A Digital Tool to Improve the Efficiency of IT Forensic Investigations

Digital forensics, 15 credits

Halmstad 2019-06-10
Tone Hansen
Abstract
The IT forensic process causing bottlenecks in investigations is an identified issue, with multiple underlying causes – one of the main causes being the lack of expertise among those responsible for ordering IT forensic investigations. The focus of the study is to create and evaluate a potential solution for this problem, aiming to answer research questions related to a suitable architecture, structure and design of a digital tool that would assist individuals in creating IT forensic orders. This work evaluates concepts of such a digital tool. This is done using a grounded theory approach, where a series of test sessions together with the answers from a survey have been examined and analyzed in an iterative process. A low-fidelity prototype is used in the process. The resulting conclusion of the study is a set of concepts, ideas and principles for a digital tool that would aid in the IT forensic ordering process, as well improving the efficiency of the IT forensic process itself. Future work could involve developing the concept further to eventually become a finished product, or using it for improving already existing systems and tools, improving the efficiency and quality of the IT forensic process.
I. Introduction
In a society where the internet, computers, smart phones and other technological devices are becoming an essential and integrated part of people’s everyday life, its involvement in almost all types of criminal activity also increases. This is a trend that can be assumed to continue, meaning that the already increasing workload for IT forensic professionals aiding in criminal investigations will keep growing. The IT forensic process causing bottlenecks in investigations is an already identified issue, with multiple underlying causes [1]. This includes for example a lack of IT forensic professionals or of their training and expertise, and in some cases also insufficient technical equipment [2]. One of the main issues, however, is the lack of knowledge and expertise among those responsible for ordering IT forensic investigations – police investigators, prosecutors and those in charge of conducting preliminary investigations [1]. Insufficient, incorrect or unnecessarily extensive inquiries can result in delays and a heavier workload for IT forensics. With the increasing number of crimes that require some kind of IT related investigation, it is becoming an increasingly common problem. As traditional crime converges with IT, the investigation of serious offences like terrorism, sexual exploitation of children, illegal drug trade and fraud will move into the domain of IT forensics to an even greater extent [3].

The focus of the thesis is how to facilitate the IT forensic process by providing assistance for those placing IT forensic orders, without necessarily demanding a higher level of competence, expertise or knowledge in the area. The purpose is to explore and evaluate the possibilities of applying a digital tool that would aid in the process of ordering IT forensic investigations, by developing, testing and evaluating concepts and the design of such a tool.

Other strategies that have been implemented or suggested for achieving the same goal, such as efforts aiming to increase the knowledge and competence using training and education on IT related crime and investigations [1] [2], do not necessarily make the proposed solution redundant. Such strategies could work well in combination with, or as a complement to, a digital tool. Functions and aids that already exist, such as expert advisors and documents providing guidance, should also be considered when developing a suitable tool. These resources could be utilized in a digital tool, by either including the information itself, or in such a way that the tool navigates the user in the direction of appropriate instances.

Even if a similar tool is already available to crime investigative organizations, the concepts presented in the study could still be useful. A system in use by the police organization that is potentially similar to the proposed tool is Tekpro [4], this system is however used for all types of forensic orders and is not designed specifically for IT forensic orders. Further comparison would require insight that is not openly available. The solution developed and evaluated in the study could serve as a valuable source for improvements of the already existing systems, or as a replacement for them.

Related work
“Computer Forensics: Digital Forensic Analysis Methodology” [5] maps outs the methodology used in digital forensics and provides an overview of the different elements of the digital forensic process. The authors highlight the importance of clear and explicit requests and explain the role and workflow of the forensic examiner receiving the request. The ideas, concepts and information presented have been used in the development of the concepts in this study.
In the report by the National Council for Crime Prevention 2016:17 [1], a survey similar to the one conducted in the present work is presented, where a lack of expertise and knowledge is identified in the problem area, among many other things. The report also presents possible solutions, and especially highlights the importance of improving the expertise regarding placing IT forensic orders. The report has been used as a basis for the present work, both in defining the problem area, constructing questions for the survey and eventually in designing the proposed solution.

In “Conducting Iterative Usability Testing on a Web Site: Challenges and Benefits” [6], a website is evaluated in a way similar to the evaluations in this study. The participants are instructed to perform a number of tasks where they are to explore different parts of the web site functionality. The moderator of the test session is sitting next to the participant so that both can see the screen. This way the moderator can watch every step of the users and note the participants’ behavior as a complement to recording the users’ thinking-aloud process. This procedure is the basis for the test sessions in the present work.

In “Guidance for developing human-computer interfaces for supporting fire emergency response” [7], the grounded theory methodology is used together with software prototypes as tools to analyze whether a graphical interface could help Fire and Rescue Services to gather understanding of an emergency situation and help them make good decisions. This approach is adapted for the present work where the aim is to evaluate whether a digital tool can help individuals place better IT forensic orders. The methods are applied in a similar manner using software prototypes and grounded theory [8].
II. Research questions

The aim of the study is to explore and answer the following research questions:

- What is a suitable architecture of a digital tool assisting in ordering IT forensic investigations?
- How can such a tool be structured and used in a graphical user interface in order to improve the efficiency of IT forensic processes?

Limitations

A potential challenge for the study is finding a level of detail for the tool that is neither too extensive nor too limited. A too extensive tool could become difficult or impossible to implement, whereas a too limited tool may not be capable of providing useful or satisfactory functionality. Finding a balance between these two is important to enable the tool to provide the user with relevant and helpful functionality, while still maintaining usability and learnability. The word “suitable” in the research question could also pose an issue, as the definition of it may vary greatly depending on the situation.

Scope

The scope of the thesis is limited to conceptualizing a digital tool that is intended for use in crime investigative organizations, specifically for ordering IT forensic investigations. The study focuses mainly on the perspective of the individual placing an order and secondarily on the recipient of the order, e.g. the IT forensic expert.

III. Method

The methods used in this study begin with an initial data collection in preparation of developing a low-fidelity prototype of a digital tool. This data collection consists of a survey that serves as a foundation for defining the problem area and the concepts used in development of the prototype. The purpose of the survey is to establish whether the problem exists and if so to what degree. It also serves to form an idea of the requirements and a suitable design for the prototype and its architecture, by asking questions on what to include, problems that can be solved with the proposed tool as well as pros and cons of the solution. Since a survey relies heavily on formulating clear and appropriate questions as well as receiving enough and sufficient responses from relevant respondents, the survey is combined with a brief literature review to explore and establish the extent of the problem area, and to collect information about procedures used in the IT forensic domain. The data collection also includes exploring existing digital tools for ideas on suitable designs. Following the data collection, a first version of the prototype is developed. Prior to the evaluation phase of the first prototype, a pilot test is conducted with a selected participant. The evaluation and development phases are designed as an iterative process, where data from the evaluation of the first prototype is used in the development of a second prototype. The evaluations are carried out in test sessions with selected participants, where the participants provide data in a think-aloud manner, combined with follow-up interviews. The analysis of the collected data is conducted using inductive reasoning to form a grounded theory, which is used to answer the research questions.

The prototype’s level of complexity is determined by the data collected and analyzed, and begins as a low-fidelity prototype for the purpose of evaluating the basic concepts. A low-fidelity prototype is a suitable starting point for developing an entirely new solution. This allows for changes, additions and new ideas to easily be implemented in the prototype without
requiring a lot of time or labor. The prototype only serves as a means of answering the research questions and not a product intended for use.

Rather than developing a finished product, the aim of this study is to find early concepts and design proposals, and to examine whether a digital tool can be useful in the problem area. At this stage of the design process, it is important to grasp the users’ thinking when using the prototype, and hence the thinking-aloud methodology is used together with subsequent interviews.

The entire study is embraced by **grounded theory**, a methodology that combines data collection and analysis in an iterative process where analysis occurs after each test session. Hypotheses are found and developed, and eventually a final theory appears [8]. In grounded theory, data is analyzed by creating codes, a statement or a sentence is interpreted and translated into a code. The more data that is collected, the more codes will begin to reappear. Eventually, no new codes will be found, and the data is considered to have reached theoretical saturation. The codes are then used in the forming of a theory that is grounded in the data. The study is conducted with an inductive approach where an existing hypothesis about the issue is missing. The study begins with as few assumptions, opinions and as little knowledge about the area as possible, and in this way a theory can be grounded in the data that can give indications to the answers of the research questions.

Grounded theory is suitable as a method in this study, considering that it is a completely new solution to be evaluated. Knowledge about whether such a graphical tool can help solve the problem is unknown, which is an important principle in grounded theory where the researcher should as far as possible limit preconceptions and prior knowledge about the target area [8].

The study conducts thinking-aloud sessions to collect data about the usage of the prototype, where it is of interest to capture the thought process of the user. The data collected in the think-aloud sessions serves as the basis for the grounded theory. This type of methodology has been used in previous studies to evaluate different kinds of graphical user interfaces, as discussed in the related work section. The thinking-aloud methodology is especially suitable for studies where a new interface is to be evaluated [6], which is the case for this study. By using this methodology, a large amount of qualitative data can be collected which can be analyzed and form the basis of a final theory. The approach revolves around the user reasoning and explaining their thought process while using the prototype, as well as answering questions throughout the process. The user’s thinking-aloud process is recorded and transcribed to be used for the grounded theory.

**Selection of participants**

Participants of the initial survey were recruited by e-mail and the target group was IT forensic professionals working with criminal investigations. Participants of the evaluation of the prototypes were selected with some characteristics in mind. The participants were not required to have a professional role of someone who places orders for IT forensic investigations, even if this was preferable. Participants only needed to have a basic knowledge of investigation processes, in order to be able to relate to a given scenario.

**Limitations and challenges**

In grounded theory, it is important that the theory formed is based on the data. Grounded theory generally has a problem with distinguishing theories that are found in the data from the researcher’s own preconceptions. This issue stems from the methodology being based on the
researcher creating codes that may be obscured by their own opinions and assumptions of what the data means. These codes, which are created by the researcher, may possibly differ from codes that another researcher would design, which risks that the result in turn differs from a similar study with the same methodology for analysis and data collection. This may adversely affect the validity of the study. This is a challenge, holding back the researcher’s preconceptions, having an open mind, and creating a theory directly based on the collected data [9].

To really create a theory based on the data, it is important that the researcher follows up on issues and ambiguities that arise by asking the participants how they thought in a particular situation or what they meant by a certain answer, instead of leaning on assumptions. Furthermore, it is important to continue with the iterative data collection until theoretical saturation has been reached, which means that no new codes appear. A saturated data collection results in that all concepts in the theory are well-developed and can possibly provide a greater validity to the emerged grounded theory. This is a time-consuming process in a project with limited time, which is a limitation and a challenge with this approach [9].

Materials
The prototype is developed as a web application, using HTML (HyperText Markup Language) and JavaScript. During the test sessions where the prototype is evaluated, participants are provided with a computer where the application is used.

Procedure

In Figure 1, an overview of the procedure is presented as a flowchart. The initial data collection consisting of a survey and literature review leads up to the development of a low fidelity prototype. The concepts of the prototype are based on the data collected in the previous steps. After this, the prototype is evaluated in test sessions where the users’ reasoning and thought process while testing the prototype is recorded and transcribed in order to find codes that serve as data for the grounded theory. For each test session, the concepts of the prototype are improved, added to and altered based on the codes and data retrieved in previous iterations of the grounded theory process. When the data collected appears to no longer produce new codes in the grounded theory, the data is considered saturated and is used to form a final theory that is used to answer the research questions and draw conclusions related to the problem area.

Figure 1 The workflow of the study
Alternative methods
One potential alternative method that could have been used for the study is a literature review to investigate similar solutions in similar situations, such as various digital tools for placing orders, or digital aids in general. This method was not selected as the identified problem area is unique in character which may pose issues when evaluating solutions applied in other areas as the demands may be entirely different.

With access to the existing systems currently in use by crime investigative authorities, a potential alternative strategy that would have been possible for the study had been evaluating these in order to find ways to improve it that could solve the identified problems. However, since such access was not available, this method was not plausible for the study. It would otherwise have been a suitable approach to reach more detailed and useful results and conclusions.

Another option that was considered, was to simply focus the study on developing and evaluating a finished product rather than a prototype. While this too had been a suitable approach, it was disregarded due to the limitations in time and resources. Such a strategy could have produced a useful outcome, but since there was no guarantee for that, the choice fell on a less extensive approach.

Lastly, an alternative method that could have suited the study would have been placing the focus on interviews or surveys with either experts in the domain, or the people who would be using the solution. This would have allowed for a far more extensive idea and understanding of the problem area, and how a potential solution should be designed. As this approach would have required individuals willing to offer both their time as well as their expertise, the chosen method was deemed more suitable for such early stages of a development process. For the continued research and the later stages of developing a solution, this would be an appropriate strategy.
IV. Results

Initial survey

The survey that was targeted mainly at IT forensic professionals within crime investigative organizations received a total of eight responses, see Table 1. Out of the eight responders, five are IT forensics investigators and one is the head of an IT forensics department. The remaining two, while not part of the target group but still contributing with valuable responses, are a system developer and a student at the police academy. The expertise assessments in the survey are however given less weight where the respondents lack professional experience in IT forensic roles. For the responders that work in the IT forensic domain, the amount of professional experience ranges from three to six years. The survey questions and responses in entirety can be found in Appendix A.

Table 1 Overview of participants of the initial survey.

<table>
<thead>
<tr>
<th>Respondent</th>
<th>Occupation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IT forensics department manager</td>
</tr>
<tr>
<td>2-6</td>
<td>IT forensics investigator</td>
</tr>
<tr>
<td>7</td>
<td>Police academy student</td>
</tr>
<tr>
<td>8</td>
<td>System developer</td>
</tr>
</tbody>
</table>

In summary, the responses of the survey indicate the following premises:

Nearly all participants agreed that there is a lack of the expertise required for composing adequate IT forensic investigation orders among the individuals responsible for placing the orders. Where the options available ranged from “very poor” to “very high”, in regard to the expertise possessed by each professional role respectively, seven participants assessed the expertise as either poor or very poor for prosecutors and preliminary investigation leaders while the remaining participant responded “neither”. All participants agreed that the expertise among police investigators was either poor or very poor.

As for the importance of improving the proficiency of the different groups, all participants were of the opinion that police investigators are in great need of improvement. For prosecutors and preliminary investigation leaders, the majority of the responders placed the need of improving the proficiency at “very high” or “high”, with the exception of one participant responding “neither” regarding prosecutors.

For the question regarding what type of shortcomings in orders that cause issues in the IT forensic process, the participants were given the following options, with the possibility of choosing multiple answers: “unnecessarily extensive orders”, “unclear or inexplicit orders”, “lack of knowledge regarding possible/necessary examinations” and “the order becomes outdated and is performed unnecessarily”. Out of these options, all of the participants responded “unclear or inexplicit orders”. Seven participants included “lack of knowledge” and six participants included “unnecessarily extensive orders”. Only four participants included “the order becomes outdated” as an issue.

When asked whether they believed that the proposed solution, using a digital tool, would facilitate and speed up the IT forensic process, three participants responded “a lot”, four responded “somewhat” and one participant responded “a little”.

The remaining questions of the survey provided the participants with an opportunity to share valuable insights and thoughts regarding the proposed tool. These included questions such as
“What would be important to take into account and include?”, “Is there any issue in particular that could be solved with the proposed tool?” and “What pros and cons do you see with the proposed solution?”. 

Simplicity in the interface and navigation of the tool was a desirable quality, as well as making sure the users understand the purpose and functionality of the tool:

*Users need to pass a test before using the system.* – Respondent 1  
*Simplicity and an intuitive interface.* – Respondent 7  
*The system should be easy to work with, as to not require additional knowledge and expertise. It should be easy to navigate, with the possibility of returning to previous steps if a mistake has been made.* – Respondent 8

A concern seemed to be that such a system would require a lot of work and resources, both in preparation and in maintenance, much due to the ever-changing nature of information technology:

*There are no resources for maintaining the database for the tool. It wouldn’t solve the major issues in IT forensics, but it could help with some of the smaller issues.* – Respondent 1  
*IT forensic conditions for mobile phones, for example, can be changed overnight, depending on updates, exploits, software available etc. [...] A digital tool would need to be updated continuously.* – Respondent 3  
*I believe it would require major preparatory work. The police became an authority in 2015, but routines are still far from similar across the organization. Making it work all over Sweden would require many representatives.* – Respondent 5  
*A con would be if the system isn’t updated frequently enough, resulting in new knowledge not reaching the user.* – Respondent 6

Another concern voiced, was that a digital tool would cause additional problems, or be met with some resistance or hesitation:

*“I saw in the system that you can do this and this, why can’t you do that? Here it says so and so.”* – Respondent 3  
*Since the expertise could be of a sensitive nature, such a system would need to be secure. It might be difficult to implement the system across all the various authorities.* – Respondent 4  
*I think that additional systems might be met with hesitation in the police. Many investigators would probably think that placing orders becomes more difficult and therefore delaying it or letting someone else do it for them. The result could then be that only a few always have to assist in composing orders. For the best investigation possible, a dialogue between the investigator and the IT forensic is necessary. I think this can have different outcomes, either that the investigator feels that it’s a better order and is*
satisfied, or that the investigator doesn’t want to be “filtered” and therefore prefers to call the IT forensic directly, which would be both good and bad. Additionally, the digital world is constantly changing which means that if there is a new kind of examination that is very specific, a function for “I want to write by myself and not be helped by the system” would be needed, and with a function like that I believe many investigators would choose to do that instead of accepting new approaches. – 5

Some participants did however believe that a system like the one proposed, could solve some problems…:

Reducing missing information in orders. – Respondent 1

Locked phones without a PIN code. – Respondent 2

Highlighting what is important to the investigation. – Respondent 2

…especially in terms of efficiency and quality of the orders, as opposed to the current situation:

The individual placing the order must be able to think about what they want to accomplish with the examination and why. What do they hope to get out that helps the investigation? How it works in practice today is more of a guessing game to see what can be found. This often leads to inappropriate time investment in different parts of the investigation. – Respondent 3

Would initially facilitate the IT forensic process. Clearer guidelines and a more efficient investigation (for IT forensics). – Respondent 4

Regarding the IT forensic area, and the orders we receive, a factor of plausibility needs to be implemented. Examining and analyzing “everything” is not possible and the orders need to be narrowed down, or rather be made more specific depending on the case and type of crime. – Respondent 4

The major issue that could hopefully be solved would be a more detailed and clear order. This would reduce the workload of the IT forensic and investigations would be faster. If, for example, the only thing needed is a chat log between person X and Y, focusing the examination on video material would be unnecessary. – Respondent 5

The orders can be made faster and more correct by clarifying what steps should be taken for a particular situation. – Respondent 8
Grounded theory
Throughout the study, data was collected in different ways in order to apply the grounded theory methodology. At the early stages, data was collected through a survey where the answers were analyzed and put to use in a primitive prototype. Following this, the prototype was evaluated in order to collect additional data both to form a grounded theory but also to evolve the prototype, conduct more tests, and build onto the existing theory. The process of forming a theory is an iterative process.

The resulting theory provided a basis for a concept to have in mind when developing a system for the purpose of aiding the IT forensic process. In Figure 2, an overview of the most vital parts of such a system is shown. Since some of the most common codes related to the interface and design of the tool were things such as “simple”, “intuitive” and “user friendly”, this has become the focus of the concept. Another dominant code regarding usability was “steps, alternatives and questions”. The entirety of a case, or an order, is regarded as the anatomy of the case, made up of the parts that have been established as most important using the data acquired through the survey, interviews and evaluation sessions, as well as reviewing literature.

Based on the grounded theory, the different steps of the order were divided into a set of categories, comprising the most important aspects of the order. The identified categories consist of: Available data sources, What is already known, What we want to know, Why we want to know, When we need the data, and Contact persons for further questions. These in turn are divided into two sections, Section 1, see Figure 3, consisting of introductory information; data sources in possession and what is already known, and Section 2, see Figure 4, consisting of questions and steps regarding the aim of the IT forensic investigation, both of which are explained further below. A Swedish equivalent of the Section 1 and Section 2 flowcharts is found in Appendix B.

Figure 2 Overview of the concepts conceived during the grounded theory approach.
The first section, Figure 3, consists of entering the information that is already known by the individual placing the order. This includes information about the data sources available, and information about the case and ongoing investigation. More detailed reasoning and explanations in a step-by-step manner follow in the discussion section below.

Figure 3 Section 1 in a more detailed view of the concepts established in the study.
The second section, Figure 4, is made up of questions concerning the aim of the IT forensic investigation. In short, this implies what the individual placing the order wants to accomplish or find out through the investigation, and why. It also includes a step intended for limiting the scope of the investigation, to prevent too extensive orders.

Figure 4 Section 2 in a more detailed view of the concepts established in the study.

A description along with images of the prototype developed and evaluated in the study can be found in Appendix C.
V. Ethical considerations
During the study, all participants have been informed of the purpose of the research. In every test session, the participants have been able to opt out at any time. All participants of the survey and the evaluation sessions are anonymous, and no identifying data has been recorded, other than optional contact information for contributing further to the study. The participants have been informed that they are being recorded during the think-aloud sessions, but that these recordings will only be used for analysis and removed upon completion of the study.

Regarding the digital tool, it should be taken into account that such a tool would be used for handling sensitive information. This is something to carefully consider and incorporate into a development process.

VI. Discussion
The concepts behind a potential digital tool that could be used for placing IT forensic orders have been evaluated using a grounded theory approach. It is important to take into consideration that the suggested concepts in the results are at an early stage in the development process of such a tool, and only serves as a basis for ideas, design principles and general directions.

Further insight into current routines, as well as already existing systems and tools, would have allowed for more detailed concepts of a potential digital tool to be developed from the beginning. Since this information is not openly available, assumptions have been made instead. The result of this is a very open solution that can easily be tailored to the actual needs of the organization. While some assumptions may have been incorrect, this could easily be amended where needed. It is possible that a similar tool or system already exists and is in use, but even so the concepts conceived throughout the study can be helpful in improving this tool or providing ideas for further development.

It is, yet again, important to take into consideration that the concepts developed throughout the study are not by any means an exhaustive or complete list of elements to include in a digital tool. A lot of additional work would be required to develop a final product, but the study lays a foundation for continued research and development, where the ideas can be evolved further, and the design of the tool customized to various organization’s unique requirements.

One aspect of concern is the extent of prior knowledge or training that a tool of this kind would require. Even if the tool is designed to guide the user through placing an order, to save time for both the user and the recipient of the order, it may be a time-consuming task to adapt to using and understanding the tool.

Another potential concern is the amount of work, time and resources that would be required in developing and maintaining such a tool. This is something that would need to be weighed against the benefits provided by the tool. It could also become an issue that users begin to rely too heavily on the tool, and are lost without it, but it is also possible that the tool would help educate the user. The tool would also help maintain uniform guidelines and routines within the organization, making tasks easier for everyone involved.

It has throughout the study been established that the problem area exists, both through previously conducted surveys [1], and through the survey conducted in the present work. It is clear that the expertise among individuals ordering IT forensic investigations is lacking and that this is an issue that needs to be solved. These assertions are confirmed by the group that is most
affected by the identified issues, the IT forensic. The concepts proposed in the study present one possible solution for the issues, but there are of course plenty of other potential solutions. Even if the tool itself is not developed, the concepts, ideas and suggestions it provides could amount to valuable contributions within the problem area.

The ordering process with the digital tool
Through the grounded theory, some dominant codes emerged regarding usability. Some of the most dominant codes were alternatives, questions and steps. The assumption of this is that it would be easier to understand the case if it were to be dissected into its smaller components. An order consists of a multitude of information, several data sources and involved individuals as well as many other factors playing a role in the case. Even for an investigator involved in the case, it can be a difficult task to explain the requirements of an order.

The idea of dividing the process into different steps, containing questions and in some cases proposed options for answers to those questions, should aid in lowering the cognitive load required of the person placing the order, as well as guiding the person in a step-by-step manner. It should also help the IT forensic expert by making sure relevant information is included in the order, to avoid time consuming amendments. This is also why several participants mentioned the need for a function to summarize and overview the order before confirming and sending it.

Section 1
The first section is made up of questions regarding the data sources, or devices, provided for analysis, as well as what information is currently known when the order is placed. The section is initiated when a user creates a new order. This section serves to provide a baseline for the IT forensic expert.

Step one
When creating a new order, the user is prompted to input some information such as the case number of the case in question and the type of crime. This step could be linked to internal registries or databases, to collect all information of a specific case in one place.

Step two
In the next step, the user enters information about data sources available in the case to aid in preparing necessary procedures for particular devices. This could for instance be the type of device – hard drive, cellphone, laptop etc., as well as the device’s storage capacity in order to give an indication of the amount of data to be analyzed by the IT forensic. This step also includes adding an explanation of the device’s relevance in the case, to help the receiving IT forensic understand why it is included in the order.

Step three
The user is prompted to explain the objective of the entire investigation, giving an idea of the context of the case, to help the IT forensic get an idea of how to proceed. Aspects such as places, dates/times and objects of interest; or general search phrases containing words, names, digits or known e-mail addresses. Any information that may help the IT forensic process should be requested in this step.

Step four
It is also of interest to establish the investigator’s, or general, expectations from the material provided. This could include the type of crime and perpetrators, as well as an assessment of
their respective technical proficiency. This allows for the IT forensic to get insight into potentially necessary additional procedures, if the perpetrator is identified as highly technically skilled.

**Step five**
In this step, the user adds information about potential obstacles or difficulties that may occur in the IT forensic process. This could for example include password protected or encrypted devices, as well as hardware that has been damaged before or after becoming evidence material in the investigation. Some hardware may also pose a risk of evidence contamination depending on the circumstances. This information is helpful in preparing necessary procedures, and could also serve as a means of extracting statistics that may be of interest for the organization.

**Step six**
If the investigator has insight or hypotheses regarding the investigation, this could be valuable information for the IT forensic prior to the analysis. While too much information could result in a biased analysis, some preconceptions or assumptions could help steer the IT forensic in the right direction, avoiding time-consuming digressions.

**Step seven**
To limit the scope of the investigation, this category is rounded up in specifying the focus of the investigation. This step is crucial to reduce the IT forensic expert’s workload as well as avoiding straying from the most relevant parts of the investigation.

After completing Section 1, the user proceeds to Section 2.

**Section 2**

The second section is made up of questions concerning the aim of the IT forensic investigation. This implies, what the investigator placing the order wants to know – and why.

**Step eight**
The user is first prompted with questions regarding hypotheses to be confirmed or disproven. These hypotheses may have already been mentioned in Section 1, but can be further specified in Section 2 and provided as an orientation for the IT forensic process.

**Step nine**
One of the main objectives of the IT forensic investigation is to provide new information or evidence to assist in a criminal case. If the IT forensic expert is aware of what parts of the investigation are incomplete, this could be helpful in finding missing pieces and focusing the search on what is of highest priority.

**Step ten**
In order to prevent bottlenecks in the IT forensic process, each requested procedure should be explained and motivated by the individual placing the order. Even if the IT forensic expert should have the last say in what procedures are necessary or not, if the investigator is able to motivate the necessity of a particular procedure, this may help the IT forensic expert understand the purpose of the request and adapt the investigative process thereafter.
**Step eleven**
If the investigator placing the order has premonitions regarding the outcome of the IT forensic process, this should be taken into account even if not given all too much consideration. If there are requests in the order that seem irrelevant, the investigator should still be given a chance to motivate these if needed.

**Step twelve**
Explaining the objective of the order allows for a clear image of what to strive for in the IT forensic process. There is a distinction between the objective of the investigation in its entirety and the IT forensic order, as the objective of the IT forensic order may be narrower.

**Step thirteen**
In order to efficiently plan and prioritize the investigative process, stating the time limitations is one of the most important parts of the order. Implementing some kind of priority classification both internally, to establish what devices or what data should be given the highest priority, and externally throughout the organization, would allow for shorter lead times, a more efficient workflow and a reduced workload for the IT forensic expert. While measures like this are already in place, a digital tool could be designed to assist in priority classifications and incorporating already established time schedules and deadlines. Finally, the user can append contact information for relevant individuals connected to the investigation. This allows for amendments, clarifications and follow up questions to solve issues related to missing information.

**Step fourteen**
At this point, the user is given an overview of the order and an opportunity to correct any input that may have been entered incorrectly, before submitting the order.

**Step fifteen**
Upon submission of the order, a confirmation is shown to the user, as well as a notification sent by e-mail or other appropriate channels. The notification does not contain any information regarding the order or investigation, it solely serves as a confirmation that the order has been sent.
VII. Conclusion and future work

This study has evaluated the concepts for a digital tool with the aim to aid an individual placing IT forensic orders. This has been done through the grounded theory approach where the results of a survey and a series of interviews have been analyzed, as well as evaluation data from a low-fidelity prototype. The aim of the study was to explore and answer the following research questions: What is a suitable architecture of a digital tool assisting in ordering IT forensic investigations? How can such a tool be structured and used in a graphical user interface in order to improve the efficiency of IT forensic processes?

The conclusions drawn from the results of the study can in short be summarized as:

The problem area exists and does have negative consequences that affect both the crime investigative organizations as well as individual investigative processes, mainly in regard to the time aspect. The digital tool proposed and developed in the study would be a potential solution to some of the problems caused by insufficient, inexplicit or too extensive IT forensic orders. The systems, routines and procedures currently in use for placing IT forensic orders are inadequate and need to be improved – implementing a solution like the one proposed would be a possible way of doing this. The proposed digital tool could help in improving the efficiency of IT forensic investigation.

The contribution of this work is a set of design principles and a preliminary architecture of such a digital tool. With these results the evaluation can be continued, and an early prototype can be developed. The ideas that have been developed in this study can be applied as guidelines for how such a tool could be constructed where emphasis has been placed on capturing important data that should be included in an order, but also guidelines for how such a system should be designed to optimize the user friendly experience of the system. These results have been made clear in a flowchart in order to present the principles in an accessible manner to convey the material as a support in further development.

All participants of the initial survey were of the belief that the proposed solution to some extent would be helpful to the IT forensic process. During the grounded theory process, a key characteristic that repeatedly emerged in the codes was “user friendly”. In development of a tool based on the concepts presented in the study, this characteristic should be a focal point.

In further developing a finished product, working alongside the end users of the product to properly and exhaustively address all the needs and requirements would be necessary. The ideas and concepts presented in the study have been designed in such a way that they can easily be transformed, manipulated and adapted to the needs of a specific organization. However, doing so would require the expertise and knowledge possessed by those most familiar with the problem area and the needs of the organization.

Future work could involve further developing the ideas that have been presented in this study, resulting in the creation of a high-fidelity prototype. This prototype can be developed in several stages where an initial stage revolves around a low-fidelity prototype that in an iterative process develops into high-fidelity and eventually a finished product. Furthermore, a potential application of these ideas would be in the form of an expert system. An expert system builds on a database of expert knowledge that has been input by experts or collected from experts. The application can draw conclusions, answer questions or give suggestions to the user based on rules specified in the software. Expert systems have in some cases been implemented in the legal domain, with applications such as systems of formal consultancy on legal matters, legal
Implementing an expert system in the context of the study’s problem area could be a useful application of the concepts and ideas derived from the study. Artificial intelligence in the regard of a self-learning system, would be a suitable solution in the IT forensic domain considering the constant changes and development it entails. Rather than continuously requiring updates and maintenance, artificial intelligence could be a one-time investment that would save a lot of time and labor. In such a future study, experts of IT forensic investigations would be consulted in the form of interviews and user studies of the prototype to produce more specific guidelines for the development and production of applications of an expert system that can ease and improve the process of placing IT forensic orders.
References


Appendix A
Appendix A contains all the questions and responses of the initial survey, translated from Swedish to English.

**Occupation:**
Respondent 1: Head of an IT forensics department
Respondent 2: IT forensic
Respondent 3: IT forensic
Respondent 4: IT forensic
Respondent 5: IT forensic
Respondent 6: IT forensic
Respondent 7: Police academy student
Respondent 8: System developer

**Years of experience in IT forensics:**
Respondent 1: 4
Respondent 2: 4
Respondent 3: 4
Respondent 4: 3
Respondent 5: 3
Respondent 6: 6
Respondent 7: 0
Respondent 8: 0

**How would you assess the expertise regarding composing orders for IT forensic investigations among the following groups of professionals?**

(Very poor / Poor / Neither / High / Very high)

Respondent 1:
  Prosecutors: Very poor
  Preliminary investigation leaders: Poor
  Police investigators: Poor

Respondent 2:
  Prosecutors: Poor
  Preliminary investigation leaders: Neither
  Police investigators: Poor

Respondent 3:
  Prosecutors: Very poor
Preliminary investigation leaders: Very poor
Police investigators: Very poor

Respondent 4:
Prosecutors: Very poor
Preliminary investigation leaders: Very poor
Police investigators: Poor

Respondent 5:
Prosecutors: Neither
Preliminary investigation leaders: Poor
Police investigators: Poor

Respondent 6:
Prosecutors: Poor
Preliminary investigation leaders: Poor
Police investigators: Poor

Respondent 7:
Prosecutors: Very poor
Preliminary investigation leaders: Very poor
Police investigators: Very poor

Respondent 8:
Prosecutors: Poor
Preliminary investigation leaders: Poor
Police investigators: Poor

**How would you assess the need for improving the aforementioned expertise among those groups respectively?**

*(None / Low / Neither / High / Very high)*

Respondent 1:
Prosecutors: Very high
Preliminary investigation leaders: Very high
Police investigators: Very high

Respondent 2:
Prosecutors: High
Preliminary investigation leaders: High
Police investigators: Very high

Respondent 3:
Prosecutors: Very high
Preliminary investigation leaders: Very high
Police investigators: Very high

Respondent 4:
Prosecutors: Very high
Preliminary investigation leaders: Very high
Police investigators: Very high
Respondent 5:
Prosecutors: Neither
Preliminary investigation leaders: High
Police investigators: Very high

Respondent 6:
Prosecutors: Very high
Preliminary investigation leaders: Very high
Police investigators: Very high

Respondent 7:
Prosecutors: Very high
Preliminary investigation leaders: Very high
Police investigators: Very high

Respondent 8:
Prosecutors: Very high
Preliminary investigation leaders: Very high
Police investigators: Very high

What flaws in orders cause the most issues in the IT forensic process?

(“unnecessarily extensive orders”, “unclear or inexplicit orders”, “lack of knowledge regarding possible/necessary examinations”, “the order becomes outdated and is performed unnecessarily”)

Respondent 1:
Unnecessarily extensive orders,
unclear or inexplicit orders,
lack of knowledge regarding possible/necessary examinations,
the order becomes outdated and is performed unnecessarily

Respondent 2:
Unnecessarily extensive orders,
unclear or inexplicit orders,
lack of knowledge regarding possible/necessary examinations

Respondent 3:
Unnecessarily extensive orders,
unclear or inexplicit orders,
lack of knowledge regarding possible/necessary examinations

Respondent 4:
Unnecessarily extensive orders,
unclear or inexplicit orders,
lack of knowledge regarding possible/necessary examinations,
the order becomes outdated and is performed unnecessarily

Respondent 5:
Unclear or inexplicit orders
Respondent 6: 
Unnecessarily extensive orders, 
unclear or inexplicit orders, 
lack of knowledge regarding possible/necessary examinations, 
the order becomes outdated and is performed unnecessarily

Respondent 7: 
Unclear or inexplicit orders, 
lack of knowledge regarding possible/necessary examinations, 
the order becomes outdated and is performed unnecessarily

Respondent 8: 
Unnecessarily extensive orders, 
unclear or inexplicit orders, 
lack of knowledge regarding possible/necessary examinations

If it were possible to compile the knowledge and expertise that is possessed by various expert functions and IT forensics into an expert system in order to facilitate the ordering process and improve the quality of orders placed, to what extent do you believe it would aid the IT forensic process?

(A lot / Somewhat / A little / Not at all)

Respondent 1: Somewhat
Respondent 2: Somewhat
Respondent 3: A little
Respondent 4: A lot
Respondent 5: Somewhat
Respondent 6: Somewhat
Respondent 7: A lot
Respondent 8: A lot

What would be important to take into account and include?

Respondent 1: Users need to pass a test before using the system.
Respondent 2: Highlighting what is important to the investigation.
Respondent 3: IT forensic conditions for mobile phones, for example, can be changed overnight, depending on updates, exploits, software available etc. The regions work differently, authorities do not cooperate in the field of IT forensics. Nobody wants to share. Some groups develop more than others which provides different conditions. The vast majority of investigators are incredibly uninterested in technology. An expert system would need to be updated continuously.
Respondent 4: Regarding the IT forensic area, and the orders we receive, a factor of plausibility needs to be implemented. Examining and analyzing “everything” is not possible and the orders need to be narrowed down, or rather be made more specific depending on the case and type of crime.

Respondent 5: I believe it would require major preparatory work. The police became an authority in 2015, but routines are still far from similar across the organization. Making it work all over Sweden would require many representatives. In some places the orders might already be satisfactory, making an expert system redundant, while in other places it might be just what’s needed.

Respondent 6: The problem is that the questions often can’t be too generic, the different needs for an investigation can differ a lot from case to case.

Respondent 7: Simplicity and an intuitive interface.

Respondent 8: The system should be easy to work with, as to not require additional knowledge and expertise. It should be easy to navigate, with the possibility of returning to previous steps if a mistake has been made. It’s important that the system represents reality in order to give correct suggestions.

**Is there any issue in particular that could be solved with the proposed system?**

Respondent 1: Reducing missing information in orders.

Respondent 2: Locked phones without a PIN code.

Respondent 3: The individual placing the order must be able to think about why and what they want with the examination. What do they hope to get out that helps the investigation? How it works in practice today is more of a guessing game to see what can be found. This often leads to inappropriate time investment in different parts of the investigation.

Respondent 4: Would initially facilitate the IT forensic process. Clearer guidelines and a more efficient investigation (for IT forensics).

Respondent 5: The major issue that could hopefully be solved would be a more detailed and clear order. This would reduce the workload of the IT forensic and investigations would be faster. If, for example, the only thing needed is a chat log between person X and Y, focusing the examination on video material would be unnecessary.

Respondent 6: Information regarding what the IT forensic can do. But this, too, changes quickly with new software and new experiences, so it’s difficult to say.

Respondent 7: Unclear orders.

Respondent 8: The orders can be made faster and more correct by clarifying what steps should be taken for a particular situation.

**What pros and cons do you see with the proposed solution?**

Respondent 1: There are no resources for maintaining the database for the expert system. It wouldn’t solve the major issues in IT forensics, but it could help with some of the smaller issues.

Respondent 2: -
Respondent 3: “I saw in the system that you can do this and this, why can’t you do that? Here it says so and so.”

Respondent 4: Since the expertise could be of a sensitive nature, such a system would need to be secure. It might be difficult to implement the system in all different authorities.

Respondent 5: I think that additional systems might be met with hesitation in the police. Many investigators would probably think that placing orders becomes more difficult and therefore delaying it or letting someone else do it for them. The result could then be that only a few always have to assist in composing orders. For the best investigation possible, a dialogue between the investigator and the IT forensic is necessary. I think this can have different outcomes, either that the investigator feels that it’s a better order and is satisfied, or that the investigator doesn’t want to be “filtered” and therefore prefers to call the IT forensic directly, which would be both good and bad. Additionally, the digital world is constantly changing which means that if there is a new kind of examination that is very specific, a function for “I want to write by myself and not be helped by the system” would be needed, and with a function like that I believe many investigators would choose to do that instead of accepting new approaches.

Respondent 6: A con would be if the system isn’t updated frequently enough, resulting in new knowledge not reaching the user.

Respondent 7: -

Respondent 8: A pro is that the person placing the order doesn’t need the same degree of expertise. A con could be that this expertise is not developed further as the user trusts the system instead. But it is also possible that the system could help improve the expertise of the user, in which case that con would instead be a pro.
Appendix B

The appendix consists of a simplified and translated version of the conceptual flowcharts developed in the study. Since the prototype was developed and evaluated in Swedish, with Swedish speaking participants, the concepts were primarily designed in Swedish, and later translated to English.

Figure B-1 A simplified and translated version of the order process flowcharts developed in the study.
Appendix C
The appendix consists of a description and images of the prototype that was developed and evaluated in the study. The prototype changed over the course of the evaluation process, and only the final version of it is included.

The prototype was developed as a web application, using HTML and JavaScript for its design and functions.

The prototype application is designed to be as intuitive and user friendly as possible, based on feedback and data collected during the evaluation phases. In summary, it consists of multiple pages where each page is a step in the ordering process. Each step includes a number of questions, text input or alternatives where the user adds information that is useful for the IT forensic investigation. The prototype is not by any means a finished product, and only served as a basis for discussion and reasoning in the evaluation process, in order to collect data for the grounded theory.

On the first page, Figure C-1, the user simply presses a button to begin a new order.

![Figure C-1](image_url) The first page of the prototype, containing a button for beginning an order.
On page two, Figure C-2, the user enters basic information about the case, such as case number and type of crime.

![Figure C-2](image-url) Page two of the prototype, where basic information about the case is entered.
On page three, Figure C-3, the user enters devices into the order along with information about them. This includes information such as type of device, evidence identification number, the storage capacity of the device, and the relevance of the device in the case.

Figure C-3 Page three of the prototype, where devices are added to the order along with information about them.
On page four, Figure C-4, the user is shown a summary of information entered in previous steps to be able to refer to it in the following steps. The summary shows the case number, the type of crime, and the devices added to the order in previous steps.

*Figure C-4* Page four of the prototype, where additional information about the case is entered and a summary of information previously entered can be seen.
On page five, Figure C-5, the user enters additional information about the crime and the perpetrator, including an assessment of the perpetrator’s technical proficiency.

**Figure C-5** Page five of the prototype, where additional information about the crime and the perpetrator is entered, and a summary of information previously entered can be seen.
On page six, Figure C-6, the user enters information about potential obstacles or issues that may affect the IT forensic process, such as encrypted or password protected devices or damaged hardware.

Figure C-6 Page six of the prototype, where information about potential obstacles or issues with devices in the order is entered, and a summary of information entered in previous steps can be seen.
On page seven, Figure C-7, additional information about specific requests or procedures is entered. The user can specify existing hypotheses to be confirmed or disproven in the IT forensic investigation and enter what parts of the investigation are missing or incomplete.

![Image of the prototype](image)

*Figure C-7* Page seven of the prototype, where additional information about specific requests for the order, hypotheses and missing information in the investigation is entered, and a summary of information entered in previous steps can be seen.

On the final page of the prototype, a summary of all the information entered in the order is shown, and a button for submitting the order.
Tone Hansen