To extract information, analyse and present how it all came by, there is a need for a supporting organisation that can handle a large number of mobile devices and have the procedural and technical knowledge to perform these tasks. There are some papers regarding specialised cybercrime units and how they function and are organised. The different research papers describe a landscape of overwhelmed cybercrime units where there is a backlog of more than a year Gogolin(2010). High-rank officers in the police, claiming that the IT-related crimes are tough to solve Willits, D., & Nowacki, J. (2016). Other discussions are about the jurisdictions regarding cloud-based crime Leukfeldt, R., Veenstra, S., & Stol, W. (2013), Jones, Vidalis(2019) and even discussions whether Cyber Crime/IT forensic units should be separate departments Jones, Vidalis(2019). The organisational theories also talk about “organisational invention” as a way of dealing with the profoundly changing world of IT and It forensics. Some papers describe how slight changes in the organisation and staffing in cases can improve the rate of cases going to prosecution and subsequently, even conviction Hansen, H.A., Andersen, S., Axelsson, S., & Hopland, S. (2017).

Talking about public opinion and High-Rank police officers that agree with the claimed fact that cybercrime is difficult to solve is countered by Willits, D., & Nowacki, J. (2016):

> *“Though the media and police leadership suggest that police struggle to address cybercrime, it is worth noting that perceptions of the police’s ability handle cybercrime do not prove that police are ill-equipped to address cybercrime.”*

The police have, in many cases, high ability to address the IT-related crimes and are continually developing skills in this area. The issue here might be that the high-ranking officers have trouble understanding the rapidly evolving IT forensic field.

If we generally look at the papers describing how the specialised cybercrime units are constructed and used, we can in almost all cases see that the persons working in these units are asking for an increase on staffing. They consider the workload overwhelming, and that the management does not understand the unit’s importance, and why the increase in personnel is needed (Harkin, D., Whelan, C., & Chang, L.,2018). The upper management is, according to Davis(2012), crucial for the development of cybercrime units. Their support is also vital in managing the groups already in place and working. Without devoted and knowledgable management, at least on an overview level in the IT forensics field, a specialised cybercrime unit is prone to failure and eventually to be closed. Another opinion that is often raised is that there is a lack of knowledge development. The Harkin, Whelan, Chang(2012) paper describes this by a quote by one of the interview respondents:

> *“There is no training for a lot of the stuff here. You just bring the skills with you. SO whilst we are a technical unit there is no training. You know it’s crazy.”*

Even in the Wilson-Kovacs, D. (2019) paper about triage use in the UK, the problem with upholding the knowledge achieved proves to be a challenge. The officers learning the triage skill may use it a few times and then do not get the opportunity to practice it for a long time. When needed, the knowledge is forgotten, and the skill is not there as it used to be. The digital crime tsunami, Gogolin, G. (2010), describes an officer that got proper IT forensic training but was assigned other types of cases for over a year. When that officer was awarded the proper IT forensic case, he had forgotten the knowledge and practice, and the licenses for the software needed had expired. The Leukfeldt, R., Veenstra, S., & Stol, W. (2013) raises concerns about the knowledge among the responding personnel. They describe it as “A deficit in knowledge when registering the offence”. They continue to claim that officers in the Netherland police consider the cybercrime cases inferior to “ordinary crime”. So less focus among the officers will result in less or no convictions due to not investigating or not correctly handling the offence.

Talking about the knowledge that is not upheld routinely leads us naturally into the discussion of more intelligent systems to support the officers in work to be done. The Irons, A., & Lallie, H. (2014) paper discusses the background to evolving more intelligent systems and mention among other things a large backlog of examinations, increased sizes on data sources and issues knowing what information is relevant and where to find it. The authors discuss AI and related techniques and highlights that they might be the way to go in the future of IT forensics. James, Gladyshev(2013) are also talking about using automation and the problem of keeping the knowledge on a high level among the IT forensic practitioners. The authors argue that automation risk to “dumb down” the profession if implemented poorly, but if used in the right way, in combination with skilled professionals, the results are shown to be increasingly better.

The increased workload is discussed in many papers. In Alawadhi, I., Read, J., Marrington, A., & Franqueira, V. (2015), the researchers have gone through 12 years worth of cybercrime records at the Dubai police force. They note a significant increase in examined devices per year. Figure 2 shows the number of devices every analyst is handling on average per year in the cybercrime force. We construct the chart from the data in the paper.

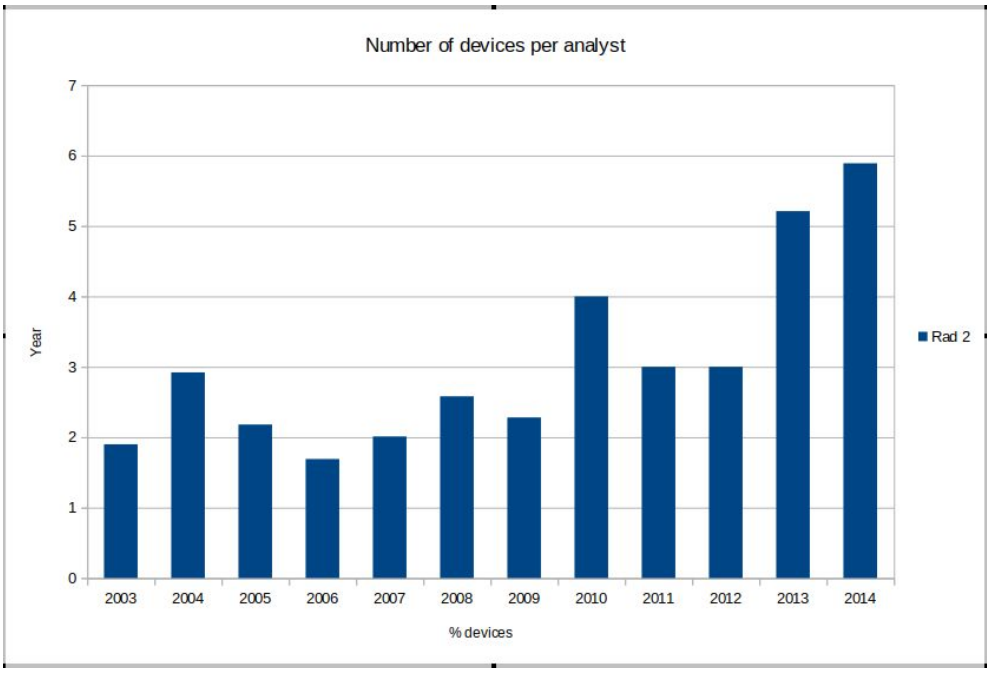

Fig 2. *The number of devices in average per analyst.*

The graph shows the devices handled by each analyst has increased from just below 2 in 2003 to almost 6 in 2014. If we then also consider how cell phones get more advanced and get more storage space, a fair assumption is that the workload has indeed increased.

The paper also describes the number of cases as increasing correspondingly, from below 100 in 2003 to around 900 in 2014. So the number of devices per analyst has tripled over 12 years. There has been no staff addition during this time, which shows that the workload has increased over the years.

Conclusions from the background research

The papers on IT forensic processes describe formalised models where the different phases/stages/levels are described. Responsible persons and the necessary forms are decided. What should have been done is also described. Formalising the work in phases give lesser room for mistakes and produce a more streamlined workflow.

The reviews show that even though there are different flavours of ideas, the various authors share the same view on the complexity, the problems with the digital acquisition, and the need for structured work methods where information sharing is vital.
The papers show a general lack of consistent knowledge in the IT forensic field, and in some cases, even indicates that IT crime is considered inferior to ordinary crime.

On the other side, there is no research done on how the extracted data is handled and analysed by the receiving investigators. The lack of research is also evident when it comes to how different departments work together. The general level of education in the field of IT forensic (and by all means, the general knowledge level of IT) is also not examined in any noticeable degree.

Ordinary police work has developed and evolved over many years with the police staff well-educated in this trade. The area of IT forensics is relatively new. The combination with the rapidly increasing amount of devices, the increased complexity of the digital devices and the increasing storage space is a challenge for entire police organisations and in particular "ordinary" police staff that do not have the specific knowledge of IT forensics. Papers describe how IT forensic knowledge is not well spread among the police staff.

Research questions

With the research reviewed above and the initial meetings with Cecila Bergsten, head of serious crimes unit, we have formulated the guiding research question below:

> "Has the Halland local police an IT forensic process that supports the chain of custody, evidence integrity and is effectively sharing the results and knowledge from the investigative process to relevant colleagues or groups in a correct judicial way?"

The research shows that police authority in other countries are facing the same issues as we suspect the Halland police are experiencing. Some of the proposed further research in the studied research papers are as follows:

> *"This study addresses the critical need for more research on the experiences of police staff as they engage in cyber-policing, Willits, D., & Nowacki, J. (2016)."*

and,

> *"Therefore, it is recommended that more research be conducted to gain a better understanding of how rapidly-evolving technologies will alter the response of law enforcement in the future. Davis, J. (2012)"*

These quotes point towards an interest in knowing more about how the IT forensic field is perceived on individual staff members level and how the ordinary police can cope with the evolving IT field. The research and the initial discussion also shows that the workload has increased. When we defined the problem areas, the outstanding question after the meeting was, can this be true? If the chain of custody is indeed broken, all the evidence extracted in this broken chain will be affected. Below we have formulated one of the working hypothesis according to this question.

Another thing we got interested in was if the local police have or are perceiving a high workload. The background research indicates that it is so. Hence the second hypothesis. We then deduced the guiding research question above according to what we suspected to find and what the background research indicated. We also drew heavily on the discussions of the first meeting since those seemed relevant and vital to the police organisation.

The hypothesis below is to be considered a work directive. They will guide us towards the correct way to answer the research question in our examination of the Halland county Local Police regarding the handling of mobile devices and the possible evidence to be extracted. The hypothesises are:

1. Through the studies, we will find holes in the chain of custody (the chain IS broken) or issues with the evidence integrity. We will also find some failures in the handling of the evidence where (hopefully) simple measures can mitigate these problems.
2. The police have significant issues with the number of acquisitions and the features of modern mobile devices.

Methodology

This work is performed by a literature review, statistical analysis and a series of interviews. The literature review is presented in the Background chapter, and we will refer to the research studied in the Result chapter when we start to show the result of our findings.

The literature review has been presented in the previous chapter and shows issues with the work with cybercrime in different parts of the world. The research mainly focuses on the pure cybercrime units and not exactly how the ordinary police handle digital devices in general and mobile ditto in particular.

The question we will focus on is whether the police has a way of dealing with digital evidence emanating from mobile devices according to the research question raised in the introduction chapter above. The hypothesis formulated works as guidance towards answering the question itself.

The IT forensic team provided the statistics which we will evaluate, present and discuss the result of the evaluation. We will refer to relevant research in the analysis of the statistical data. The statistics are stored in excel files and covers four full years worth of cases. We were not able to get more than four full years and the first few months of 2020. Before 2016 the police organisation looked different because the nationwide police reorganisation took place in 2015 (*Justitiedepartementet, 2014*). The statistics, if any, were not possible to obtain for that period, at least not in an easy manner.

The interview study performed is inspired by *Harkin, D., Whelan, C., & Chang, L. (2018),* but the manuscript we have put together are aiming towards our research question and with the basis in the thought-up flow of the mobile device. We have also considered the further research topics as is described in *Harkin et al,* and in the *Lundström, J & Wirman, J.(2018)* paper. We focus our work on the processes, methods or guidelines used in the police work and if the chain of custody is unbroken. The interviews are not to be considered statistically relevant, but the quality of the interview discussions will show a direction which might need to be investigated further.

In *Willits, D., & Nowacki, J. (2016)*, they are talking about “organisational innovation” we wanted to find out whether the positions as IT administrators were such an organisational innovation and if these positions could be used for solving some of the issues that could surface during the research. We ask the group managers for the local police in two precincts about their view on how the positions came about and what they think about the outcome. We also talk about how they want to develop this position in the future.

The Statistics and the interviews are then evaluated and contrasted with the background research to see if there are any common grounds or possible contradictions between the two.

The entire thesis builds on an idea of following a made-up suspect device from acquisition to prosecution. The flow consists of a device which is physically apprehended. Then show that the information is extracted and subsequently, how the data is analysed. Figure 3 shows the imagined flow of an acquired cell phone. This flow chart is, of course, a VERY simplified model. There are details we do not need to disclose and also somewhat irrelevant details that are not added and things we do not even know anything about. A mobile device in an investigation can be acquired in many ways, and the following handling of it can also be done in many different ways.

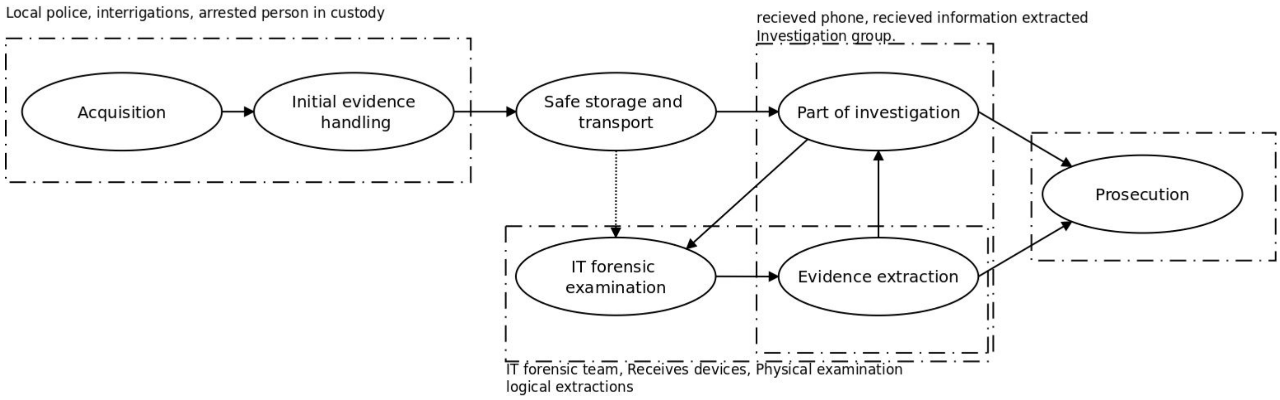
Local police, interrigations, arrested person in custody
Acquisition
Initial evidence handling
Safe storage and transport
recieved phone, recieved information extracted
Investigation group.
Part of investigation
Prosecution
IT forensic examination
Evidence extraction
IT forensic team, Receives devices, Physical examination
logical extractions

Fig 3. *The imagined flow of a mobile device from acquisition to prosecution*

This illustration is supposed to be a mental representation of a thought-up flow of a mobile device through the police organisation. It is thought to be used as a way to visualise how the phone itself, and the data/evidence is handled and where the possible issues might occur.

At the far left, the acquisition is handled by the local police, and they are also taking care of the initial, physical, evidence handling. It is the proper “bag and tag” protocol that is happening here. The crime itself is conducted outside of this figure.

The device is transported securely either to the investigative group or to the IT forensics unit. The IT forensic unit is doing the extractions and is handing over the data to the investigative group.

The investigative group is set out to analyse the extracted data. Hence the shared oval “evidence extraction”. This oval incorporates both the extraction and the analysis part of the evidence extractions. Here is also where the physical “open the phone and look into it” takes place.

The evidence that has been found is incorporated in the report that is created by the investigative group. The prosecutor is leading the investigation process and has close contact with the investigative group.

The prosecutor takes the evidence to the court, which is not either covered in this picture.

Results

Introduction

From the IT forensic department, we were provided statistics over four years and a few months. The statistics are examined and the data used for statistical calculations. In the "statistics" section, this is more thoroughly described.

The interviews were performed, at first in person, then due to the corona pandemic, over the phone and skype. The respondents were representing different groups at the Halland police force and had both experience and proper knowledge for the respective work assignments. They were both sworn and unsworn staff. The interviews were conducted and the manuscript written with the hypothesis formulated above in mind. The interviews are attended to in the "interview" section.

Statistics

In the *Alawadhi, I., Read, J., Marrington, A., & Franqueira, V. (2015)* paper, the workload is described as an evergoing increase of units needing examination. Even in the *Harkin, D., Whelan, C., & Chang, L. (2018)* paper, the same things are described. Looking at statistics provided by the Halmstad local police IT forensic department, the statistics do not show quite the same picture. As will be shown later in this chapter, the statistical calculations show the perceived increase in workload, rather the other way around.

The statistics cover only four years. The reason for the short period of time is that a large police reorganisation took place in 2015 in Sweden. The local authorities became one national organisation. The statistics from before the reorganisation can, according to the IT forensic unit, be somewhat hard to come by if possible at all. The graphs show the year 2020 as not a full year. The statistics were provided at the beginning of 2020 so that column covers only a few months worth of data. We decided to keep the column. We are using that data to calculate a quote. It can be viewed in Fig.6.

The statistical data contain errands (ärenden). One errand is the same as one Crime Report (brottsanmälan). In one errand there can be several units taken into custody, smart cars, computers and information not located in any device, i.e. internet-based information. Examining the statistic data shows that over these four years, the number of errands does not increase. It is actually a slight decrease in the number of errands as can be seen in the Fig.4.

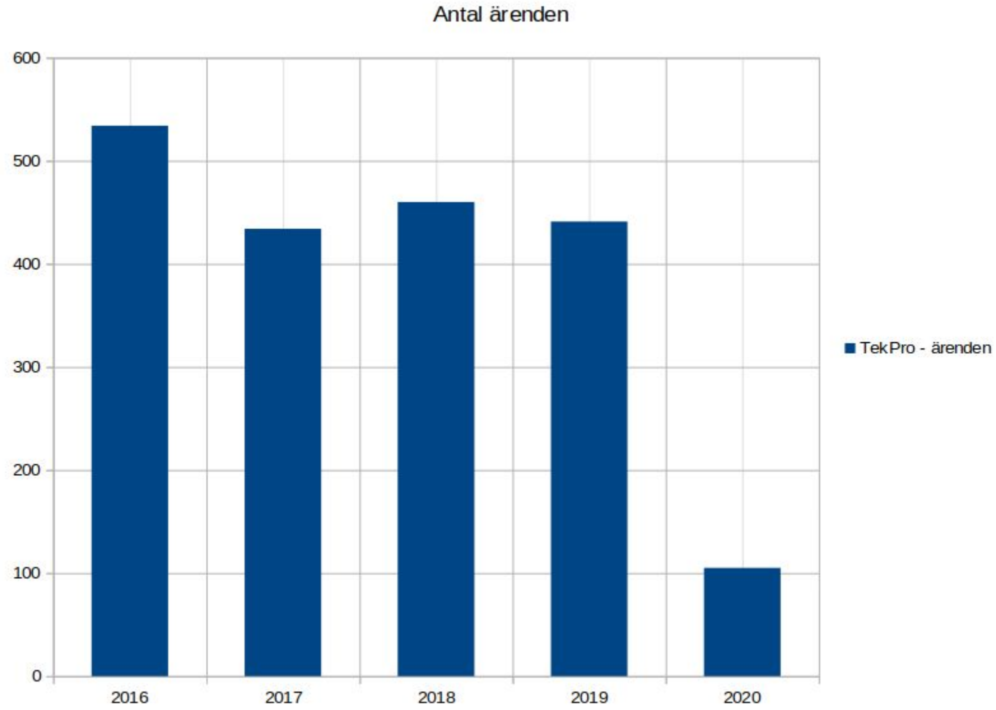

Fig 4. *Number of errands (crime reports)*

Then looking at the number of examinations, we see that the number of them is more or less constant. The examinations, in this case, covers all the different examinations made by the IT forensic group, i.e. mobile phones, tablets, computers, vehicles or internet examinations (Fig.5).

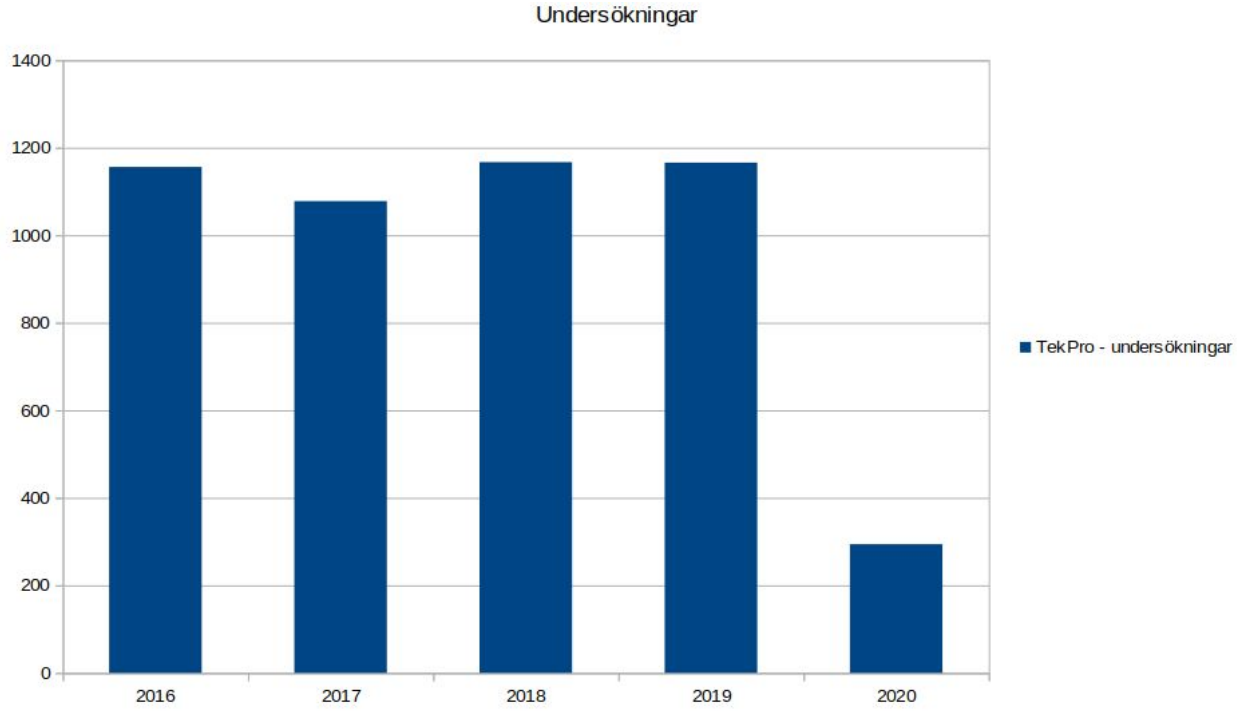

Fig 5. *Number of examinations*

We cannot prove an increase in workload from this statistics extraction, and if we calculate the average number of examinations per errand, we see only a slight increase. True, the increase is apparent and annual, but it increases from 2,16 to 2,8 examinations per errand. But in the same period, the number of errands has in reality decreased. We have no result for the number of errands for the year 2020 so when this year comes to an end it might show another result. This is interesting because we feel that the perceived increased workload is real, and the answers in the interviews support that notion.

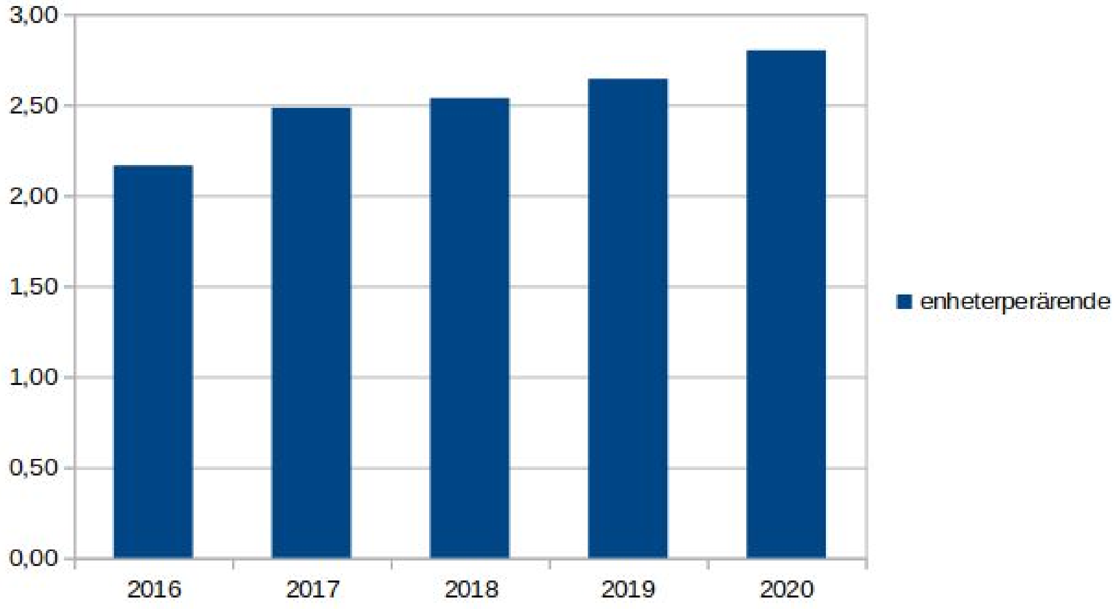

Fig 6. *Number of units examined per errand*

Another way of looking at the calculated workload is to multiply the errands with the examinations. This gives a visual representation of the calculated workload. In this graph, the curve is clearly going down. According to these data, there is no increase in workload (Fig. 7).

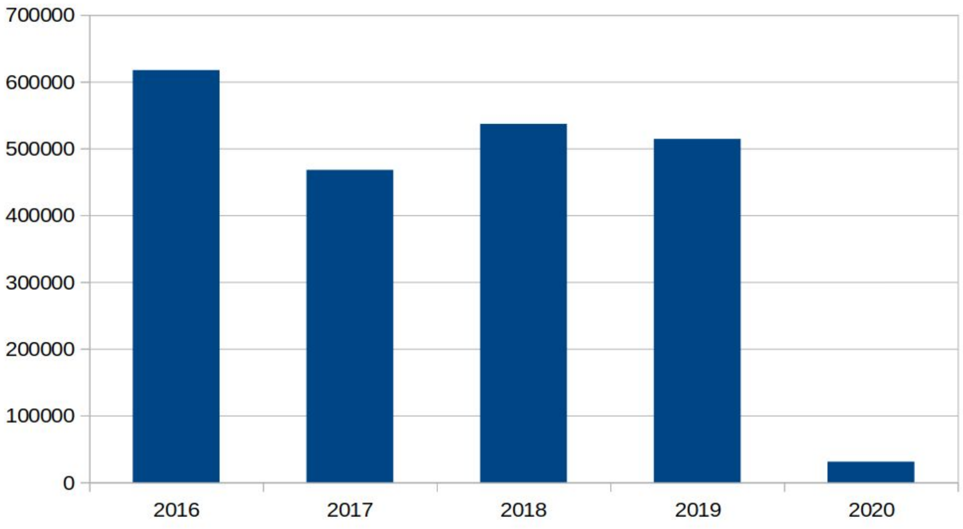

Fig 7. *The product of errands and examinations*

The total number of errands in the material is 1997. The distinction in the material is "open" (öppet) and "finally reported" (slutredovisat). We have not checked the distinction in the material between the different distinctions. Looking at errands per year, the top year in this material is 2016. They hit off with a dashing 543 errands, while in 2019 the number of errands had decreased with almost 100 errands to 441.

The "examination" data are more diverse compared to the "errands" data. The total number of examinations is 4861. The distinction between the states in the material is: "Not started" (Ej påbörjad), "Finished" (Avslutad), "Ongoing" (Pågår), "Not done" (Ej utförd), "Canceled" (Makulerad), "Resting" (Vilande)[1]. We have not looked at the respective distinction and the statistical distribution of those in this material either. The result is somewhat surprising to us. All the interviewees are talking about an increase in devices and an increased workload. The corresponding papers are also talking about an increase in devices and an increased workload for the IT forensics departments eg. *Harkin, D., Whelan, C., & Chang, L. (2018), Alawadhi, I., Read, J., Marrington, A., & Franqueira, V. (2015), Leukfeldt, R., Veenstra, S., & Stol, W. (2013), Wilson-Kovacs, D. (2019), Gogolin(2010).*

So why can we not see this in the statistic material? Just to be clear, we do believe that the perceived increased workload is a real thing; we just cannot see this in the statistics. We have several hypotheses why the statistics look like this. These include increased size of storage media, encryption that makes extraction harder to perform, more locked phones that makes it harder even to enter the phones etc. However, without additional information and research, this cannot be proved. We believe that if the time spent on each examination were included in the data a completely different picture would emerge which in turn would support the background research.

Interview study

At an early stage, we realised we would need information from the staff of the police. In other research, the interview technique proved to be the right way of getting ideas and insights into how the field of IT forensics worked at a local police authority (*Harkin, D., Whelan, C., & Chang, L., 2018).* We wanted to see how a made-up acquisition is going through the organisation from the local police to prosecution. The thought here was that the crime was not to be directly investigated at the local police station but transferred to another team. In our case, we had contacts with the serious crimes unit, so we imagined the actual crime to be more severe. That is why we decided to try to get several different persons from different groups to interview. The groups represented are from a local precinct, the IT forensics group, the serious crimes unit and a prosecutor from the local prosecution authority. The interviews were conducted during the Covid-19 pandemic, which made interviewing in person a challenge. Three of the meetings were actually performed in person while the rest were conducted on the phone and over skype.

[1] Translations are made by us.

A manuscript was compiled as a base for discussions. A disclaimer where the objectives of the interviews were stated. The ethics considered were read aloud at the start of every interview. We then described what we wanted to achieve at the beginning of the meeting. The script can be studied in full in appendix 1.

Four main topics can be discovered in the interview script. First, we talked about the respondent, years in the force, education and title (if applicable). Second, generally about cybercrime and the perceived knowledge in IT and IT forensics. Third, Processes and if or how they are used in the police. Fourth and last, Administration. The interviews were conducted more as a conversation with deviations within this topic. The interviewees were very outspoken, and we had a wonderful time talking to them. We got a lot of concerns, a lot of exciting ideas on how to improve the investigative work and a feeling that they were very dedicated employees, happy to work in the police force. At the interviews, we were careful not to challenge the answers. We did not contradict the expressed notions; we asked follow-up questions where we could. We never tried to "correct" the answers. We wanted the unbiased perception of how the work and the cooperation between groups and individuals work.

Two interviews were done after all the interviews mentioned above. We also felt a need to interview two group managers regarding IT case administrators, and the perceived success, the work the administrators do and what they would like for them to be able to do in a future. These interviews were shorter and covered only the IT case administrator question. The manuscript for that interview is located in appendix 2.

Talking in the interviews

This section will summarise the performed interviews. The order follows the thought-up flow of a seized mobile device through the organisation. The first box is the local police, where many mobile devices get acquired. Then the IT forensics where the seized phone gets extracted, after that the serious crimes unit where the more serious crimes are investigated. Finally, the prosecutor who, in a Swedish police organisation, leads the investigative work and is responsible for the evidence presented in court. The evidence and the report are also provided to the defence by the prosecutors. A note worth mentioning is that even though the thought flow off a seized phone leaves the local police station and, in our made-up case, the serious crimes unit handles this particular device, many investigations are handled locally. The analysis of the phones extracted information is done at the local police station.

The interviews are summarised in the same order as the thought-up flow of the phone is thought to take place. The first interview is the Local police in Varberg. We discuss the acquisition, how the phone or mobile device is handled. And the perceived need for more training. The next interview is with the IT forensics. The discussions drew more towards the actual extraction handling and whether processes should or could be used in the day to day work. Next are two interviews with staff at the serious crimes unit; one of the investigators and one case analyst. They are sharing similar views on how the work is performed and what could be done to make it better. The last person to be interviewed in this set is a prosecutor. He is talking about having good cooperation with the investigating group. He is also mentioning the need for more training.

When the first interviews were done, we got interested in the problems that some of the respondents mentioned. These issues, in combination with the organisational innovation concept described in *Willits, D., & Nowacki, J. (2016),* made us interested in the newly formed positions as "IT case administrator". There are employed administrators at a few local police stations, and there is at least one more being employed at a unit in Halmstad. We decided to interview the group managers at two local stations where they have employed persons for this work to see if that can be one way of addressing some of the issues mentioned below by a few of the respondents.

Local police in Varberg

I talked to the local station officer at the local police station in Varberg, and we started the interview by discussing the acquisitions done by the local patrols. When getting a phone, they most often do not start them or look into the devices. This is the preferred way to do it as expressed by the IT forensics in the later interview. If on a crime scene, they describe the seizure, the surrounding environment and make an acquisition protocol where the device is tagged with a bar code and stored away. This is the proper "bag and tag" protocol. The physical seizure, handling and storage of the devices in that manner is described as "foolproof".

> *"You cannot compromise the device unless you do it on purpose"*.

The physical handling of a device is regulated in legislation and has been developed for a long time. The need for an acquisition to be correctly handled is vital when the evidence reaches the courts. If doubts are raised in how the acquisitions have been handled, there might be problems to convince the court that this evidence is valid. We also discussed the chain of custody, and he was confident that the chain of custody is not compromised.

Talking about the general IT knowledge of the individual police officers, it is described as "not very good". He claims that:

> "The general public is probably better at this than what we are".

He describes the younger officers as having better IT -knowledge and that the current generation will be the last with lower general IT competence. The notion of poor IT knowledge is supported in *Leukfeldt, R., Veenstra, S., & Stol, W. (2013)* where the authors, in that case, describe the investigation of pure cyber crimes as being poorly handled mostly due to lack of knowledge in the IT forensic field.

All the phone extractions are done in Halmstad. The transport fo the device there is handled securely. The order to make an extraction is passed along with the device electronically. The investigating officer needs to fill out the form with the required information. What to specifically put down has, as far as our respondent knows, never been communicated from the IT forensic department. He states:

> *"We don't even know what to put down in the extraction order form"*.

The communication seems to have been missing for a long time. The local police are not educated in what to fill out in the form. We were not able to see such an order form, but we can deduce that the form probably leaves room for interpretations.

A common theme in our interviews is the explicit need and wish for more education within the IT forensic field. That is also asked for here. When this is mentioned and discussed, the respondent gets somewhat concerned:

> *"Now that I am talking about this, it sounds really terrible"*.

The first responders' patrols which in some cases also do the seizing of devices have basic if any knowledge of IT forensics and the acquisition of digital evidence. The need and use for at least primary education in IT forensic and how to treat digital proof are mentioned several times during the interview. The IT forensic support, if asked for, is there, but over the phone. There has also not been any IT forensic analyst at the local police station training the local staff in these things.

The perceived workload with digital devices has increased, and also the number of extraction orders that are sent to Halmstad. The time for the results of the device extractions to reach the local investigator is a significant constraint in the investigation. He expresses the wish to do more locally and mentions that they want the possibility to do more uncomplicated extractions, perhaps on plaintiffs phones during interrogation. That way, the plaintiff would not need to leave the phone for several days or weeks to be extracted by the IT forensic unit in Halmstad. This would also help the IT forensic unit to lessen their workload so that they can concentrate on the more complicated work items.

IT forensic unit, Analysts

The IT forensics group handles the extractions of digital devices. True, their work consists of other tasks as well, but we will focus on just mobile devices and extractions of the same in this work. The respondents are quite newly employed in Halmstad, but they have experience from other regions and police authorities and has an IT forensic university education.

Talking about the workload for IT forensics, they appreciate it to have increased. Today, almost every person has a mobile phone in their pocket, and the storage spaces have become significantly larger. The extractions conducted generate huge files. That in combination with a record in the number of people arrested talks for itself. The perceived workload has increased.

They describe how the focus of the work has deviated towards more mobile units. Just a few years ago, you could find almost all the useful information on a computer hard drive. Today, the data is located on the cell phone in the perpetrators pocket. The information is also often stored in the cloud, with possible encryption techniques added on top of the data. The difficulties of unlocking phones are also a complicating issue.

We discussed processes and whether the IT forensic unit is employing any. At the group, no formalised processes are used. There are training, but it is conducted by a more experienced colleague at least in the beginning and does not contain anything about processes. The method is of the type "show and tell". The difference compared to what the other units describe, is here that the IT forensics has either a lot of experience or relevant university education as a base for the IT forensic trade. The use of processes is also problematised by one of the respondents:

> *"It is hard with routines/guidelines they will get fuzzy if written down. You will eventually get "if you don't follow these guidelines, do thorough documentation", which we do anyway"*.

The respondent means that guidelines or processes will not have an especially significant impact.

Cooperation with other groups in the police is not that evolved. The most contact the IT forensic group has with other units is when they get an order for the extraction of a device. The requests that they receive is often missing relevant data, for instance, what they should focus on, type of data and the time and dates. An order can be of the type: Find anything relevant, which is virtually impossible to adhere to.

Even though the extraction tools are competent, they are not entirely in sync with all the new apps and the databases that these apps are using. There are often some 200 apps that reside in the phone and with the data using different databases is a complicating factor.

The respondents support the notion of education being essential for the other teams. The investigators, patrols and others need to get information and training on what to think about when seizing a digital device, how to do a correct extraction order etc. They need to learn that phones should be sent to the IT forensics untouched, which in all cases are done. They do not see erased phones that often.

The respondents are confident that the chain of custody is not broken, at least not during the time the device in their care. The device is handled, the actions performed are documented, and the extractions made are stored securely.

serious crimes unit - Investigator

Our respondent works as an investigator at the serious crimes group. He has extensive and in-depth experience in the "police trade". His expertise ranges from being driving patrol cars until today's job, working as an investigator at the serious crimes unit. There they investigate the more serious crimes, like murder, arson and the likes. Over the years, the amounts of mobile acquisitions have increased. Today, the seizures and extractions are done in a kind of routine manner. The number of devices and then the size of the storage has increased in the later years. That increases the perceived workload for the investigating team.

Today's guidelines are that the analysis of the extracted information is to be done by the investigators. This is seen as a problem by the respondent:

> *"I can't really be certain that I have found everything that is to be found in this phone that is relevant for the investigation"*.

He describes himself as not very knowledgeable in general IT and that the same goes for IT forensics. The skill of analysing the extractions is considered hard to uphold since there is no continuity in working with it. He explains that there are persons at the group that is better at this:

> *"There are those that are a hell of a lot better than me in finding the information from the phone since I do it, maybe, every third month, or maybe once every six months!"*

There might be another way of dealing with the analysis of the extractions. He raises the suggestion to have one or more resources dedicated to the analysis of phone extractions. This person or persons could also be working as a dedicated resource with investigations just as is suggested in *Hansen, H.A., Andersen, S., Axelsson, S., & Hopland, S. (2017)*. They could then also help the more knowledgeable colleagues with more advanced skills in extraction analysis and other related tasks.

Talking about the extractions, there is uncertainty if they contain all the relevant information for the case. Before, when extractions were made, it was considered to be final. That was it; no more information could be found. Today, there are uncertainties about the content of the extractions. In one case, a suspect mentioned that there were SMS conversations at a specific time, and no such information could be found in the extraction. After having extracted the data once more, it could be found and validated. Not being able to trust the extractions add quite a large amount of uncertainty in the investigating group and, in some cases, generate more work and a longer time to finish the investigation.

When mentioning the extractions, our respondent tells that the reports from the IT forensic group are in many cases, insufficient. They lack phone ID in the form of IMEI, IMSI or even the phone number and they often miss a summary of what was on the phone. The investigators then need to go back and ask for more information or go through the extraction themselves, again. The phones physical identity is always noted through the bar code sticker that is tagged on it at the acquisition time. But that is not always possible to use in the analysis of the extractions.

Processes in the police are nothing that is being discussed. He can not mention any kind of processes that is written down and that they are supposed to adhere to. The cases that are being investigated are very diverse, and there is hard to see a process that could "fit all". Since the group work in close cooperation with the prosecutors, they have a close dialogue on what is needed to take the investigation further. A process for that is maybe not something possible to develop or even relevant.

The chain of custody and the evidence integrity is not at risk according to our respondent. You can find the information on who has handled the phone and where the acquisition took place. The information on who did the extraction and who has looked at the data is also possible to find. The potential issues are, as has been mentioned, whether all the relevant data has been extracted and if the analysis has found all the information that is interesting for the case. The data needs to be stringent and possible to explain to the courts, which generally does not have a good understanding of IT forensics. The information requested from the courts needs to contain even "non-information" to close all possible interpretations of the evidence.

To sum things up, there is a lack of education, and when the training is there, the problem is to keep the knowledge and the acquired skills due to long periods in-between cases where the specific work is performed. There is a request for a new staff member to work with these issues; Device extraction and finding the digital evidence, Helping the investigators with the analysis and other IT forensic areas. The chain of custody is intact, the evidence integrity is also good, but there might be evidence from mobile devices extractions that are being overlooked due to missing knowledge and poor general IT knowledge.

serious crimes unit - Case analyst

The case analyst position at serious crimes are mainly dealing with analysing phone lists, both lists externally acquired from the telephone operators or banks but also the phone extractions themselves. Our respondent has a university degree and several courses in intelligence, intelligence methods and such. She started working at the police 12 years ago with intelligence. After some time she started working at serious crimes and is mainly working with different kinds of phone analysis. She has extensive experience in crime intelligence and feels that this applies to the current work.

Training for this particular job has not been given, more than seminars and lectures internally organised. There is more extensive training that she wants to go, but personal matters have been in the way for that. This training is focused on the practical parts of the analyst work.

There is no basic formal training for doing the phone analysis. The training that the analyst receives is of the type "show and tell", and it is a more experienced colleague that is showing what they know about the craft. So, the analysts are more or less self-taught:

> *"Amateurs teaching amateurs, it is not good!"*

The lack of training and knowledge is compensated by experience. Looking for evidence in an extraction several times make the skill evolve. The analysts feel that they know how to find the relevant artefacts in the extractions. The issue is though, not the extractions, but the sizes of the extraction files:

> *"The feeling is that it is getting more information. It takes more time to go through. In an investigation, the person getting the phone extractions to analyse is getting the rotten apple because of the time it takes to go through the files."*

Taking this and combining it with the fact that it is not only the analysts that are self-taught and lacks formal training in the analysis part of phone extractions but also the investigators, we understand that there is a problem. Our respondent estimates that around 50% of the investigators are uncomfortable with the phone extraction analysis because of lack of skill, or previously acquired but forgotten skills, with the result that the analysis is not done on time. The analysis might, in some cases contain vital information that can be used to get externally acquired information.

We raised the question of automation in the analysis work. The respondent was very hesitative in regards to automatic tools:

> *"Automatic tools where you don't know what you are doing is not super good. You need to know what you are doing. From where you get the information and how you got it."*

There is a knowledge gap between the individual knowledge of the investigators and analysts, and what they are assigned to do. Our respondent raised a valid question:

> *"The extraction files and the information is getting more and more complex and large, is it reasonable that everyone should master that?"*

Also, in this interview, the thought of having a dedicated resource for the serious crimes unit who would focus on extractions, images and help the investigators in these areas was raised. The respondent concludes that there is a need for at least one dedicated resource. This person should partake in investigations which makes him or her updated on the case. He then knows what artefacts to look for in the extractions that are valid for the investigation.

The respondent has a hard time seeing how a process should be formulated to cover all the workflow from acquisition to prosecution. Also, here is mentioned the fact that all cases are different. There is though an idea to develop guidelines or templates on parts of the work. For instance, there exists a process description for how to work with lists provided by mobile operator companies which are created internally. The same should be good to have for the extraction analysis and possibly other areas as well.

The units or groups do not have very much cooperation. They seem to be working in small islands instead of exchanging information regularly. We get a feeling that there is a lack of information sharing that actually affects the quality of the outcome of an investigation. The respondent points on the extraction reports and that they often miss vital information such as IMEI, IMSI or the phone number. Remembering the sticker with a bar code and the acquisition number that always should accompany the phone, our respondent had never heard of that before we mentioned it to her. This small example shows the need for standard training for all the staff that is going to work with mobile devices and the evidence extractions from them. With the acquisition number, the analyst still can not make out which phone it is and the IMEI of the phone. The respondent wants a protocol that contains at least the IMEI. She wishes that the report should include a summary of information, a list of which apps that have been used at a specific time. The number of contacts there are in the phone book, and this type of information should also be listed.

Prosecutor

The last step in the imagined flow of a mobile device and its information is the prosecutor. Our respondent decides to prosecute based on the case and the investigative results. The digital evidence is only one part, sometimes it is crucial and sometimes not that important. Our respondent has a Law school exam and has been working for many years as a prosecutor. He has no specialised training in IT forensics apart from the few lessons in general education as a prosecutor. He would like more training in the subject, a couple of weeks to get to know what is possible. He does not wish for in-depth technical education; the IT forensics are the experts who know the specialities. The respondent would like this knowledge to be able to ask the right questions both in court and to the investigating teams. This correlates with Erlandsen(2019) where it is described as the prosecutors having quite low competence in the IT forensic field. Even there is a need for training described as vital.

The IT forensic analysts are a critical resource, and you need a particular reason as in an unusually severe crime investigation to get that dedicated resource. The IT forensics unit is otherwise used as is described in the previous interviews. The information extracted is left to the investigator to analyse. The investigator thus needs the skill to be able to do that. There are also times when the device needs to be extracted once more. Maybe in another tool.

The number of devices that are present in the investigations is very high. At the serious crimes unit, the rate goes probably above 90%, and in crimes in close relationships, the rate of mobile devices is 80-90%. The number of tools and the increased complexity in the information increases the need for skilled analysts to find and process the data from the phones and combine this with information from other sources.

The work with mobile devices has gotten more complicated. Encryption is mentioned several times during the interview, as one of the more complex issues to solve. In planning a police raid where there are encrypted phones, special care should be taken to this. The legislation on forceful means to get the encryption keys on the phone, like face recognition or using the fingerprint on a suspect does not allow this. Our respondent expresses that it is scandalous that the authorities cannot use these means.

Working as a prosecutor means that you lead the investigation and work in close cooperation with the investigating team. He stated when we lifted the question on the chain of custody:

> *"I am absolutely convinced that the chain of custody is unbroken. If I had doubts, I would have already talked to the investigators about it"*

He is trusting the work that the police is doing, and he feels that he does not have the competence to question the standard methods used by the police. If any uncertainties are discovered, the investigative team are asked about these issues.

Local Police Falkenberg, Varberg, Group managers

With the interview conducted and with the research read, we felt we needed to pursue a track mentioned by several respondents, namely the perceived need for a more specialised resource focused on the phone extractions or other technical insufficiencies. The research also suggests "organisational innovation" as a way of solving a particular problem. In Willits, D., & Nowacki, J. (2016), the innovation mentioned consist of the specialised cybercrime units themselves. We thought of the IT case administrators (IT handläggare) as a form of organisational innovation since these employees will solve a specialised need that the ordinary organisation has problems solving.

As far as we know, there are at least three employed at local police stations in Halland police district at investigative groups, and one is employed at the crimes in close relationships unit but has not at the time for this report started working yet. The respondents for the local police stations were both group managers for the specific groups where the IT case administrators (henceforth, *the administrators*) work.

In the beginning, there was a financial room to develop a new type of employment. The person searched for was "supposed to know excel" which means they should have general IT knowledge, but apart from that, the job was meant to evolve into what was needed. One initial idea was that they would handle media and mainly finding evidence in surveillance footage. The employee was also to be helping the investigators with ordinary tasks in, for instance, excel.

The two precincts have gone in slightly different directions. In Varberg, the administrator has had the opportunity to become a civilian investigator, in Falkenberg, the employee is excelling in finding evidence in image material and in crafting presentations for the courts. Both managers feel that the employees are doing an outstanding job and help the departments in the right way. This was also the main idea with the hiring of these persons.

The Administrators are today helping with more straightforward phone analysis but as one notes:

> *"We are not home yet; we still want to do more locally"*.

Both managers stress the wish to be able to do more at the local police station. And mentions a wish to, for example, be able to do more uncomplicated phone extractions at the local police station. This is because all the extractions are done in Halmstad today. The time a plaintiff is without their phone should be minimised.

It seems as if the IT case administrators are solving the issues the local police investigative groups are facing in a relevant and useful way. The administrators have been given training according to the problems they are supposed to address. Their job is then also helping the not so technically advanced investigators with the issues that before was taking a lot of time due to lack of knowledge, experience or other hardships. The administrator's tasks have evolved in slightly different directions which suits the local groups appropriately.

Results summary

The interviews have given us some interesting and in some cases, unexpected results. We had expected that the perceived workload would be high and increasing. We did not expect that the statistics would not support that notion. The reason for this needs more investigation, which in turn still could show in numbers that the workload is indeed high and increasing.

The chain of custody and evidence integrity is explained and is not compromised. This is not due to the groups and individuals following any specific IT forensic processes but the routine of documenting and presenting the findings in a clear and judicially correct manner.

Knowledge, education and skills in the IT forensic field are not well evolved in the Halmstad police force apart from the IT forensic team staff of course. The eagerness to get more information stands out in all the interviews as a topic that needs more focus and direction. The training required and asked for would not aim to turn all staff members into fully-fledged IT forensic examiners but just to get a more focused knowledge within the specific areas of the individuals work tasks. E.g. the first responders should know more about how to treat digital evidence on a crime scene, how to treat and write the extraction orders to the IT forensic team. The investigators ask for hands-on help with the analysis of the extraction materials, and the prosecutor would like more overview knowledge of the IT forensic possibilities within the field to be able to ask the right questions to relevant persons in the investigative groups.

Talking of processes, no one of the staff can see the need or even a possible method to cover the entire flow of a digital device. Some respondents see the use of guidelines or templates for parts of the process. They mention, for instance, the phone extractions, where a guideline would help the less knowledgeable to at least start the analysis. Adding to this, no team is aware of a specific written process to guide their work in the IT forensic field, not even in an overview level. None of the respondents is describing a formalised way of handling digital evidence. The feeling is "we do as we always do", and in some cases, this is not a feasible way of handling the elusive character of some of the evidence.

Working on a case makes the groups operate in "islands". The knowledge sharing of useful things is not sufficient, and the training of staff in this field seems sadly neglected. A colleague conducted training for many of the respondents regarding the IT forensic field. This was done in a "show and tell" manner. There is no formalised documented training path for fresh employees. One of the respondents calls this "amateurs teaching amateurs" which means that there is a need for the "professionals" to educate the amateurs in IT forensics. The IT forensics unit is the professionals here. On the other hand, the prosecutor is content with the results and trust the results from the evidence analysis. The analysts and investigators have extensive experience, so that is helping the analysis to be valid and correct.

The lack of knowledge sharing can also be seen in the extraction orders and reports that are sent between the teams. The local police describe the order for a device extraction with:

> *"We have not had any information from the IT forensics what kind of information they want us to add to the order protocol for a seized phone."*

The IT forensics respondents, on the other hand, say that they often get extraction order forms that with the request, e.g. to find everything that is interesting. So, on one end the local police say that they do not know what information the IT forensic team want in the order form, and on the other end, the IT forensics get unsatisfactory filled out order forms. This is yet another example that information sharing is not satisfactory. Another example is the reports from the extractions handed over to the investigative team. When an extraction is finished, basic analysis is done by the IT forensic team. The respondents from the investigative group criticised the following report. The report could miss device id such as IMEI; the conclusion could be "Nothing of interest is found". The wish was a more detailed report containing IMEI and more details about the data extracted.

We discussed extractions, and concerns were raised about the uncertainty that the extractions contain all the information. There have been multiple occasions where the investigative team has asked for a second extraction because the information that was supposed to be on the phone could not be found.

The local police have a wish to do more in a local environment. The newly employed IT case administrators, which has been a successful step, could maybe be trained to perform more uncomplicated extractions of, e.g. plaintiffs phone while they are interrogated. The time for them to be without a phone should be minimised.

While we mention the IT case administrators, this possibility is brought up by the investigative team as a possible solution to the problem of upholding the knowledge in phone extraction analysis and such. These IT case administrators could then help with the analysis and other related issues on the departments.

Discussion

The respondents unanimously mention the need and wish for more training in the art of IT forensics. All the respondents are also raising this as quite a big issue. They feel that the level of knowledge in the IT forensic field is not adequate to the tasks they are set to fulfil. There is no formalised training in place, and the training they receive is when a more experienced colleague is showing how the work is done. The notion "an amateur is educating an amateur" is mentioned by one of the respondents. This respondent wishes that "the professionals" teach the IT forensic skills, which means that it is the IT forensic group or similar that should teach about their specialities and on the right level for the individual staff member. In a process model, this step would probably be named Forensic readiness. That is, how to be prepared for when the crimes happen. One way is - training. Forensic readiness is not in the scope for this work, but is an important concept worth pursuing in future research.

The training asked for by the respondents in the "hands-on" skill of the IT forensics that is relevant for the individuals work tasks. The local police has a need that differ significantly from the needs of the prosecutors It forensic knowledge. The interviews show that there also is a gap in the knowledge of what the other groups need. Knowledge sharing, talking to colleagues in different groups with a purpose to spread specific information does not seem to happen that often. The groups are working in "islands" within the organisation and are not sharing other information than the minimum needed to get the investigation forward. A specific example of this is the order for a phone extraction which was seen as a problem for both the local police officers and the central IT forensic team. The apparent conclusion is that one group have no insight into the needs of the other group. Knowledge sharing, training, or just making a phone call would help mitigate this problem. True, the more persistent solution would be training in combination with a proper formalised process with the duties outlined for what information to supply to the other group and the responsibility for this information decided beforehand. Another example is the extraction reports that are provided along with the extraction file. The reports often lack the phone ID in the form of IMEI, IMSI or even the phone number. Due to not entirely understanding what and how the investigating team uses the information extracted, the information in the protocols supplied is not adequate to the need of the receiver, in this case, the investigator or case analyst at the serious crimes unit. A formalised process would have these steps formalised, with the minimum content described and which staff member has which responsibility for what part in the process.

There are also raised several warning signs regarding the analysis of the said extractions. The most crucial is the fact the analysis is supposed to be performed by the investigating team. Many of the investigators at the serious crimes unit are not comfortable with this type of work since these analyses depend on experience and some level of training. Many do these analyses very seldom and with a long time in between and have a hard time remember how to do the analysis. Keeping the level of the knowledge is hard, and in combination with the large extraction files, make the work hard for the investigators.

Another warning sign that several respondents mention is the insecurity if the extraction contains all the information from the phone. There have been occasions where another device extraction had to be done due to missing data in the extraction file. It creates insecurities about the data retrieved and in the long run, more work that needs to be put into the case.

Regardless of the above-described issues, we can not see that the chain of custody or the evidence integrity is compromised. The acquisition part and the transfer to the IT forensics is well documented, and the physical acquisition is according to the local police - foolproof. The extraction work, the work handover to the investigating group, are recorded and reported, even if the report leaves some to wish for, it is done. The evidence extraction analysis seems to be handled appropriately and thoroughly worked through. There is no sign that the evidence is not correctly handled throughout the process.

As mentioned above, the analysis of the extractions is where the possible evidence loss can be found. The device extractions are a vital part of the work with mobile device evidence. These device extractions are correctly performed even though the information in the devices might need a re-extraction. When the investigators get to analyse the file, there are several that are not very comfortable performing this task. The problem here is that the craft of performing the analysis is a skill that needs both initial training and experience. When that knowledge is acquired, it needs to be maintained. The latter is the tricky part when investigators perform the analysis task with a long time in-between occasions. One of the respondents suggested that this particular task is a good starting point for the implementation of a formalised IT forensic process. The extraction analysis is in great need for a guideline or template on how it is supposed to be performed. It can guide the staff in what to keep in mind when starting the analysis, and it could function as a template for more inexperienced investigators. The respondent also asked the rhetorical question - "*is it reasonable that everyone should master that (analysing the extractions)"?* The respondent explained that the extraction files are getting bigger, and analysing get more complicated due to the evolving technology itself. Not all investigators have that knowledge, perseverance, or even interest to learn this field in such detail. We had a discussion with the head of serious crimes unit who was supporting this notion and added more insights. The extractions are getting increasingly technical. The level of complexity is soon at a level too complicated for non-technical staff. The analysis of the extractions will soon need a person literate in IT forensics. These persons have little or no insight in the investigation trade, whereas the investigators have little or no insight in the IT forensics trade. The technically knowledeble staff is hard to come by but if we are supposed to be able to get all the data from the devices they are needed. She also mentioned that a general upgrade of the “ordinary investigative police work” is necessary. The knowledge of how an investigation should be performed is an art which needs training and experience much like the IT forensic trade.

The increase in workload is something that all respondents are mentioning. A lot of research is also describing this issue with overwhelmed cybercrime units and a significant backlog, e.g. Gogolin(2019). The statistics we received from the IT forensic unit are not supporting this picture. According to the supplied statistics, the IT forensic units workload is on the same level, or even decreasing, over the years 2016-2020. The statistics we got had very little detail. A general idea regarding statistics on work performed is that there needs to be a clear idea of what to measure and why you should measure these parts of the work. To be able to use the statistics, to show and to make decisions based on it, there need to be more detailed data. According to the statistics we had access to, the IT forensic unit does not require any more staff and the workload is stable. We do, however, believe the workload has increased, but according to these statistics, this is not a conclusion that is possible to draw. A just statistic measurement is vital to give the management a fair opportunity to make the right decisions regarding, e.g. staffing and equipment investments.

We have here discussed the general IT technical level of the staff as being low. Staffs IT knowledge is also investigated in several research papers studied. Other things to consider in this area is that if a police force already is technically more advanced, the higher the probability is that the police force will apply new technology and solutions as described in *Willits, D., & Nowacki, J. (2016)*. They also claim that:

> *"Specialisation begets specialisation."*

Meaning that if there already exists a specialised unit, it is easier to address a problem with yet another specialisation. The digital technology is continuously evolving, and the use of digital and mobile devices are also changing. The respondents from the IT forensic unit support this by talking about a shift in where information is stored. A few years ago almost all the essential information was located on computers hard drives. Today, virtually all the information found resides on a mobile telephone. The use of mobile devices is not likely to decrease, more the other way around. Another upcoming development, not covered in this thesis, is the rapidly evolving Internet of Things (IoT). This concept is only briefly mentioned in the research we have studied. The IoT devices generally have a frighteningly low level of security. There are indications that these devices can and are used for attacks in new, strange and innovative ways, e.g. *Finance Monthly (2019)*. With this in mind, the police staff needs at least to be aware of the risks and the new possibilities of criminal activity emerging with new technology. So the suggestion would be to increase the technical level of the staff in the Halland police force to meet the evolving and changing digital landscape. The rhetorical question of whether all staff should master these technicalities is still valid. We would consider a general raise in IT awareness and IT forensic knowledge among the teams, and combine that with hiring IT case administrators to be the technical link and support between the IT forensic unit experts and the investigative staff. The administrators could also play a vital part in taking an active role in the investigations and for instance, doing extraction analysis. Research shows that if a forensic technician is an active member of the investigation, the results get significantly better. The case information is more naturally spread to the persons needing it for the extraction analysis, for instance.

This work has focused on trying to see if a formalised IT forensic process is implemented and used at the Hallands police force. The concept of processes are talked about throughout this work. But, what is the benefit of using a formalised IT forensic process anyway? The research studied talks about phases or stages where certain actions should be fulfilled in order to be allowed to advance to the next stage. The stages has responsible persons and a decided list of actions that should be completed before moving on to the next stage. A well implemented process support and guide the work that is needed to be performed. In this “best of worlds” the final result (like a conviction in court) is reached faster and with a more thorough documentation of how the evidence came about. There are though informal workflow processes at all workplaces. If an implementation of a formal process collide to much with the informal workflow the formal process will in most, simply put, not work. We have personally seen that in our previous employments. The formal stages will be sidestepped and the necessary documentation will be created after the process is finished. contrary to the thoughts of the process. Process implementations are a tricky business which involve a lot of effort and work among the staff.

In the research shows that there are several different approaches to processes and many proposed methods to meet the needs for handling physical devices, act at a crime scene and finding digital evidence in digital devices. Research has also introduced different ways to look at the digital crime scene itself. This research has not affected the work with digital devices at a local police authority. The Halland Police force has not any IT forensic processes in place that the respondents know. The question we came to ask ourself at the end of the interview sessions were:

> *"Are there really a need for processes? And what good would these do if they were implemented?"*

Asking the IT forensics, they are hesitant to whether there is a process model that could be implemented to work appropriately for all the tasks they are fulfilling. The same goes for the investigator at the serious crimes group. He also has trouble seeing a process model that would be covering all aspects of the various tasks they are performing. The flow of the mobile device appears to be formalised, the steps are not formally written down, but the phones' information gets extracted anyhow. In a way, you could argue that there is already a process in place. The immediate need for a formalised process is not apparent. Processes are supposed to give support and guidance on how to proceed in individual cases and phases in the workflow. They also assign responsibilities for content in each step. In this report, we have seen issues that could have been mitigated if a formalised process regarding the digital evidence extraction analysis had been in place and implemented. That said, the issues mentioned could also have been reduced with the right training for the staff that needs it. Training in combination with knowledge sharing between the various groups would possibly receive the same results, and we would expect it to have a lower price tag compared to a full-fledged process implementation project. Even with this thought, a general process modelled according to how things run today with the addition of responsibilities for specific steps pinned down, a list of what should be reported as finished at every stage and the proper documentation would be a benefit for effectiveness.

Conclusion

We are concluding this thesis with the following statement. We decide to answer the research question with the following:

"Our respondents are not aware of any IT forensic processes that are used by the Halmstad police force. The chain of custody does, however, not seem to be endangered nor is the evidence integrity. However, knowledge sharing regarding investigative results is somewhat satisfactory; the sharing of knowledge to colleagues in other groups seems to have areas of improvement."

Explaining the answer in more detail; the staff is not aware of any formalised process for evidence extraction and analysis. Regardless of the lack in process knowledge, the respondents' answers support the notion of an unbroken chain of custody and the uncompromised integrity of evidence. The results from the extractions are reported to the investigating team, accompanied by an extraction report. The results are thus shared. The way the report is shared is sometimes not satisfactory, which we believe is due to the lack of understanding of how the receiving team are using the extraction reports. In conjunction with the research question, we had formed two hypotheses as follows:

1. Through the studies, we will find holes in the chain of custody (the chain IS broken) or issues with the evidence integrity. We will also find some failures in the handling of the evidence where (hopefully) simple measures can mitigate these problems.
2. The police have significant issues with the number of acquisitions and the features of modern mobile devices.

Examining these hypotheses answers in detail, first, we have not found any evidence for a broken chain of custody. The evidence integrity also seems ok. There is though failures in the extraction of digital evidence. With this, we mean the analysis of device extractions are made by sometimes insufficiently trained or inexperienced staff in the field of IT forensics. We see a gap in the understanding of the other groups' work and their particular needs which make the transfer of the tasks from one group to another somewhat a challenge. One respondent raises an important question is if everyone should master everything within the IT forensic realm. This notion is supported by the head of the serious crimes unit as well. The increasingly technical complexity of the extracted phones will eventually need to be addressed. There will be a need for more technically well-educated analysts to be able to find the relevant evidence in a mobile device.

Looking at the second hypothesis, we were not able, from the statistics, to deduce that the workload has increased. When we examined the data, the calculated workload is more or less constant over these four years. The answers in the interviews tell another story. The perceived workload is increasing. The respondents talk about more devices, larger extraction files, encryption that make extractions harder etc. The Halland police force is experiencing issues with evolving mobile technology. For the statistics to support the witnesses of higher workload, we need more detailed data. Adding timestamps for how long an examination takes would be a good start, and we suspect that the results from the statistics would change radically.

To summarise: There is no formalised process, the chain of custody and evidence integrity is ok, the risk lies in losing evidence due to insufficient trained/guided staff and the organisational knowledge about the other groups is not adequate.

On a more personal note, in the beginning, we were quite concerned that the staff working within this field were not able even to mention any possible process regarding the handling of digital devices and their evidence. Remarkably, not any single person could describe a formalised way of handling IT-based evidence. "We do like we always do" is the feeling we got after the interviews. The results were not expected, but in a sense, they are logical. The newness of the boom in the number of IT devices and their changed usage combined with the increase of apps used in everyday life makes the mobile forensics (and IT forensics at large) a considerable challenge. The immediate need for a formalised process regarding IT forensic evidence handling is not apparent. In the future, with the emerging IoT devices, there might be another urgency to develop a more stringent way to handle these issues. The possible future development in the IT field might prove to be a valid reason to implement some sort of generic process for IT forensics.
Lastly, we would like to suggest a few things that might improve the points we discovered.

- Training.
  - Making sure the staff has a fair chance of knowing what to do, training is a crucial part. Increasing the technical level will benefit in the long run when future technology evolves and come to be used in criminal activities.
- Increase knowledge between groups.
  - The fact that the different groups are not working together in a higher degree but are in fact like different islands in the police archipelago is something that should be looked into. A more significant understanding of what the other teams are doing will make the cooperation closer. The entire organisation will benefit from this.
- Create guidelines where it is beneficial.
  - Create guidelines on tasks that today has issues. For instance, the analysis of the device extractions on the serious crimes unit is one of these tasks.
- Responsibilities
  - Decide which group or individual is responsible for the tasks that today have issues.
- Processes.
  - We still believe the organisation would benefit from implemented general processes within the IT field. The work at the police organisation in Halland has already informal processes in place and evolving the already working methods would be a start.
- Organisation
  - The workload and the increasing sizes of the extractions. Combined with the complexity in the extraction files need to be addressed. We need more research to find a way to counter these issues. As a start implementing IT case administrators could be a good idea.

Future work

This work has touched on some issues that could not be covered. We have recognised several items that should be looked into further. First, we have the extractions done on telephones. One of the identified issues was the uncertainty that all the relevant information could not be found. An exciting research area would be to look into how much of the data in a phone is not possible to find.

The perceived increase in the workload could not be shown through the statistics we were sent. A more extensive study with more detailed data would be interesting to follow. We are confident that the result would show another picture than the one our statistics showed.

This pilot study on "ordinary local police" should be possible to perform on several police districts focusing on the "ordinary" police and how they interact with each other. The way digital devices are handled and if they have organised themselves in some effective way to cope with the perceived increase in workload.

The previous paragraph leads us to the next topic. We have just briefly touched upon the police reorganisation in 2015 in this thesis. The thought was that the Swedish police force should use the same methods and be organised similarly all over Sweden. We would like to see how that has worked out. Why we raise this as a future work area, is because we have gotten indications on the fact that different regions work in different ways. Contrary to what the reorganisation aimed to counter.

We have found issues in education and the general training within the IT forensic field. A topic to look into is a comparison between the Swedish and the Norwegian police academies and their respective curriculums. In some research papers, it is described that the Norwegian police academy has some IT forensic training in the schedule. Looking into this and compare with how the Swedish police education is organised would be interesting to see.

We have mentioned IT Forensic readiness briefly in this work. The police should be ready to counter crime. How is the police preparing for this is another topic to look into.

Acknowledgement

This is the last thing I write in this thesis. This work would not have been possible to finish without the help of several persons.

First of all, I want to thank my supervisor Stefan Axelsson. He has encouraged me and given insights and research papers, all with the same good mood. He has let me do my thing and just given me hints of what I should remove and add.

The next person I would like to thank is Cecila Bergsten. Cecilia has been supportive and fast in finding the right persons to interview. Even when I got a wild idea, she provided me with additional persons to question. She has commented on my emails, checked the paper for "sensitive data" and given me late comments on my findings. All with the idea: You should always try to do better, every day. A sentence I will try to adhere to.

Anneli Lorentsson-Carlviken, the manager for the IT forensic unit, has helped me find the IT forensic analysts to interview. She also took part in the start-up meeting, where we decided to start this work properly.

The interviewed persons, thank you all. Since I have decided to keep you all anonymous, I can't disclose your identities. The interviews were without exception enjoyable. Without all the ideas and explanations, this would have been a very thin thesis.

The staff at ITE. With this, I mean all the lecturers and teachers in the different courses leading up to this point. Among others: Matts, Linus, Olga, Rasool, Malin, Mohammed, Abbas, Sergey and many others. Thank you for this time!

On a more personal note, I would like to say thank you to my wife, best friend and the mother of my children. Thank you for being there and that you had the good fortune to get a new kidney at the end of this thesis work.

Thanks to my children for making my life less boring.

I would also like to say a huge "thanks friend!" to Adam. You have been supportive and a true friend through these two years I have known you. Thanks!

Sagar, Chhota Bhai, we have had a great time and done some excellent work together. Thanks for being there!

References

[1] Alawadhi, I., Read, J., Marrington, A., & Franqueira, V. (2015). Factors Influencing Digital Forensic Investigations: Empirical Evaluation of 12 Years of Dubai Police Cases. *Journal Of Digital Forensics, Security And Law*. https://doi.org/10.15394/jdfsl.2015.1207

[2] Carrier, B., & Spafford, E. (2003). Getting Physical with the Digital Investigation Process. *International Journal Of Digital Evidence*, *2*(2). Retrieved 17 April 2020, from.

[3] Carrier, B., & Spafford, E. (2004). *An Event-Based Digital Forensic Investigation Framework*. Dfrws.org. Retrieved 17 April 2020, from https://dfrws.org/sites/default/files/session-files/paper-an_event-based_digital_forensic_investigation_framework.pdf.

[4] Davis, J. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing: An International Journal Of Police Strategies & Management*, *35*(2), 272-284. https://doi.org/10.1108/13639511211230039

[5] Gilibrays, O., Mutua, S., Barasa, M., Karume, S., & Matovu, D. (2019). Evaluating factors responsible for inconsistencies in mobile devices digital forensic evidence process model. *International Journal Of Advance Research, Ideas And Innovations In Technology*, *5*(6), 116-121. Retrieved 17 April 2020, from http://www.ijariit.com.

[6] Goel, M., & Kumar, V. (2019). Layered Framework for Mobile Forensics analysis. In *2:nd international conference on advanced computing and software engineering*. Retrieved 17 April 2020, from http://ssrn.com/abstract=3351029.

[7] Gogolin, G. (2010). The Digital Crime Tsunami. *Digital Investigation*, *7*(1-2), 3-8. https://doi.org/10.1016/j.diin.2010.07.001

[8] Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. *Police Practice And Research*, *19*(6), 519-536. https://doi.org/10.1080/15614263.2018.1507889

[9] Hunton, P. (2010). Cyber Crime and Security: A New Model of Law Enforcement Investigation. *Policing*, *4*(4),385-395. https://doi.org/10.1093/police/paq038

[10] Jones, A., & Vidalis, S. (2019). Rethinking Digital Forensics. *Annals Of Emerging Technologies In Computing*, *3*(2), 41-53. https://doi.org/10.33166/aetic.2019.02.005

[11] Leukfeldt, R., Veenstra, S., & Stol, W. (2013). *High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands*. Cybercrimejournal.com. Retrieved 17 April 2020, from http://www.cybercrimejournal.com/Leukfeldtetal2013janijcc.pdf.

[12] Willits, D., & Nowacki, J. (2016). The use of specialized cybercrime policing units: an organizational analysis. *Criminal Justice Studies*, *29*(2), 105-124. https://doi.org/10.1080/1478601x.2016.1170282

[13] Wilson-Kovacs, D. (2019). an exploratory analysis of triage practices in four English constabularies. *Policing: An International Journal*, *43*(1), 77-90. https://doi.org/10.1108/pijpsm-07-2019-0126

[14] *Irons, A., & Lallie, H. (2014). Digital Forensics to Intelligent Forensics. Future Internet, 6(3), 584-596.* https://doi.org/10.3390/fi6030584

[15] *Årnes, A. (2018). Digital forensics. J. Wiley & Sons*

[16] *Beebe, N. (2009). Digital Forensic Research: The Good, the Bad and the Unaddressed. Advances In Digital Forensics V, 17-36.* https://doi.org/10.1007/978-3-642-04155-6_2

[17] *Hansen, H.A., Andersen, S., Axelsson, S., & Hopland, S. (2017). Case Study: A New Method for Investigating Crimes Against Children.*

[18] *Adams, R. (2012). The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice (Doctor of Philosophy). Murdoch University*

[19] *Aftonbladet (2019), Riskfyllt hacka kriminellas mobiler, https://www.aftonbladet.se/nyheter/a/wP5M21/riskfyllt-hacka-kriminellas*-mobiler*, Accessed 2020, 29 Jan, 12:26*

[20] Advantages and Disadvantages of Questionnaires (Updated 2019), https://surveyanyplace.com/questionnaire-pros-and-cons/, accessed 2020, 29 jan, 15:04

[21] Lundström, J & Wirman, J.(2018). Riktlinjers roll I IT-forensiska utredningar. Candidate Thesis. Halmstad university.

[22] Riksdagen(2020), Hemlig dataavläsning blir tillåten vid allvarliga brott (JuU19), https://www.riksdagen.se/sv/dokument-lagar/arende/betankande/hemlig-dataavlasning_H701JuU19 , Accessed 2020, 23 April, 12:30

[23] UML(2020), UML website, https://www.uml.org/, Accessed 2020, 23 April, 15.30

[24] Finance Monthly (2019), The Worst and Weirdest IoT Hacks of All Times , https://www.finance-monthly.com/2019/09/the-worst-and-weirdest-iot-hacks-of-all-times/,Accessed 2020, 23 April

[25] Erlandsen, T. (2019). *Fallacies when Evaluating Digital Evidence Among Prosecutors in the Norwegian Police Service* (Master). Norwegian University of Science and Technology, Department of Information Security and Communication Technology.

[26] Heitmann, O. (2019). *Digital investigation: The malnourished child in the Norwegian police family?* (Master). Norwegian University of Science and Technology, Department of Information Security and Communication Technology.

[27] Justitiedepartenentet. (2014, March 17). *En ny organisation för polisen.*Retrieved June 6, 2020, from https://www.regeringen.se/rattsliga-dokument/proposition/2014/03/prop.-201314110/

Interviews

[28] *Bergsten, C. (2019). Initial Meeting [Interview in person]. Halmstad Police.*

[29] *IT Forensic staff (2020). IT forensic processes in the Halmstad police force. [Interview in person]. Halmstad Police.*

[30] *Local Police (2020). IT forensic processes in the local police in Varberg, Sweden. [Interview over the phone].*

[31] *Investigator (2020). IT forensic processes in the Halmstad police. [Interview in person]. Halmstad Police.*

[32] *Prosecutor (2020). IT forensic processes in the Halmstad police. [Interview over Skype].*

[33] *Police group manager, Falkenberg (2020). Perceived results in hiring IT administrators. [interview over the phone].*

[34] *Police Group manager, Varberg (2020). Perceived results in hiring IT administrators. [interview over the phone].*

[35] *IT case analyst (2020). IT forensic processes in the Halmstad Police Force.*

Appendix 1

Frågemanus inför intervjuer för Magisterarbetet vid Halmstad Högskola. Frågorna bör inte direkt besvaras med ”ja eller nej” utan en följddiskussion är att föredra. Frågorna skall besvaras utifrån den position och kunskaps nivå respondenten har. Detta kan innebära att vissa ämnen kan vara svåra/omöjliga att besvara för vissa medan andra frågor kan verka alltför triviala. Det är precis som det skall vara. Personliga tyckanden efterfrågas. Intervjuerna spelas in, materialet är endast tillgängligt för mig och skall raderas när rapporten är inlämnad och färdig.
Det finns inget intresse av namngivna specifika fall eller personer för detta arbete. Jag är intresserad enbart av ”metadatat” kring arbetet. Hur man gör och varför.

Manus:

- Personliga allmänna
  - Ålder
  - Arbetsplats – grupp
  - Titel el. dyl.
  - antal år inom polisen
  - Högsta utbildning (akademisk, annan än polishögskolan; Polishögskola; Annan)
  - Har du fått någon intern utbildning inom myndigheten vad gäller hantering av IT relaterade bevis/enheter (t.ex. mobiltelefoner och surfplattor)
  - Skulle du behöva det och isåfall vad?
- Allmänt om cybercrime
  - Hur skulle du beskriva din allmänna kunskap inom IT?
  - Hur är det med kunskapen inom IT forensik?
    - Är din kunskap inom IT forensik och IT tillräcklig så att du känner att du kan utföra ditt arbete tillfredsställande?
      - Om inte,vad tycker du saknas?
  - Känner du att du kan få/har tid med vidareutbildning inom detta område (om det skulle behövas)?
  - Hur skulle du definiera IT-brott?
    - IT-relaterad brottslighet?
    - Är det något man pratar om hos er?
  - Hur, anser du, att arbetet med mobila enheter och andra IT relaterade enheter har förändrats över tid?
    - Lättare/svårare?
    - Mer/mindre?
    - Slags enheter?
- Processtänk
  - Hur fungerar samarbetet med andra avdelningar?
    - Vad fungerar?
    - Vad kan bli bättre?
  - Finns det något samarbete med organisationer utanför Polisen?

        - Om ja, isåfall vilka och vad är det man samarbetar kring?(om det är möjligt att säga)?
    - Finns det beskrivet hur samarbetet ska fungera?
        - Nedskrivet?
        - ”muntlig tradition”?
    - Hur Behandlar ni inkommande mobila enheter och dess information/bevis?
    - Finns det instruktioner, mallar, processsteg etc. framtagna?
    - Finns det ett standardiserat sätt att överlämna resultatet till nästa grupp?
        - Får ni feedback på om man är nöjd med det ni gjort?
        - Får ni ofta tillbaka frågor om kompletteringar?
        - Ger ni feedback tillbaka dit därifrån ni fått enheten/informationen/bevisen från innan?
    - Vet du om någon process eller riktlinje ni bör använda i jobbet med mobila enheter och dess bevis?
    - Arbetar ni efter någon process eller riktlinje idag?
    - Kan du säga att beviskedjan är obruten från beslag till Åtal?
        - Hur gör ni för att hålla beviskedjan intakt på er avdelning?
        - Kan ni säkra bevisens integritet på er avdelning?
        - Kan ni kontrollera att beviskedjan inte har varit bruten i ett tidigare skede i processen?
    - Hur fraktar ni mobiler o.dyl. från ställen där ni inte har forensikmöjligheter?
- Administration
    - Hur sköter ni registreringen av resultatet av arbetet?
    - Finns det riktlinjer för vad som ska som minimum registreras?
        - Om nej, Tycker du det borde finnas det
        - Vad skulle det vara isåfall?
        - Om ja, Fungerar det?

Appendix2

Presentation -

Ove Andersson, Halmstad Högskola.

Magister utbildning i Nätverksforensik, intresserad av processer för att se om dessa kan ge ett extra stöd i utredningsarbetet. Vill följa ett tänkt beslag från början till slut, dvs. från beslagstillfället till åtal. Jag vill se om bevisintegriteten och beviskedjan är obruten, hel och att de digitala bevisen är säkrade. Det verkar vara så, förresten…

Jag har genomfört ett antal ganska långa intervjuer med olika delar av organisationen där jag fått ganska många intressanta idéer och inblickar i hur saker och ting fungerar. Jag har läst rapporter inom det här området och fått lite mer infall jag skulle vilja kolla om det är på det viset. Jag har tänkt på IT-handläggarnas roll i organisationen och är lite intresserad av att veta hur tankarna gått när man inrättat dessa tjänster.

Så mina undringar är som följer:

- Vad gjorde att man inrättade dessa tjänster, vad ska dessa personer fylla för funktion?
- Vad har dessa personer för utbildning? Anser du att den tillräcklig och finns det vidareutbildning inom polisen eller på andra ställen för detta?
- Min hypotes är (utifrån att ha pratat med lokal IGV) att man generellt vill kunna göra mer (när det gäller IT forensik) lokalt dvs. slippa skicka iväg t.ex. telefoner/kameror etc, kan detta ha spelat in när man anställde (och inrättade tjänsterna) IT handläggare?
- Tycker du att det ger den effekt man eftersträvade? Om inte, vad skulle vara en önskesituation?

Ove Andersson has moved from the field of Linguistics via computer science to IT forensics. He is located in Mellbystrand just south of Halmstad.

HALMSTAD
UNIVERSITY

PO Box 823, SE-301 18 Halmstad
Phone: +35 46 16 71 00
E-mail: registrator@hh.se
www.hh.se