UNIVERSITY OF TARTU
Institute of Computer Science
Cybersecurity Curriculum

Priit Lahesoo

The electronic evidence examination reporting system by the example of West prefecture

Master's Thesis (30 ECTS)

Supervisor(s) Truls Tuxen Ringkjob
Raimundas Matulevičius

Tartu 2017

The electronic evidence examination reporting system by the example of West prefecture

Abstract:

The master's thesis examined ways to speed up the examination of electronic evidence content analysis inside the examination process. Making police work with electronic evidence more effective to helping them save time can save taxpayers money and this is good for society. The problem is a constant lack of time during the examination of electronic evidence processing procedure and currently the fact that notes are collected disorderly by the examiners. This work will focus on practical issues like how to improve the speed of drawing up an electronic evidence examination protocol. The work was done basing on examination data results that collected in the West prefecture based on real work statistics and permission by the Police and Border Guard Board. Invented data collecting model can lead examiner to be more productive. Quantitative and qualitative analysis imply that this is definitely one way to speed up electronic evidence examination. As part of the work, the practical Microsoft Access application was developed by the author. We can conclude from the thesis that using the database in order to organize the examiners' notes will make the examiners' work faster and more productively. Designed solution can be used in electronic evidence examinations as a result of this thesis.

Keywords:

Electronic evidence, cybercrime, device examination, computer forensics, mobile forensics

CERCS: P175 – Informatics, systems theory

Elektrooniliste tõendite uurimise aruandluse süsteem Lääne prefektuuri näitel

Lühikokkuvõte:

Magistritöös uuriti erinevaid viise eesmärgiga kiirendada elektroonilise asitõendi sisuanalüüsi uurimist vaatlusprotsessis. Muutes politsei tööd elektrooniliste asitõenditega efektiivsemaks, aitab see säästa ka maksumaksja raha, mis on ühiskonnale kasulik. Praegune probleem seisneb pidevas ajapuuduses elektrooniliste tõendite menetlemise protseduuris ja faktis, et vaatlejate kogutud märkmed on üldjuhul korrapäratud. See töö keskendub praktilistele probleemidele, nagu kuidas parandada elektroonilise asitõendi vaatluse protokolli koostamise kiirust. Töös kasutatakse tehniliste uuringute andmeid, mis koguti Lääne prefektuuris ning mis põhinevad tõelisel tööstatistikal ja Politsei– ja Piirivalveameti loal. Loodud andmekogumisemudel võib tagada arvuti vaatleja töö suurema produktiivsuse. Kvantitatiivne ja kvalitatiivne analüüs näitab, et see on kahtlemata üks võimalus kuidas saab kiirendada elektrooniliste asitõendite vaatlusprotsessi. Osana tööst valmistas autor Microsoft Access rakenduse, eesmärgiga aidata ekspertidel vaatlusandmeid koguda. Magistritööst on võimalik järeldada, et andmebaasi kasutamine organiseerimaks vaatlejate märkmeid tõstab nende produktiivsust. Koostatud rakendust saab selle magistritöö tulemusel kasutada elektroonilise asitõendi menetlusprotsessis.

Võtmesõnad:

Elektroonilised tõendid, küberkuritegu, arvutiuuring, simsurf

CERCS: P175 – Informaatika, süsteemiteooria

Table of contents

Acknowledgments

The author wishes to publish his appreciation to all helpers, supporters and advisers who have contributed to the completion of this master's thesis. The author gives his thanks for the preparatory research contributed by various supervisors and teachers. The author also thanks his colleagues for helpful comments and suggestions on the testing and use database.

Many good words to supervisor MSc Truls Ringkjob for invaluable guidance, diversified and substantive comments and discussions. You have set a case of incredibleness as a scientist, coach, educator, and just a good example.

Good words to supervisor PhD Raimundas Matulevičius for directing how to format and design thesis much more readable document.

Great thanks go to dear colleagues for their advice and for their patience with real work trouble. The author would also like to thank all people who assisted in the reviewing process. The author also wishes to thank all those involved, who shared their own comments, suggestions, and helped the collection of data experts: Nils Sempelson, Marge Kera, Andrus Toomla, Ragnar Õun, Karl Põder, Kait Kolberg, Oskar Gross, Riho Erend and all other colleagues who has contributed to this work. Your discussion, ideas, and feedback have been absolutely invaluable.

The author would like to thank family for their encouragement and patience, for not losing faith in the completion of this work. In particular, author would like to thank his spouse Ave and daughters Tiina Silvia and Marie Kristiin.

List of abbreviations

Abbreviation	Details
Autopsy Forensic Browser	Digital forensics platform and graphical interface to The Sleuth Kit®
BICEP	Basic Investigation of Computers Electronic Crimes Program
Bluetooth	Wireless technology standard for short distance
CryptHunter	Computer program that detects mounted encrypted volumes
DB	Database
EKEI	Estonian Forensic Science Institute
EnCase	Suite of computer forensics software by Guidance Software
ER	Entity – Relationship
FTK	Forensic Tool Kit Forensic Toolkit computer research software by Access Data
FTK Imager	Forensic Toolkit imager software by Access Data
GUI	Graphic User Interface
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
IrDA	Infrared Data Association wireless technology standard
ISO	International Organization for Standardization
IT	Information Technology
JTAG	Joint Test Action Group
LAB	Laboratory – controlled conditions place where research or experiment may be performed
LAN	Local Area Network
LCD	Liquid-crystal-display
MD5	Message Digest 5 Algorithm cryptographic hash function
Mouse Jiggler	Computer program that fake mouse input to Windows
MS	Microsoft
MySQL	Open-source relational database management system
NAND	Digital electronics logic negative-AND
NOR	Digital electronics logic inverted OR

PBF	Push-button forensics
PC	Personal Computer
PHP	Hypertext Preprocessor server-side scripting programming language
RAM	Random Access Memory
RS-232	Recommended Standard 232
SATA	Serial Advanced Technology Attachment
SHA1	Secure Hash Algorithm 1 cryptographic hash function
SMS	Short Message Service
The Sleuth Kit®	Computer forensic oriented library and collection of command line tools
TraceHunter	Computer program that detects for traces of evidence
U.S.	United States
USB	Universal Serial Bus
VCR	Video Cassette Recorder
Wi-Fi	Wireless Fidelity wireless technology standard
WLAN	Wireless local area network
Write-blocker	A piece of hardware that is used to block alterations being made to a device
XRY	A popular forensic tool designed by Micro Systemation for extracting and decoding information from mobile phones

1. Introduction

In the examination of electronic evidence content, it is very important to collect initial information from the crime scene. When that involves a criminal sourcing of information from electronic appliances, this information must be documented as a minimum:

1) The official's title and name

2) The case number

3) The case description

4) The name and characteristics of the observed object

5) The mission of observation

On the basis of the description of these five requirements, it is later possible for specialists to see whether the electronic device contains relevant information for the case. Having stated the preceding information, the electronic device can be separated from the packaging and prepared for duplication. Depending on the electronic device there may be different approaches of how to retrieve the media from the appliance and that causes a variation of technically correct approaches. Furthermore, a sense of criticism is necessary in following the different technical guides, because they are generally written with only the best technical needs in mind. As a result of that, the guides may contain possibly destructive instructions, regarding the preservation of the data. Making an identical copy of the hard–drive is very important in order not to damage or alter the data of the source device. The forensic people use both hardware and software write–protection devices that offer options with various special features to separate data from technical devices. Each study should keep in mind the data protection principle whereby only the relevant data must be taken out from the processing equipment. It is difficult to follow this principle in practice because of integrity. It is often the only possible way to get the information as a whole and this is the only way how the forensic software will describe it. Here the technical realization and literal vision will differ from each other and the examiners must start considering a variety of options. Furthermore, this will create a situation for making serious errors in the chain of evidence. Ideally, each investigator must find the most suitable approach that guarantees the preservation of the evidence chain, and through this, its proof of authenticity. In order to simplify and organize the process of the work flow, this can only be based on past experience. Examiners need to constantly develop basic understandings of key technical and legal factors. However, in the absence of experience, it is always good to have a simple guide or framework for the execution of the work. In business effectiveness of mitigation measures equals the weakest link. By Thomas Reid description "In every chain of reasoning, the evidence of the last conclusion can be no greater than that of the weakest link of the chain, whatever may be the strength of the rest."[42, ch. I, p. 377] Therefore, it is probably not a very good idea to put the investigators themselves in weakest link position. The Estonian Code of Criminal Procedure [1] will describe in detail in § 83 what is the objective of inspection and the objects of inspection.

Digital forensics can be divided in relation to the type of information source devices involved like computer forensics, mobile forensics, database forensics, live forensics and network forensics. [18] Every investigated device can be divided to two parts a physical base and logical base. The most investigated objects in cyber forensics are probably computer and cell phone devices. Other areas cover mostly the devices' having logical content that may be evidential. There is not always a very clear line between physical and logical content because physical content always includes the same logical content and it is always very easy to make mistake by examiner just by describing them.

In criminal proceedings it is necessary to follow some routine operations which are mandatory:

1) Photographing & taping the crime scene

2) Conducting the survey

3) Examination of the evidence in the LAB

4) Seeking & packing the electronic evidence

5) Finalizing the report of electronic evidence examination

6) Data processing and storing

Thesis will focus on the problem of how using a specific method can speed up activities between points 3 to 5 through the author's practical experience with the electronic evidence examination reporting system by the example of Estonian West prefecture where author is working at the present time.

Edmond Locard's exchange principle (1910) states: "every contact leaves a trace". Every crime leaves traces by which the pre–trial investigation can to seek the offender and ascertain circumstances needed for guilt proven. Everything here implies that the strategies of the police inspectors should continually advance with innovative changes. Additionally, this underlines the significance of preparing and previous experience. While the inspectors will regularly experience new gadgets and advances and adjust their systems according to that, there is a never–ending flow of data that the analyst will have to search for. [28, p. 5]

1.1 Background

Police and Border Guard Board is the largest state agency that are responsible for solving crime in our country. The background of the problem goes back to the point in time in year 2005 when the author begin work in the cybercrime unit of West prefecture of Estonia. The cybercrime unit supports the police core activities through an IT knowledge base and this unit must make all electronic evidence examination protocols in West prefecture area. Firstly, the aim of the electronic evidence examination is identification of significant facts and search an information with evidential importance. In this field, public authorities have

a serious problem with composing electronic evidence examination protocol, because necessary specialists are few and composing examination protocol takes too long. This research work has been investigated before by EKEI and South prefecture examiners and has not been studied in depth. There is unfounded opinion that IT forensics examiner must produce computer examination protocol 40 hours and other devices examination 15 hours and cellphone surf 4 hours. Author have an idea that there is a possibility to change electronic evidence examination handling more effective through automation with unique Microsoft Access database solution. It does not harm research work related to that done by others. Finally, research has been done on automating electronic evidence examination protocol writing with a view to shortening the examination time. Technological engineering concepts related to author research aimed to improve scientific theories understanding of phenomenon.

1.2 Research problem

Police need to respond to violations quickly. If there is electronic evidence involved, the duration of proceedings may be prolonged and this is a problem and a condition to be improved upon. Research will focus on how to shorten the time spent on examining electronic evidence and write final examination protocol quicker that was done before. Through this problem, another problem rise. There is need to support examiners without any experience in the field. Solving the first problem can help to explain how we can get faster examination results with wise examiners. Producing an evidence examination protocol is definitely one of the bottlenecks that will always slow down the investigation proceedings. Logic tell that examiner can work faster with special tool adapted for examiner needs. Author propose solution with MS Access database for collecting examiner notes. Author is using database and his two colleagues using their own tools to execute computer examination. Research will be done as deductive quantitative primary data analysis. **Hypothesis is that by giving basic framework to electronic evidence examination it is possible to speed up the writing electronic evidence examination protocol**. It will be researched through collected primary research data which is collected for statistical analysis' purposes by the author and his colleagues during the electronic evidence examination job.

1.3 Objective

The purpose of the electronic evidence examination report is to describe electronic items in sufficient details, to photograph and to take measures for their preservation. The police must not change the information in the electronic evidence in a manner that would change its evidential value. In order to ensure the preservation of electronic evidence and safeness, the person responsible should act immediately. The current work aims to explore the process of the examination of electronic evidence content with a goal of speeding up the time taken to finish electronic evidence examination protocol. A good practice could be the work–flow automation. It means that the experts can leave routine work aside and focus on the deep research to investigation problems.

Automation is the premise for collecting knowledge. Applying automation in the initial stages of the investigation could be extremely important to the process, as it may bring attention to obscure evidence that could be inaccessible to the investigator. The automation does not take into account the institutionalized procedures in the office. [3, p. 11]

However, the same standard of first–level examination could happen all over the planet, paying little respect to the examiner or the office's learning and spending plans. This could make first–level computerized examinations possible in nations that lack the ability to conduct digital investigations. Eventually, a mechanized first–level examination connected to the person in the call phase of the examination may take into consideration a quicker, higher quality, institutionalized preview with very little related preparation work. [3, p. 11]

1.4 Scope of work

IT Forensic examiner data collecting process is sometimes trivial and the collected hardware, data and reports are liable to vary or change. That data either resides in examiners' forensic computers or published reports only and it will not be available for public use. The scope of work covers the search, discovery and identification of electronic evidence areas focusing on electronic evidence seizure, analyzing and reporting issues. Scope of work described in more detail below.

To identify work process and describe what computer forensic examiner do.

To determine basic requirements for digital evidence handling.

To describe digital forensics process, computer and mobile phone forensic examination procedure.

To estimate digital forensic examination work process and time limits.

To develop further MS Access working database solution for examiner notes.

To develop MS Access database to meet examiner needs.

To collect statistical data about examiner work.

To compare collected statistics

To analyze outcomes.

The examiners' work–flow statistical research cover years 2014 – 2016 in the West prefecture of Estonia. The usefulness, satisfaction, and ease of use analysis conducted to examiners who agreed to try database model solution finished during this work, measuring usability with the questionnaire.

1.5 Review of previous work

The consistent development of innovation makes it hard to characterize a solid arrangement of standard practices for removing evidential information from advanced gadgets. New cell telephones are discharged to advertise on a month to month bases, regularly with redesigned security conventions that should be circumvent by police inspectors. While the innovative development of PCs is less dynamic, each working framework oversees the information in an alternate way to the others. Another trouble confronted by the inspectors is the assortment

of uses that are accessible on cell phones and PCs, a large number of which store evidential information in different areas in their particular record frameworks. Application overhauls can likewise bring about an adjustment in the area of this data. [28, p. 5] The purpose of the electronic evidence examination is to describe examination object in sufficient detail, photograph and take measures for their preservation.

During research period there was 3 officers working in the West prefecture IT Forensic LAB. The leading police officer and two police officers as computer forensics examiners. All three do electronic evidence examinations. Their work analyzed by public job descriptions revealed on job announcements pages [31], [32]. The second examiner in the West prefecture IT Forensic LAB works a leader [31] whose main tasks include:

- Internet monitoring analyzes.
- Data processing of electronic communications.
- Data visualization through specific software tools.
- Producing storage media surveys and analyzes.
- Procedural and undercover operations needing information technology expertise.
- Office advice and assistance to other units and assistance in information technology crimes which require special expertise in preventing, combating and pre–trial proceedings in their cases.
- Organizing the work of the service.

Requirements for taking position of the unit leader are:

- Higher education preferably in police or the IT field education.
- Estonian language at the advanced level, and a good English.
- The ability to use table and word processing programs, and the ability to use databases and the Internet programs used in police work.
- Possession of knowledge about information technology expertise.
- A deep interest in the field.
- Willingness to learn and its continuous development in the field of information technology to keep up with the newest innovations.
- Very good communication skills, stress tolerance, and time management ability.
- Compliance with the law on police and border police officers to set conditions including physical education requirements.

There are two examiners the first and third examiner place in this research, working in the

West prefecture IT Forensic LAB [32] whose main tasks are:

- Finding, fixing, and formalization of digital experience in the criminal proceedings.
- Organizing the preservation sources of evidence.

- Helping and advising the criminal bureau and other structural units with finding, fixing and forming digital evidence.
- Offering analytical support in the criminal proceedings.

Requirements for IT forensic examiners are:

- IT field education.
- Estonian language proficiency in advanced level (C1), a very good English and Russian language skills.
- Honest and ethical conduct, high self–discipline.
- Readiness for team work, flexibility and stress tolerance.
- Good ability to communicate and judgment skills.
- Wwillingness' to learn and continuous development in the field of information technology to keep up with the newest innovations.
- Category B driving license and driving experience of at least 2 years.
- Compliance with the requirements established by the Public Service Act Officer.

In both cases the advantage is prior experience in computer disassembly and maintenance job. An interesting phenomenon is that the job advertisements do not meet the requirements set out with the requirements of the current job description in any way. It is obvious that it will cause big problems while developing any software by job description. Like as the work differs from the senior investigator job description (main job No 374) [32] and the lead investigator job description (main job No 368) [31]. Both job description numbered documents are restricted and that cause presenting only number. In this research first and third examiner apply main job No 374 and second examiner apply main job No 368 described above through work advertisements. The author has decided to use work advertisements instead of job descriptions to analyze present situation because job directives does not match the job description. The choice was made on the basis of logic and experience. Conflict described refers to the problem that persists. If process described wrongly then methods and tools chosen by process does not guarantee the main objective what must be the quality.

1.6 Limitations

Privacy issues demand to encrypt data which are third parties involved – so worked out Microsoft Access database solution is working from software named True–Crypt container and if it's mounted to partition R. Using True–Crypt is not secure anymore as it may contain unfixed security issues however there is no limitations to use some other safe encryption software. The author used True–Crypt for his convenience to avoid random observers. There are some experimental modules helping to export data from database and they need to be in container folder called Access–Classes. Temporary folder is for exporting and importing reports if needed to do so. Because of the software upgrade arrangement in the organization, unchecked software cannot be utilized. Microsoft Access database test solution needs for best performance Microsoft Access 2003 or newer software in Administrator rights. The program developed by author can help making the evidence examination protocol and try to handle observation data but it will not make all the needed paperwork, because it is the

examiners' job. Another interesting problem is how to customize the program to fit for business needs, it must be decided by examiner who can work out his own solution.

As of now there are specialists that are not running the majority of the computerized instruments accessible to them. For instance, amid dialogs, a few analysts who settle on the choice to proceed or to stop the examination have asserted that they never utilize known hash databases in cases of misuse since hash correlations "never find anything", and is therefore a waste of time. Both of these are difficulties of information, and perhaps of the approach, which have been examined already, yet it is likewise about the specialists' states of mind. These difficulties give off the impression of being incompletely brought about by the over–utilization of automation itself, yet the issue is truly what is robotized, where automation is placed, and who is utilizing it. [3, p. 11] Examiners run tools what they like most and trying to avoid tools that don't work like they expected to work.

2. Digital evidence handling

The International Organization for Standardization (ISO) and the International Electro–technical Commission (IEC) consist of national bodies who participate in the development of International Standards for products, services and best practices. ISO/IEC 27037 provides guidelines for First Responders, and their expert advisers in relation to the identification, collection, acquisition and preservation of digital evidence. The most important three principles of digital evidence are: relevance, reliability and sufficiency. Relevance – with respect to importance, it ought to be conceivable to exhibit the reason why the material gained is applicable to an examination and what esteem it has to an examination. Reliability – the dependability standard requests that all procedures which are executed when procuring and dissecting the proof ought to be auditable and repeatable. Reviewing is the way toward reporting each strategy and instrument utilized amid the securing and examination of the confirmation and the conditions under which they were utilized. This incorporates the product form quantities of the instruments utilized amid investigation. Reviewing makes it conceivable to build up repeatability and reproducibility. This is vital since an autonomous assessor might need to check the exercises performed by a person on call or measurable expert at a later date. The proper documentation of each reference taken will guarantee that they can do this and accomplish the very same results. It ought to be noted however that repeatability is not generally conceivable, for instance the securing of unpredictable information. Sufficiency – the last rule of computerized confirmation taking care of is to guarantee adequacy. Now and again it may not be conceivable to grab a whole machine and the particular obtaining of potential confirmation might be more fitting. For instance, if the seizure of the gadget will influence business congruity, the gadget is a necessary part of a well–being or mission–basic framework, or the physical size of the gadget makes it unfeasible to transport. The competency of people on call is central, specifically concerning the particular obtaining of computerized proof, and in a few jurisdictions this must be shown and checked. It is the obligation of the business and the person on call for guarantee that fitting abilities are kept up through steady preparing and operational experience. It may not be reasonable to keep up an abnormal state of ability with each sort of computerized framework. In any case every person on call ought to have the capacity to speak with a suitable expert, when a gadget is experienced that is past their own level of mastery. First responders must know that computerized evidence can likewise be a wellspring of physical evidence. [28, pp. 14–15] First responder could be police inspector or examiner. On the crime scene there is always need to respond properly.

Discovered traces have evidential significance in clarification of the crime facts. Because of that the trace detection, recording and evidence taken away in investigative proceedings, wrapping the objects confiscated need to pay more close attention. This must be done skillfully. Traces can be used resolving various identification tasks. Transmitted material should contain as much evidential information needed to establish investigation goals. Best practice is to bring from a crime scene an object with a trace. Because it is not always possible, then a part with a trace may cut out or certain part of object can be separated. If this is not possible, or good trail copying resources can be used, then trace prints or specimens can be done. What hardware or software to use depends on the examiner awareness? [39, pp. 34 – 35] So basically can happen that officer may want to cut off from the wall firmware RAID system that was used for the criminal activities. This is not always the best solution to trace cybercriminals and it will definitely shut down business process.

A comprehensive report of all activities undertaken by the investigator during an investigation would contribute positively to an investigation. This is an essential step which could be critical when a case reaches court. If appropriate, use a template to document the examination and analysis. Should such templates not be available, you should ask for such to be elaborated. To have a structured report prevents you from overlooking certain things, and makes it easier for those who hate to read various reports emanating from different investigations. Remember to write the summary and the memo without using too much of specialist terminology. The report will perhaps be read by persons without any specific knowledge in the subject. Include technical descriptions as enclosures. Discuss problems of secrecy e.g. trade secrets the safety of the realm etc. Make a "dictionary" that explain technical expressions. [40, p. 45] All activities with electronic evidence must be repeatable or explained why the action cannot be repeated later.

2.1 Importance of the routine work automation

It is critical to mechanize routine works. It's obvious and entirely understandable that the attention fades if we repeat same thing several times. Computerization can be extremely useful in a cases like that. Exceptionally automated computerized crime scene investigation – in some cases alluded to as "push–button forensics" (PBF) – gets much critical feedback from the advanced examination groups. For the most part, reactions seem to concentrate on two parts of advanced examinations: a weakening of master learning by an over dependence on PBF, and an apparent less exhaustive, or lower quality, examination when depending on an abnormal high state of automation. [3, pp. 1–2] The author found that the BPF can be as addictive as computer game, but influence analysis is beyond the scope of this research.

Be that as it may, pundits likewise as of now acknowledge a specific level of automation to help them in their everyday assignments. Physically looking at every hash in a hash database, for instance, would be unrealistic without some level of computerization. The test–task comes when more elevated amount procedures, for example, examination, are being mechanized, furthermore when the examiner starts to free comprehension of the subordinate ideas of the examination. Somehow both of these methods are currently implemented. Computerized examination programming suits like Encase, Forensic Tool Kit, Autopsy Forensic Browser, and others permit an examiner to direct preparatory, and even some mind boggling examination assignments basically by knowing which button to press. These well–known instruments try to make the employment of the specialist less demanding, or even evacuate the master through and through, as found in a case from Access Data (2009): "Digital investigations are no longer the exclusive domain of highly trained experts". Full–included legal programming suites are not by any means the only potential wellspring of issues. Basic projects, for example, Trace Hunter [8] give connection, understanding, and some examination of the Windows Registry paying little mind to the specialist's information, and the same can be said for scripts composed by experienced agents that are then appropriated to other people who may have practically no knowledge of the hidden procedures and information sources. Despite the criticisms, the truth today is that specialists are right now utilizing an abnormal state of computerization in examinations, and more up to date, or uninterested, agents who are prepared on a particular apparatus might be not able or uncertain how to do examinations without the utilization of automation. [3, pp. 1–2] Beautiful PBF reports can be sign of manipulation or try to hide a lack of knowledge IT forensic examiner in practice.

2.2 Exploring the analogies limitations

After searches author did find two similar solutions in Estonia. First solution is working in EKEI another in South prefecture of Estonia. Described solutions are made for managers to collect statistical information about examiners work and focus to satisfy manager needs. There is no practical solution yet like described in this work. EKEI program have no practical use for examiner to get data to analyze his own work. Both programs work like web based tables where is possible to mark some scores with minimal examination data. It is good if a manager can manage unit, another thing is helping IT forensic examiner to get better in his doings. There is no solution at the present time that will focus on examiner work and data collecting tools that can help electronic evidence examination expert later to remember what was exactly done with evidence during electronic evidence examination process. When the expert needs an information he writes it down into his notebook. To remember everything that is done during the examination is very important to the examiner in case of expert witness testimony. There is no use of manager statistic notes for witnessing because that is needed there are forensic examination notes. Furthermore, other investigators who are usually involved with investigation process will ask examiner notes repeatedly and manager data cannot give good preview about all procedures done by an expert.

When the focus is on manager, a work rear phenomena named “dry–labbing” can take place. It practically means that an examiner starts collecting points only counted by the manager and writes down fake reports, lying about performing an assigned experiment that is never done. Even when an examiner wants to get better results, it is seriously wrong to do “dry–labbing”. Avoiding the “dry–labbing” phenomena described, there is a solution that an expert should take photos (look Appendix 1 and Appendix 2) of the experiment or research. Taking photos solves the problems arising in the course of the examination too. Sometimes things need to be pointed back and then it is good to have the photo from the exact condition of the item like for instance cabling of the hard–drives. Photos help to recreate the atmosphere which can contribute to the authenticity of examination. Appendix 1 consists laptop staged examination and Appendix 2 consists mobile phone staged examination photos done by author.

2.3 Technical aspects

The specialized perspectives incorporate for the most part GUI design issues. All database GUI points of interest must be there for a reason and just on the off chance that data gathering must not be permitted. Forbidden structure perspective was utilized for entering information since it was helpful to utilize. Looking over structures on a large scale won't give all the information that was significant in choosing process on a single glance. A fascinating part is associating the analysts’ data with structure, permitting to include inspectors’ information when required. This usefulness will guarantee that the base can be utilized by more than one examiner if required. Additions should be possible by simply selecting the examiner’s name or pressing button "Add" for additions. The view of examiner’s form is presented on Figure 1.

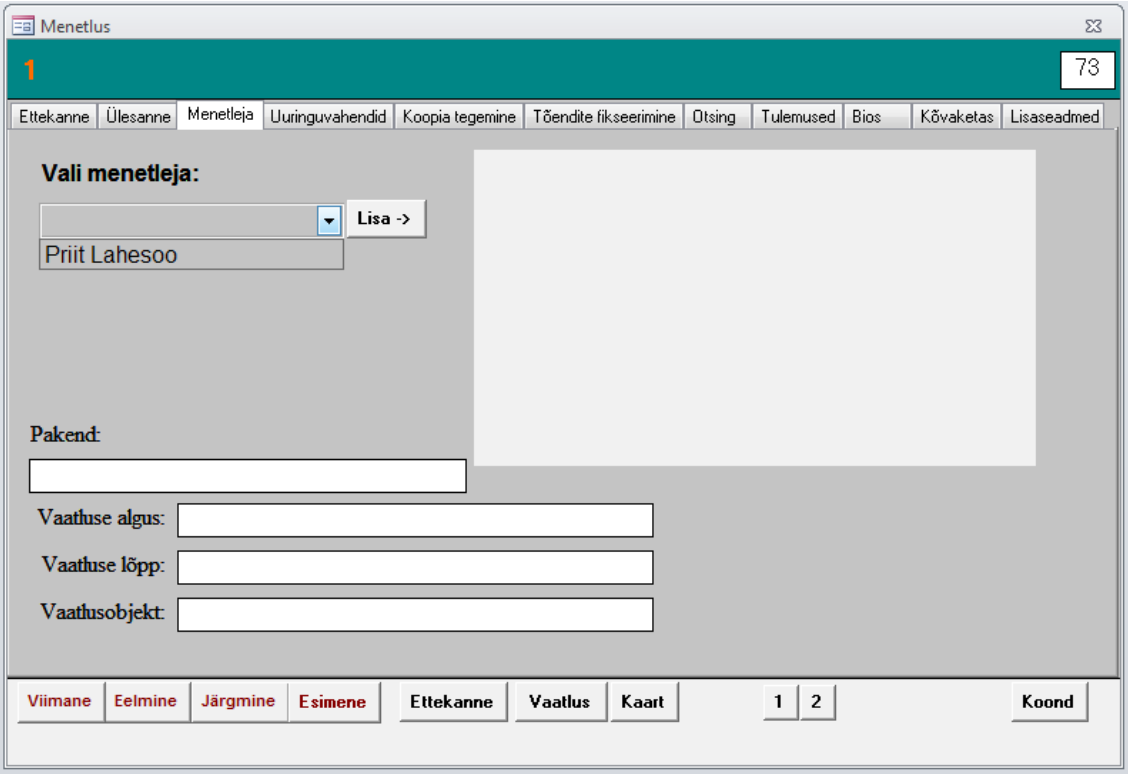

Figure 1. Examiner form view (by author).

Graphical Interface is made essentially and obviously so when MS Access is working legitimately, it ought to be reasonable through touch and test hone that author like to do most frequently.

2.4 Juridical aspects

Database will be should have been enlisted according to the law. However, the law does not decide precisely what level of enactment report is required when a database is made. Estonian Public Information Act directs the circumstance in § 43[9]. It is sufficiently clear that IT Forensic inspector notes cannot be open data. It is data that is characterized as confined or is all the more profoundly involved with privileged insights that cannot be distributed. Estonian Public Information Act characterizes limited data in § 34[9]. Created database test is intended to be for inspector individual note pad tool and picking insurance measures is left to the proprietor shoulders. There is no lawful difference with agent dark note pad, so there cannot be an issue of monitoring how the employment is finished by analyst. Be that as it may, national law ought to be taken after when wanting to change the work process.

In electronic evidence examination is only allowed to use the equipment and techniques which does not cause changes in critical characteristics of the electronic device. Electronic evidence examination protocol shall be drawn up in accordance with the national law. The Estonian Code of Criminal Procedure [1] §86, §87 and §146 must be followed. The participants in investigation proceedings, with the exception of the suspect and the person accused, must be explained that according to the Estonian Code of Criminal Procedure [1] § 214 the pre–trial proceedings information shall be published only with the permission of the

prosecutor's office and only to the extent specified. The defense counsel is required to maintain the confidentiality of the information obtained during criminal procedure. In the course of criminal proceedings, defense counsel is permitted to share information obtained through legal assistance have become known to the defendant only. Information about defendant can be published by defense counsel only with the consent of the defendant and when the interests of justice require so. In criminal proceedings may participate translator, who has warned unjust refusal to perform person duties and conducting a knowingly false translation. Failure to follow the warnings can cause criminal liability to the translator.

2.5 Institutional framework for automation

Cognitive work analysis is adapting the work to the individual, practical and cognitive changes to the assignments or relationships by altering their borders. Concentrating on data conduct at work, cognitive work analysis sees human–data cooperation with regards to human work exercises. This implies that the creation of every system which work in accordance with the people creator should thoroughly understand – the work people do, how they behave with information, the domestic life in which they work, and the causes of their behavior. Along these lines, Cognitive work analysis concentrates at the same time on the errand the on–screen characters play out, the earth in which it is completed, and the perceptual, psychological, and ergonomic qualities of the general population who do the assignment. A realistic presentation of the system is given in Figure 2. In this presentation, every arrangement of qualities specified above is assigned with a circle and is viewed as a measurement for examination. In this way, every measurement is a large group of qualities, elements, or variables, contingent upon the reason and technique for a study. As cognitive work analysis explores the settings of data conduct, one–time studies must be done approximately, because it is important in order to outline data frameworks, not to configure a general information system. Results from an assortment of concentrates, in any case, can be joined together and summed up to advice the outline of other information frameworks. [15]

To further clarify the cognitive work analysis measurements, consider an undertaking to concentrate on the data conduct of instructors in an IT forensic LAB, with the point of creating outline suggestions for a data framework to bolster the examiners' work. In this thesis cognitive work analysis measurements for deeper analysis can be explained in detail:

The workplace – it examines the situations in which the IT forensic LAB works. Case of inquiries: What are the government, state, and IT forensic LAB region directions under which the IT Forensic LAB works? What is the state strategy and measures for the IT forensic LAB educational modules? What is the populace from which the IT Forensic LAB can select studies? [15] Determines the general variables and development opportunities.

Work–space examination – considers the work that is done at the IT forensic LAB. Case of inquiries: What are the objectives of every association? What are the limitations inside which it needs to work? What are the exercises in which every association is included? What apparatuses and innovations it uses to solve examination? [15] Analyze workspace for development.

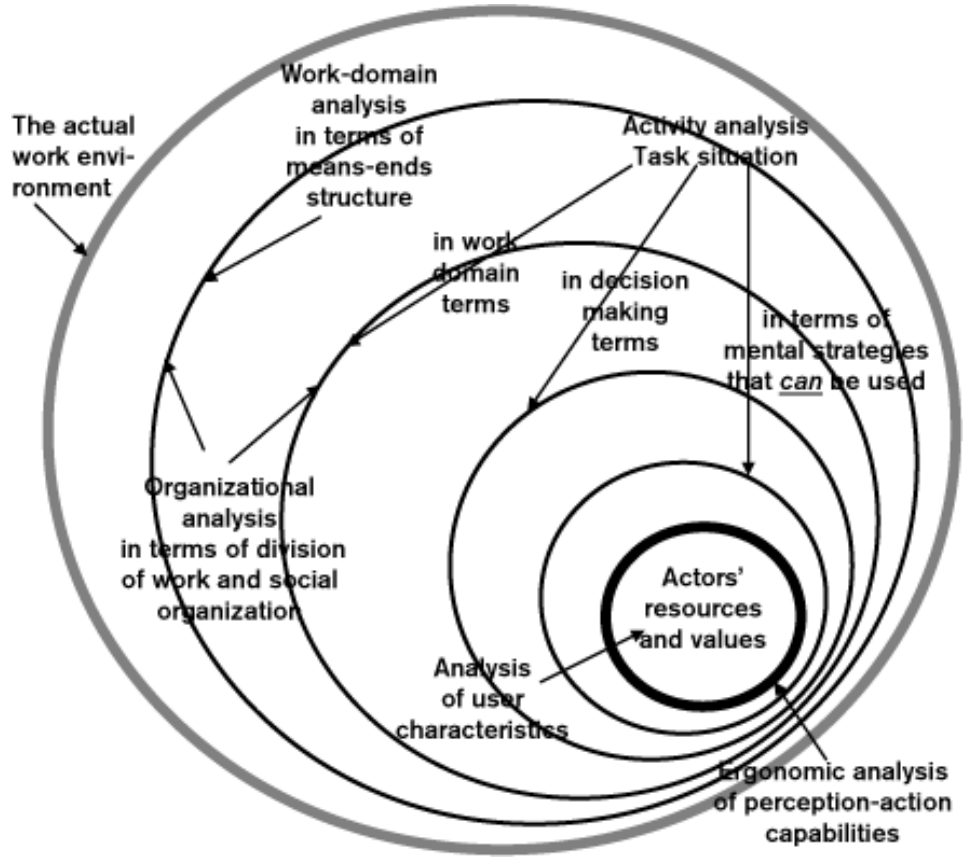

Figure 2. The dimensions of Cognitive Work Analysis [15]

Assignment analysis – takes a gander at particular assignments and break down them with the same inquiries. Case of inquiries: What are an examiner's objectives for examinations? What are the requirements an examiner faces in get ready and conveying an examination? What data sources does an examiner counsel? [15] It is very important to find answers to understand examiners work.

Organizational analysis – it analyzes the administration style, the authoritative society, the social traditions, and how parts are dispensed. Case of inquiries: How does the examiner speak with the investigators? Why was the examiner distributed to educate investigators? Who chooses whether or not the examiner ought to give a presentation in a court session? What method does this procedure take after? [15] How management works is always important also.

Decision analysis – gives a more particular investigation of individual choices. Case of inquiries: for an examiner's choice whether certain information would be significant for an investigator, for occurrence the issues included may be: what data does a LAB manager need to settle on this choice? What data sources are accessible to him? What tools are attractive yet not accessible? [15] All people are different and choices can be too.

Strategies analysis – for every errand and choice, analyzes which procedures are conceivable. Case of inquiries: How can an instructor who is searching for example to use in his instruction discover it? Case in point, would he be able to get some information about example? Could he search in a book in the library? Can he go to a web page he knows on the Web? Will he look workmanship databases? [15] It explains the operation options.

Client's assets and qualities examination. Distinguishes attributes of every gathering of clients. Illustrations: What is the experience an instructor has in searching for visual data? What is the information an instructor has of expressions of the human experience necessities gauges? What are the most critical qualities an instructor holds? What is the learning of a LAB bookkeeper about craftsmanship? What is the level of significance a LAB manager ascribes to incorporating craftsmanship in the educational modules? [15] Quality must correspond to the price ratio.

Despite the fact that the measurements are laid out in a specific request, utilizing them in real ventures takes after no settled grouping. Due to the reliance among the measurements, a scientist moves starting with one measurement then onto the next in an iterative procedure. The way of this development is controlled by the specific issue within reach furthermore by commonsense contemplations. [15]

From the point of view of data looking for, one may translate Figure 2 unmistakably. Assume one wishes to break down data looking for conduct of a gathering of individuals (as opposed to outline a data framework). Data looking for conduct shows itself by the methodologies that individuals utilize (see Figure 2), that is, the techniques they use to discover data. Plainly, a large group of variables outer to the conduct itself impact the determination of methodologies. In the frameworks approach wording, such components are called requirements, calculates that influence information conduct, yet can't be changed by it [16].

The measurements introduced by cognitive work analysis speak to the limitations on data looking for, beginning with the outer environment of the work spot to the individual assets and estimations of the on–screen character. Every dimension makes the imperative for the one settled in it. Along these lines, the workplace influences how a work spot is working, and this method of operation shapes the undertaking that a performer performs. The undertaking, thus, influences the choices that an on–screen character makes, and these choices impact looking for conduct. In addition, the actor's characteristics have an effect on seeking behavior and so does the social organization of the work place. Cognitive work analysis, require that while one can portray data conduct, without considering these limitations, the most ideal approach to investigate data conduct is through a top to bottom examination of these requirements. Work examination is, in this manner, an investigation of the limitations that shape data looking for conduct. Concentrating on the examination of the conduct forming limitations, instead of on the watched conduct, makes Cognitive work analysis especially helpful for the outline of data frameworks. [15]

A minor depiction of a watched conduct presents different issues for designers. Individuals' data conduct is educated by the mental models they have on the data world around them, yet some of these models can be deficient or off–base. The configuration of data frameworks ought not to be driven by such models. Further, not all individuals have the same mental model but rather an originator can't know which models are finished and revise. Moreover, the data frameworks that are as of now set up, and their impediments, enormously impact their clients' mental models and their data conduct. When in doubt, be that as it may, fashioners attempt to make new, or enhanced, frameworks, as opposed to duplicating existing ones. [15]

On the other hand, by picking up a top to bottom comprehension of the elements that shape data conduct, specialists can figure out what data conduct examples can happen, or what techniques can be utilized, autonomously of how watched on–screen characters collaborate with current frameworks and so on. [15]

This liberates the configuration from its reliance on the capacities of existing frameworks and their adequacy during the time spent human–data communication. As a result of its inherent adaptability, Cognitive work analysis gives no formulas to its deployment. While other exploration structures frequently train analysts what techniques to utilize, and what things to ask, Cognitive work analysis does not subscribe to an arrangement of strategies, or examination questions. It offers a general approach, and requires the individual analyst to choose the fitting strategies and the particular things to ask, in light of the wonder that is being researched. This presents two noteworthy difficulties. To start with, to apply the methodology successfully requires some learning and involvement in human data conduct research. Fledgling human data conduct analysts may experience challenges when endeavoring to utilize this structure interestingly. Furthermore, while rules about helpful strategies and exploration inquiries can be created for a specific work space, these cannot be naturally summed up to another area. Be that as it may, it is likely that building up a rich custom of applying Cognitive work analysis to the configuration of data framework would produce rules that would control future studies in different spaces. [15]

Notwithstanding the learning level required from a specialist, completing an intellectual work examination with the end goal of outlining a data framework is profoundly asset requesting. Since the cognitive work analysis approach requires a top to bottom comprehension of the imperatives and procedures set up, an ordinary study includes a broad field study notwithstanding the lab experimentation that is required for the outline itself. While not inalienably a test, such an inside and out methodology is not generally simple to bolster in our seasons of rare assets for examination and inclination for quick results. The need to make a scaffold between the investigation of human data conduct and the outline of data frameworks has been voiced in Information Science and additionally in different ranges, for example, Information Systems [17]. [15]

Cognitive work analysis gives one way to deal with how to research in human–data communication pertinent to frameworks outline. While tending to the broad zone of human–data communication, Cognitive Work Analysis adds to the investigation of data looking for in setting in different ways. [15]

While it doesn't recognize the particular connection related variables that influence human–data communication for all on–screen characters, it depicts the measurements that together with shape and add to this association. In addition, these measurements have been created through numerous experimental investigations of human cooperation with frameworks in the work put, and can be utilized to break down this collaboration and help in the outline of data frameworks. Through its measurements, layouts, and developmental methodology, Cognitive work analysis has demonstrated exceptionally successful in exploring the intricate and element nature of the connection and the marvels that human data conduct research addresses. On the range of exploration methodologies, going from the reductionist and generalizable methodologies, to the all that encompassing and individual ones, cognitive work analysis is set some place in the center, adjusting a comprehensive methodology concentrating on the errand or capacity on–screen characters perform. [15]

While, to date, just a couple data frameworks have been planned in according to this methodology, they have demonstrated very well and had huge influence on configuration. Since the headway of cognitive work analysis relies on upon exploratory examination, future investigation in human–information association won't simply bring about improving the requirements for the diagram of additional information systems, it will in like manner encourage refine the general utilization of cognitive work analysis to the design of information structures. [15]

Because author is working in West prefecture where research has been conducted, he has some experience and cognitive work analysis is much easier to do, otherwise there could be a big problem to meet customer needs. Way how author did work analysis description was presented in section 1.5. Mistake that job description differs from job people do, can happen very easily and that is the reason to do work analysis. Especially before starting building whatever solution or design.

3. Study area

General principles of electronic evidence examination protocol are basing on inspection of the crime scene protocol. The basic part of the electronic evidence examination protocol must always be complete and exact. Collected information must be presented systemically and objectively.

There must be described starting from crime scene:

1. The observation conditions (light, weather).

2. The milieu of the crime scene.

3. Items taken from the crime scene. For complex objects their general features and unstable peculiarities must be recorded. Electronic evidence examination protocol can be compiled later in the LAB on that draft.

4. Negative factors (evidence is not in accordance with the kind of investigation version).

5. Used equipment tools and results.

6. Packaging method description of the items confiscated.

Into the protocol must not written explanations or conclusions. After transporting electronic evidence in the LAB, IT forensic examiner can start electronic evidence examination and fulfill protocol. Because electronic evidence does have a latent content there is not enough just describing device outside. There is a need to describe devices logical content and produce feedback to investigator, if there is something blocking access to devices content or device just broken. There is more about activities in the LAB in section 4.5

3.1 The role of the processing unit

Information technology crime unit will not process criminal cases alone. They have a supportive role in the criminal cases processing for other entities e.g. making copies, fixation and analysis of electronic evidence. Based on unit issued data storage analysis report, a police officer specialized on computer forensics (IT forensic specialist) compiles investigative activities protocols. Fulfilled documents belong to a criminal case under the direction of another police officer. In addition to the above, the unit offers counseling as assistance to the police officers who need it. Back–office service is people behind–the–scenes working. In order to better understand this, two practical examples presented here.

A police officer is calling from the crime scene, where electronic equipment is found. What is this? Does it contain any electronic evidence? How should this to be handled, to properly preserve evidence?

A police investigator plans to conduct a search and is known in advance that the electronic evidence will be found at the location of the search. What guidelines should be followed, so

that the evidence will be preserved? In certain cases, it is reasonable that someone has to go from IT Forensic specialist units to provide assistance.

Digital forensics is the act of gathering, examining critically and giving an account of information in a way that is lawfully allowable. It can be utilized as a part of the recognition and counteractive action of crime and in any question where proof is gathered digitally. PC criminology takes after a comparable procedure to other scientific trains, and faces comparable issues. [34] Electronic evidence examination may in many ways be considered one of the wider spectrum of expertise in all species. Kristel Meikas bachelor thesis is most revealing document for author to understand what methods are used by EKEI experts in computer forensic examination [41].

Digital forensics can be divided between five different shares – computer forensics, mobile forensics, database forensics, live forensics and network forensics. [35], [18] There are certain procedures and methods that should be taken after to keep electronic evidence authentic. Every share can be treated like it is presented on a figure 3. [18] Destruction is missing from figure 3.

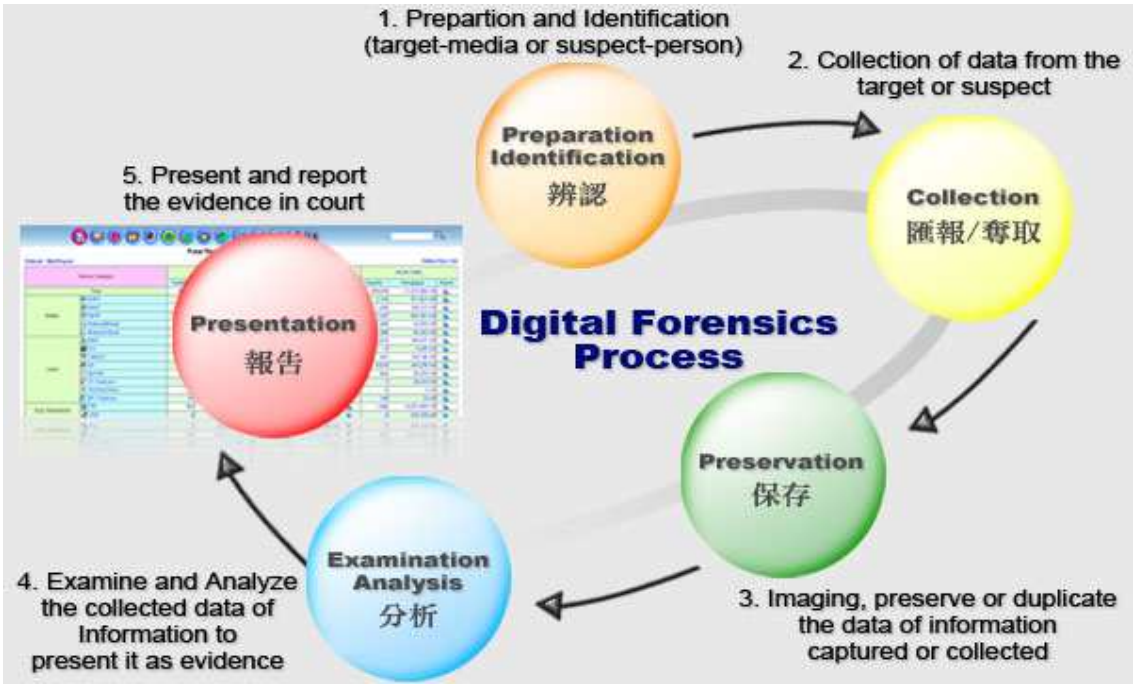

Figure 3. Digital forensics processes and procedures [18]

Destruction is commonly used after presentation phase. The magistrate may decide to order destroy the equipment. Because court usually don't have to destroy devices. The knowledge gained through examination will help examiner destroy electronic evidence effectively.

3.2 Digital forensics processes and procedures

Unlike to the picture 3 in Estonia there are essentially six stages of digital forensics forms – Preparation and Identification, Collection, Preservation (Imaging and Duplication), Examination and Analysis, Presentation, Destruction.

3.3 Preparation and identification

Forensics examiner or investigator has probably done all their planning before leading the legal sciences case. This incorporates the readiness of the apparatuses and fundamental hardware for conduction of the work. Forensics examiner of investigation must have the capacity to distinguish the suspect, a man or a gathering of individuals, (for example, acquiring the suspect's individual data which incorporates settlement, work, voyaging records and so on.) or the objective, (for example, the suspect's tablet, PC, cellphone, scratch pad etc.). Computer forensic examiners ought to survey the advanced confirmation completely, regarding the extent of the case and they need to decide the strategy to take. [18] Preparation must be made according to a criminal offense.

3.4 Collection

Once the suspect or target is recognized, the following phase of cybercrime scene investigation procedure is to gather the key information and data which will be helpful for examination and investigation. This accumulation of required data can be from a physical gadget, for example, a PC hard drive, USB disk and so on. It can be an ongoing information exchange session, for instance, information that is caught or gathered from a LAN or WLAN networks. [18] Before electronic evidence examiner starts activities on the crime scene he must get the leading officer – crime scene manager permission.

3.5 Preservation, Imaging and Duplication

Electronic evidence, by it's extremely nature, is delicate and can be adjusted, harmed, or crushed by ill–advised taking care of or examining. The examination is best led on a duplicate of the original device content. The first proof ought to be gained in a way that ensures and preserves the trustworthiness of the evidence. There is a need to protect the copy of the gathered information or data to secure the collection in the event of any harm for further examination or reference. At the point when protecting of imaging this gathered information of data, crime scene investigation specialist needs to guarantee that there is no adjustment of information copied. Along these lines using write block device and hashing is typically mandatory (MD5 or SHA1). [18] Most part of imaging work will do computers so in practice this work is done at night.

3.6 Examination and Analysis

Criminology inspector and agent will need to look at and investigate the acquired information. This critical data recovered or acquired will be valuable to be introduced as an evidence in court or to be used for further knowledge operations. The motivation behind the examination procedure is to withdraw and study digital proof. Extraction alludes to the recuperation of information from its media. The analysis alludes to the elucidation of the recouped data and placing it in a coherent and helpful format. [18] Examination produce input for presentation. Poor job at this stage is reflected in presentation stage.

3.7 Presentation

The presentation phase of the computerized criminological procedure is to report and present the discoveries and confirmation in intelligible and conspicuous form which might be valuable in term of law and in court. [18] Present findings in court house is always challenging task. In this stage, the experiences are very important.

3.8 Destruction

There is a lot of business software that destructs information by overwriting. Another approach to pulverize remaining information is to make a solid magnetic field which destroy data. Delicate data can destroy by physical destruction this may be the safest solution to destroy data. Physical destruction should be permanent destruction, avoiding of all possibilities to recover the information. Overwriting, demagnetization and physical destruction are three ways to destroy information by court order or request. Which way is best the examiner should decide.

4. Examining evidence

In computer forensic examination, it is important to describe in detail the appearance of the computer. Describing the appearance of the device is very important to distinguish particular gadget from other similar devices. Development in digital photography will let digital photos be made in a cost–effective manner and there is very appropriate to use for a wires placement fixation photographing. Photos taken should be based on the practical need and minimum indicative views could be photographing e.g. in a case of desktop computer: view in package, a front view, a rear view, view onto the side panel or after mounting side panel removal, view of the hard disk cabling, view hard drive and view onto making an identical copy with write–block device. Each device typically requires a unique approach e.g. in a case of laptop computer minimum indicative views are: view of the package, a top plan view, a bottom plan view, overlooking the serial number on the sticker, laptop open view, view of the arrangement of the hard drive in computer case, view of hard drive, view onto making an identical copy with write–block device. To ensure chain of evidence hardware write protection device is one very important tool to describe if making identical copy. If software method is used there is certainly need to write down the name and version of the software. One possible approach how to make electronic evidence pictures from laptop shown in Appendix 1 and mobile phone in Appendix 2. Taking photos sometimes can expand examination if new memory devices come out from certain device slots.

PCs and information transporters are currently utilized so widely that in the medium examination case essentially a PC can be discovered that requires speedy exploration like a little book with clear pages for composing notes in. In such cases, it is adequate if the individual directing the procedures has a straightforward tool for secure digital media visual perception. Regular home or office PC archives, email, the review don't require complex mastery in programming, and the user does not need to know file system highlights. It is sufficient to simply prepare, which concentrates on computerized media to the right treatment of media duplicate. It is essential that the overview would be guaranteed in the readiness of unique information's perpetual quality of physical evidence, and in addition the media information would be settled in a manner that the data storage medium by rehashed attacks is indistinguishable to the obtained outcome. [13, p. 11] Examiner work need to be valid, authentic and repeatable by third parties after examination is done.

In reality there are three most basic strategies being used. Scientific, overview or examination and blend. [4, p. 18] The basic strategy is chosen by examiner when examination starts and it often determines the course of the all other proceedings.

4.1 Scientific approach.

Scientific methodology resembles a global approach to inspecting a PC in pursuit of proof. It is an experimentally affirmed strategy to distribute discoveries after examination. Fred Cohen gives the best knowledge here to clarify the electronic evidence examination philosophy. Estonian methodology utilized as a part of IT scientific examinations by author won't fluctuate from this system. [4, p. 18]

In many zones of science, an exploratory strategy comprises of four components:

> (1) Examine the past and also current speculations, strategies, and test bases;
>
> (2) Distinguishing irregularities between current speculations and repeatable exploratory results,
>
> (3) Conjecturing new hypothesis that clarifies discredited speculations, and performing experiments to test the new hypothesis, and
>
> (4) Distributing the outcomes. [10, p. 8]

This is the most tedious examination technique. From study to get distributed it might take years which can't be from beginning to end examination in the sensible limits of time. In any case it is the farthest reaching and distinct technique. [4, p. 18] Author practice with this technique has been very splendid. Good explanations and intelligibility confer an advantage in the court and that is fascinating. It is time consuming method and if time is really an issue blend method can be used. Describing author version of this method there is an examination protocol that contain data about examination activities and different appendixes that contain photos about device, identical copy making data and evidence files found descriptions.

4.2 Survey and examination approach.

Survey and examination are for the most part the utilized methodology by Estonian Forensic Science Institute specialists. This method can be used by all examiners to get quick and dirty results if speed is an issue. Each case has an interesting profile and a specialist will attempt to help with study to make sense of what is truly required by the agent. The survey is essentially a basic, down to business way and tedious works like catchphrase inquiry with file recovery can be alluded to as examination. An overview can develop into an examination. [4, p. 19]

4.3 Blend approach

Blend or mash–up or chicken soup called method mean a composed mixed report. In this work second and third examiner use this kind of approach on a regular basis. While writing this type of report, the expert will put all pictures, appendixes and examination data into one big examination report. The reason for making a report like that is based on national law that demands signing all appendix pages when they are submitted separately from the examination protocol. Making a blend report, the appendix becomes a part of the examination protocol and separate signing is not needed. The overall logic of this is that appendix is the separate document also, such as the examination protocol, and is an integral part of the examination protocol. The idea of signing of each document is the point that the author of the document confirms the accuracy of the document by giving the author's signature. In practice, it is essential that different procedural steps are conducted by a number of investigators. When one investigator describes the operation launched, the second draws a diagram and the third takes photos, and will make printouts later. In a case like described here, every investigator will take responsibility for the work done and gives personal signature to confirm it. [4, p. 19] Blend is most popular report type at the moment of writing this thesis.

A mash–up report is not always a very clear and understandable report so if the expert witness testimony is in order, a blend report should not be made. It is better to choose scientific approach. [4, p. 19] This technique has the speed advantage of other methods. It also raises many questions as always occurs when things are mixed up. With confusion over reporting electronic evidence examiner is responsible for ensuring that all mixed up parts are treated as appropriate. Another problem with this report is that sometimes investigator cannot expose some part of electronic evidence examination protocol to defendant for example in case of indecent images of children. If electronic evidence examination report written like a chicken soup it is very difficult to take indecent images of children out from the examination protocol. This may lead to the offender undue happiness. It is probably not good for the offender to have his electronic evidence examination pictures in jail. The world does not need to be a rough place. Blend report is still most popular method for reporting, because learning to use scientific method takes a lot of time and effort. It is also not a big problem if the right people doing the right things duly.

4.4 Fieldwork with electronic evidence

Preservation of the evidence at the scene of crime does not differ significantly from retaining the electronic evidence at a LAB. On the other hand, the time for wrapping up is noticeably more limited than in a LAB. Technical operation must be carried out immediately and making mistakes must be avoided at all costs. In case of the failure of a technical operation, evidence may become unfit for use. Situations like that must be avoided. Time factor and the accuracy of work at the scene of crime are of high importance and all that must be considered too. Making an identical copy, the examiner must also be very careful with planning the time. Copying huge data arrays take a lot of time and very often, copying all of the information is unreasonable – sometime an excerpt would be enough. Certainly there must be cooperation with the officer responsible on the scene of crime and in case of problems, asking extra information and specifying the facts from him would be the only proper behavior.

Estonian Forensic Science Institute (EKEI) has given proposals for specialist on call activities on the crime scene as it takes after:

It is not prescribed to turn on the PC when it is turned off. At the point when the PC is turned on, then work as it takes after. Take care not to go up to open the PC locks up it is not amended. This ought to be done again and again to move mouse by your hand, or utilize some kind of uncommon program that will do it for you, for example Mouse Jiggler. [4, pp. 392–393] Don't turn on or off rule must be known by every examiner and police inspector.

Documentation of all exercises and projects open need to be captured by a camera. The less disk changes made, the better, for instance, the PC screen pictures, or other data into the PC store, as opposed to specifically to outer media a PC disk for recording new data is written over the erased data that may have probative worth. [4, pp. 392–393] Taking photos on the crime scene dependably dodge allegations.

In case it is feasible, duplicate the RAM (e.g. software FTK Imager [6], or some other kind of freeware instrument), subsequent to the shutdown wreck the whole RAM and destroy all accessible data. [4, pp. 392–393] Memory duplication is always complicated operation on the crime scene.

It should be checked (e.g. software Crypt Hunter) whether the PC is open crypto containers. At the point if there is an encoded PC disks, there should be a specialist to make sensible duplicates with software, such as FTK Imager. Logical duplicates to be made in view of the physical duplicate is made for one single duplicate, which implies that the information will be replicated as scrambled, so there is not something to do with this copy later. [4, pp. 392–393] Cases where encryption is used are always very time-consuming cases.

To kill a PC power–cord unplugged or close down the association with "shut down"? There is no single truth, which arrangement is the best, in the light of the fact that every variant has its own particular advantages and disadvantages. The accompanying illustrative data on the premise of grabbing the PC to choose whether to interface the PC to the electrical plug or to close it in the ordinary way. [4, pp. 392–393] When in doubt, it is wise to consult with another examiner.

The old regular rule cable is hauled out to protect the information stockpiling medium, for example, they were exploiting the physical proof right now. By method for disparagement beyond any doubt the cable cannot be hauled out from the server. Nor ought to the cord be hauled out of the PC, if a database that have evidential worth is open, in the light of the fact that the database might be off base and become unsuitable for use. While hauling the cable out, it should be considered that now and again the operating system may never again start properly, and the suspect, after the PC has been returned will start complaint. When pulling the cord from the back of the computer, one needs to be sure to take into account that in some cases, the computer may no longer start the operating system. [4, pp. 392–393] Police should never damage legal business processes with the stupid actions. However, accidents happen even in the best families.

4.5 Lab–work with electronic evidence

The seizure and search of the data from electronic proof is normally better to be sought in the research center than on the crime scene. Hands–on work governs additionally apply to the LAB shown on figure 4. The shifting uncommon projects offer the chance to invest more energy, to break down the confirmation in the lab as opposed to at the scene. Information technology expertise and judgment to lead research must concentrate on the nature of basic leadership which ought, is not be left just in the hands of the machine. Information recovery is a critical part of the work of IT forensic specialists. The product capacity given by the information recovery is not generally sufficient for a specialist opinion. Completely programmed recovery tools' presence and use is important, generally speaking. No individual can extensively interpret any file system and consider it to be exactly like operating system demonstrates us. However – IT specialists must assess the outcomes and the opinion of the individual to give his skills and capacity to think at the same time in both human and computer. [13, p. 11] Year 2016 there was couple of free days for IT forensic examiner whose place of work is in the picture on figure 4.

Figure 4. IT Forensic examiner's workplace (by author)

4.6 Structured reporting

Organized reporting mean essentially a clear reporting framework. It resembles a recording report where each piece has its own particular spot. So a very much organized report leaves appendixes aside and spotlights on the important parts which are suitable for the last report. The last report must contain references back to the addendum data. The methodology depicted above won't generally won't ensure that the last report is comprehensible and justifiable. In any case, it will be huge stride towards understanding.

As indicated by sources depicted some time recently, PC and its substance can be dealt with like physical proof, perception or as master conclusion. In any case, if there are signs that PC is a significant proof in a criminal case, it ought to be dealt with by Estonian Code of Criminal Procedure [1]. [4, p. 20] Reporting structure is determined by law that must be followed.

Depicted standards show how to handle proof gathered from the crime scene in the most solid way. Practically speaking, this implies recording it, pressing it into plastic bag and taking it into a LAB. In the examination of PC as physical proof, there must be gathered just necessary data. Information must be gathered with the motivation behind comprehending the criminal case or finding new hints of the crime. For depicted purposes, it is expected to analyze the substance of a PC. That should be possible with computer research software. It is essential to examine and assess the gathered information. [4, p. 22]

Through proof examination we can find a heap of data about various traces and about criminal individual, about carrying out of the criminal act and about losses. From Estonian Code of Criminal Procedure [1] §86, §87, §143 law sections are compulsory to take after if a specialist needs to make computer forensic examination in a way that is legitimately acceptable. [4, p. 22] It is always important and reasonable to take photos [37 pp. 952–953], [36 pp. 10–11] (look Appendix 1 and Appendix 2) to support described structured reporting.

5. Database model

Initially, the relational data model was created for database – that is, data put away over a drawn out stretch of time in a PC framework — and for database administration frameworks, the product that permits individuals to store, get to, and alter this data. Database still give us with critical inspiration to comprehension the relational data model. They are discovered today, not just in their unique, extensive applications, for example, carrier reservation frameworks or managing an account framework, but also in desktop PCs taking care of individual tasks, for example, keeping up cost records, homework grades, and numerous different employments. Different sorts of software other than database frameworks can make great utilization of tables of data too, and the social information model helps us outline these tables and build up the information structures that we have to access them proficiently. For instance, such tables are utilized by compilers to store data about the variables utilized as a part of the project, monitoring their information type and of the capacities for which they are characterized. [14, p. 403] Every table and relation in database has its unique purpose.

A gathering of relations is known as a database. The principal thing we have to do when outlining a database for some application is to settle on how the data to be put away ought to be managed into tables. The outline of a database, similar to all configuration issues, involves business needs and management response. In a case to tail, we might grow our utilization of an enlistment center's database including courses, and in this manner uncover a portion of the standards of good database plan. Probably the most intense operations in a database include the utilization of a few relations to express coordinated types of information. By setting up fitting information structures, we can bounce starting with one thread then onto the next productively, and hence acquire data from the database that we couldn't reveal from a solitary connection. [14, p. 406] Searching for illustration, database creator found that relational data model may be the most appropriate for handling the issue.

5.1 Model structure

Input data consists usually of collected observation data. Simplistic model represents all processes between evidence arrival and leaving in the LAB. Basically it consists of computer forensic examination, mobile forensic examination and some other special device forensic examination. So the most critical data are the device name, model and serial number. Other details depend on the device and examination purposes. Determined entities are people with roles like an investigator or an examiner, a device with roles to be researched or special research device and case. The chain of evidence report that is on the base criminal case written by electronic evidence examiner is a one final result document.

5.2 DB–modeling process

Database modelling can be started from idea with making Entity – Relationship (ER) model. That is a model or schema of how things are divided between tables. On figure 5 is presented ER–model that was practical object used by author for collecting examiners notes. The database solution that is practical solution of this thesis contains the following tables:

process {process_id, examiner_id, base, package, number, description, features, task, note, begin, end, given, model, serial, making, fix, ks_header, ks, result}

examiner {examiner_id, name, office, town, address, department, place, job, suitably}

bios {bios_id, process_id, enter, pass, boot1, boot2, boot3, time1, time2}

disk {disk_id, process_id, disk, model, serial, size, type, copytime, path, hash, name}

edevice {edevice}

device_link {process_id, ldevice}

itool {tool}

itlink {process_id, tool}

The database contains the following forms.

bios_subform, etk, disk_input, disk_subform, e_device, add_itool, edevice, examiner, examiner_subform, process, edevice

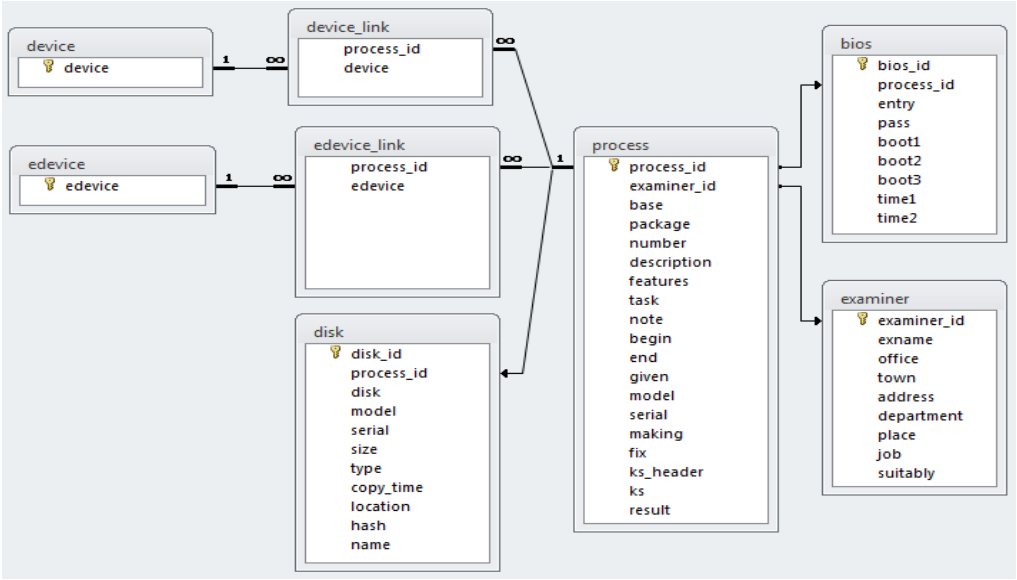

Figure 5. Database ER–diagram (by author)

Database user interface presented on Figure 1 was done by the author with some help of Microsoft Access sample databases. Sub forms are shown in tabular panes of the database solution. Tables and forms working together that is part of the solution. Experimental justify function was adopted from Justin Leban fJustiDirect Version 3.11 script. There are a lot of option to modify the database to meet examiner exact needs or develop it further to do more than just hold electronic evidence examination data.

5.3 Business model integration

General simplistic Police structure model is presented on Figure 6.

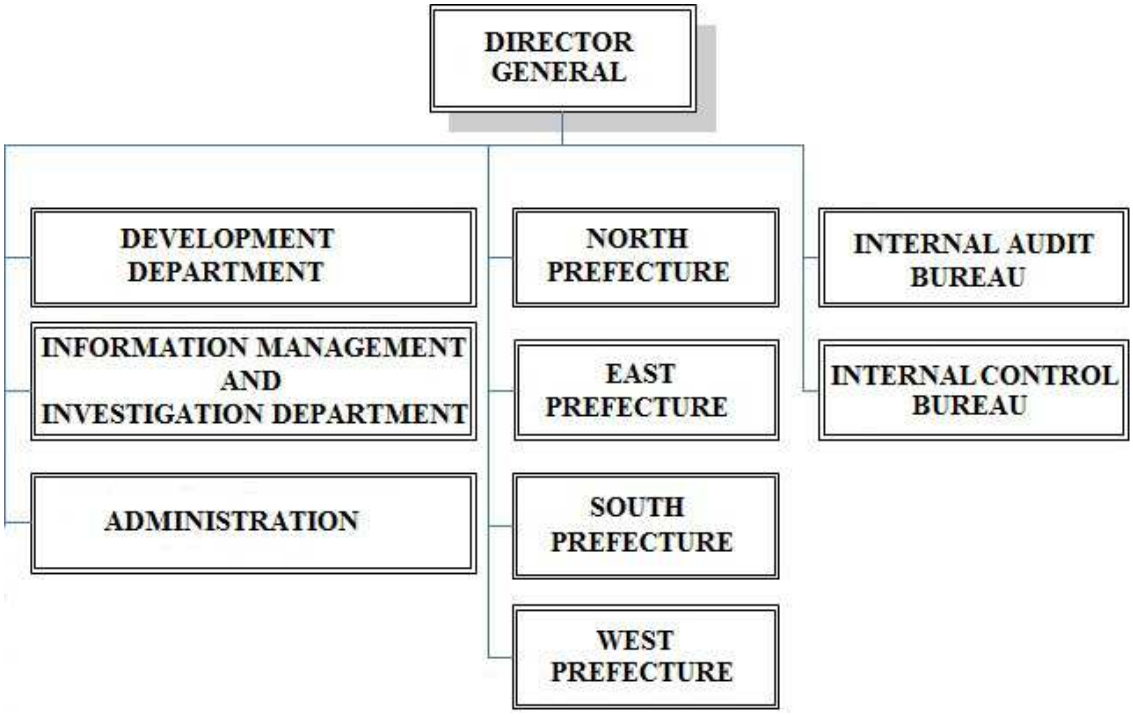

Figure 6. Structure of the Estonian police [20]

The author is working in West prefecture in criminal police bureau and testing data is needed for reporting and analyze of author's work results. Data is not collected specially for this research. However, it can use only by permission of owner for researching. Collected statistics are all about assignments, computer forensic examinations, other devices examinations, mobile and SIM surfing, other technical works, crime or criminal activities related technical consultations and other tasks. Collected data is used only for the stated research purpose and cannot be used for any other purposes. In the current research the data is used according to the permit from data owner (Letter from the Estonian Police and Border Guard Board, 11 February 2016, No 1.1–14/106–2).

The ISO 9001:2008 universal business standard contains the segments that have been recognized as basic to success. The standard, obviously, does not ensure achievement nor does it infer consistency in structure and documentation. It just recognizes the fixings that have been utilized to develop a division society portrayed by the execution magnificence and nonstop change. Administration and execution groups are relied upon to make extra parts and shape these fixings to fit their work units. It is the duty of the general population inside the division to consistently work with their inward and outer clients and suppliers to successfully utilize the fixings to at last build up an association particular quality administration framework contained interconnected business forms that frequently deliver law authorization items and administrations that meet all client needs. [29]

At the point when duty officers capture a subject as per office arrangement, state statutes, and/or city laws, care must be taken to guarantee strong association is kept up with supporting work units, including, however not constrained to, records, recognizable proof, crime lab, examinations, property administration, and prosecutorial forms. Generally, the yield of one procedure is the contribution of another process. The ISO 9001:2008 standard recognizes the structure required to successfully deal with the info yield availability of the organization’s arrangement of procedures. [29] Standards can help to build system.

Association's quality administration standards are vital to address client issues, since certainty of clients produces dependability that is required for organization’s presence. One of the meanings of a "standard" is that it is a fundamental conviction, hypothesis or guideline that impacts the path in which something is finished. "Quality administration standards" are an arrangement of crucial convictions, standards, decides and values that are known as genuine and can be utilized as a base for quality administration. [30, p. 3]

The quality administration standards can be utilized as an establishment to manage an association's execution change. They were created and overhauled by global specialists of ISO/TC176, which is in charge of creating and keeping up ISO's quality administration guidelines. [30, p. 3]

The seven quality administration standards are:

Customer center

Leadership

Engagement of individuals

Process approach

Improvement

Evidence–based decision making

Relationship administration

These standards are not recorded in need request. The relative significance of every standard will shift from association to organization and can be required to change after some time as well as organization changes. [30, p. 3]

The essential center of value administration is to meet client necessities and to endeavor to surpass client desires. Supported achievement is accomplished when an association pulls in and holds the certainty of clients and other interested individuals. Each part of client collaboration gives a chance to make more esteem for the client. Understanding present and future needs of clients and other invested individuals adds to sustained success of the association. [30, p. 4]

6. Method

First research is done as deductive quantitative primary data analysis. Examiner 1 was using Microsoft Access program solution as a basis for examination report. Examiner 2 and Examiner 3 using best word processors. **Hypothesis is that by giving basic framework in electronic evidence examination it is possible to speed up the execution time of the analysis work–flow.** It will be researched through collected primary research data which is collected for statistical analysis purposes by author and his colleagues.

Second research is done by six cases from every examiner in the LAB mentioned above. It is done researched through by author collected primary research data. Also is available to use evidence examination protocols for every electronic evidence device that come into LAB at least one year back however all sensitive data must be removed from the case to protect the third–party's privacy. Conditions were the same like in the first research. Goals was **by giving basic framework in electronic evidence examination it is possible to speed up the execution time of the analysis work–flow.**

Third research is done by sharing examiner 1 Microsoft Access database solution with other colleagues who interested to use it. Because research is done on the program learning phase it will not have influence previously collected statistics and does not affect the results of previous research. Assessment measuring usability with the Usefulness, Satisfaction, and Ease of Use (USE) survey [38] that was created by Arnold Lund and statistics collecting webpage is created and updated 18.05.2015 by Gary Perlman who work on making information more useful and usable by people.

6.1 Input Data

Authentic statistic data collected about years 2014 to 2016 sorted and unclassified for public level use. Table 1 will show analysis total results during the selected period. It must be mentioned that 2015 period end data consist unique seasonal data because of two unexpected expert witness testimony cases performed by examiner I. Table 2 contain devices by year comparison data. Table 3, Table 4 and Table 5 contain data about cybercrime group by years 2016, 2015, 2014 and table layout is similar to table 1. Table 6 is a summary of the examinations total by examiner. Table 7 is originally generated with Microsoft Excel analysis tool descriptive statistics and modified by author into one table. Table 8 contain z–test analysis result data. Table 9, Table 10 and Table 11 contain second research data about six cases time analysis. Table 9 is first examiner six cases data analysis, Table 10 contain second examiner six cases data analysis and Table 11 contain third examiner six cases data analysis. Table 12 is page count single factor analysis of variance about examiners six cases records. Table 13 is third research measuring usability with the USE Questionnaire analysis usefulness statistics. Table 14 is third research measuring usability with the USE Questionnaire analysis ease of use facts. Table 15, Table 16, Table 17 and Table 18 contain third research measuring usability with the USE Questionnaire analysis information. Table 15 consists usefulness information. Table 16 hold ease of use data. Table 17 accommodate ease of learning and Table 18 include satisfaction knowledge.

There was arouse an idea about categorization input data sorting in collection phase selection by category which can be high, medium or low. Author suggesting to collect examination times from initial stage more precise, now it has done on daily basis. It is reasonable

because it is feasible and give a very accurate picture of the situation. At the moment collected data do not contain information about the start and end exact time of the examination and there is only start date and end date, which makes the analysis more looking at the key trends. Qualitative research is basing on real evidence examination protocol data which are qualified as restricted for public use. Research itself does not contain third–parties identifying information or restricted data for public use.

6.2 Data processing

Distribution of working time hours during period of 2014 – 2016 show every examiner's contribution in work with electronic evidence findings. Due to different work tasks contribution, electronic evidence researches may vary. The selected period will focus only on the research problem. Statistics picking is made with an MS Excel project with different spreadsheets. Statistics collecting spreadsheet allow to select the appropriate start and end dates that are located in cells B1 and B2. The rest of the boxes were calculated automatically by formulas. Observing the hours of digital evidence found is basing on the assumption that it takes 40 hours to view the computer, 15 hours to view other device and 4 hours for a mobile surf the information. The starting point for doing this is the earlier results of practical measurements and evaluation of EKEI average computer examination time. In Table 1 analysis period is 01.01.2014 – 06.10.2016 and one working day consists eight hours. There are 698 days left after subtracting 24 national holidays. Table 2 consists devices by year comparison and basing on Table 1 information that come from Tables 3–5.

Workdays on D1 field equals NETWORKDAYS(B1;B2)–(national holidays).

Upper hours total equals 40*B3+15*B5+4*B6.

Lower hours total equals SUM(B9:B11)

Upper percent normal work–time total equals 100*B7/(3*8*D1).

Upper percent normal work–time for Examiner I equals 100*B18/(8*C7)

Lower percent normal work–time total equals 100*B12/(3*8*D1)

Lower percent normal work–time for Examiner I equals 100*C12/(8*D1)

Other investigator percent normal work–time is calculated same principles like Examiner I.

Computer examination total values are provided in Table 6 and distributed among examiners.

National holidays that fall on workdays are excluded from this analysis. In total 2016. Year national holidays 6 days fall on workdays and 6 days fall a day of rest. In report is recorded 5 days which cover data period. 2015. Year national holidays 9 days fall on workdays and 3 days fall a day of rest, total 12 days. 2014. Year national holidays 10 days fall on workdays and 2 days fall a day of rest, total 12 days.

The average time for computer examination is 40 hours by EKEI recommendation. After observing technological changes in computer forensic examination reporting author want to check does computer examination time is shortened. Three employees were chosen like one of them is using for examining computers the special designed MS Access program, and others are using best word processors.

The average time spent with the program, the first examiner used for the examination was 960 hours with standard deviation 2254,65443 hours.

Computer analysis total 3 employees on the period 2014 – 2016 have spent 63688 operating hours for viewing 126 computers. Computer examination by examiner in detail is presented on figure 19. That takes average 21226,7 hours per employee. Descriptive statistics are presented in Table 7. First examiner mode value show that most of the examinations did by this person take more time than one day. Other examiners indicator is at one day.

1. Statistical hypothesis:

H0: μ_0 is less or equal with 40 hours

H1: μ_1 is bigger than 40 hours

2. The sample survey of resulting statistical parameters for the first examiner:

Sample size n=31

The arithmetic average of the sample 960 and the sample standard deviation

s = 2254,65443

The empirical value of the parameter $Z = \frac{\bar{X}-\mu 0}{s/\sqrt{n}} = 2{,}65$

3. Significance level of 5% critical value is 1,645.

4. 1,645 < 2,65 consequently, the parameter drops to a critical region.

5. Because the z–test parameter falls, into a critical region, we must reject null hypothesis.

The observation result is consistent with the statement that the first examiner examination mean time is actually longer than 40 hours. Z–Test results are presented in Table 8.

Looking at the results it seemed strange that statistical analysis does not support directly hypothesis about speeding up work–time with a new tool. First and second examiner work about the same rate and third examiner is working significantly slower than others. So author took 6 random cases evidence examination protocol from every investigator participated in quantitative research. To be really sure that compared devices are compared like apple to apples, the author asked colleagues to leave out all cellphone and memory stick devices and count in only computers or computer like similar devices. Figure 20 describes in more detail how to calculate time for per case analysis. Analyzing the cases more closely the following were found:

The first examiner uses a well–established observing method for making evidence examination protocol with references to various appendixes. All observations made during examinations will be fixed in the protocol. The first appendix photos, second the data about hard disk copying, in subsequent appendixes can prepared by adding the file lists or more accurate statistical data etc. Number of pages per computer forensic examination is an average of 10.7 pages. Computer examination protocol is readable and all appendixes are referred. Observation time for six cases was 154 workdays, 156 days, 5 hours, 30 minutes. Counting down national holidays it will be left 153 days. More detail information about first examiner six cases work analysis is presented in Table 9.

The second examiner uses a concise laconic presentation style, which may be due to immature performance practice. Examination report constitutes the blend report, which has pictures, technical data and survey data all mixed with other observation results. The report is readable and terms in general comprehensible. Tightly stuffed data in the examination protocol always link to the digital material as an annex. Examination protocol is on average number of pages 2.7 pages. Observation time for six cases was 155 workdays, 158 days, 20 hours, 25 minutes. After the removal of national holidays, it will be left 143 days. More information about second examiner work analysis is presented in Table 10.

Similar to the second examiner, the third examiner uses immature and blended report base in presenting. Examination report contains various statistical information, screen–shots and images, and data found from the examination. The report is difficult to read but contain all the necessary data. Examination protocol size number of pages is an average of 10.2 pages. Observation time for six cases was 358 workdays, 360 days, 10 hours, 15 minutes. After national holidays removal there will be left 347 days. More detail information about third examiner work analysis is presented in Table 11.

Comparing show that most faster works second examiner, however there are hiding data in second examiner statistics that could be indicating wish to data manipulation. Second examiner selected and gave to author a period that consists a lot of national holidays that must be subtracted from workdays. Issue come out if to calculate the number of working days, however it’s not that significant in bigger plan and does not have influence to other data. Author leaved the tables unaffected. On the figure 21 is a graphical representation of the examiners selected period analysis. Figure 22, time analysis by six cases presenting weakest link pointing arrow exactly to the weakest link. Looking at the results it is clear that something speeding up first examiner work, because evidence examination protocol length is

about same size with third examiner protocol length and first examiner work time is about same with second examiner whose protocol length differs three times from others.

Usefulness, Satisfaction, and Ease of Use (USE) survey [38] was created by Arnold Lund as methods for comprehend the capability of interface of a framework and to make sure that created items could have a usability. USE poll comprises of 30 rating scales isolated into four classifications: Usefulness, Satisfaction, Ease of Use and Ease of Learning. Each of propositions classes have a few explanations that should be appraised with positive 7–point Likert scale. Essential is to understand, what regions the database GUI succeeded at and which require change. Affirmations in italics were found to weight not exactly the others. Author selected electronic form that was available from Gary Perlman webpage in order to collect the necessary data. Test description is presented more in detail in this work Appendix 3. All examiners agreed that it is useful and it saves time. It gave back control over activities in examiners life and make things accomplishment easier. Conclusion can be here that database is useful and need definitely further attention. About ease of use 3 examiner from 5 found it is easy and simple to use. It is flexible, using it is effortless and examiners did not notice any inconsistencies as they use it. It is interesting that only half of investigators can use it successfully every time. Ease of learning show that it is easy to use and most examiners learned to use it very quickly and become skillful. Satisfaction show that it was not annoying examiners. It is pleasant and fun to use and it could be a tool to recommend to friend.

6.3 Data protection

Data protection is an essential part in making a database or taking care of any information. There is access allowed to each client who has legitimate access to a PC account. Microsoft Access is not an extremely secure database framework. Generally, it's the inspector's issue how to keep the notes secure, so author determined the issue with scrambling database arrangement with outsiders' programming. It won't take care of the issue totally and somebody can take scrambled folder content when it is open. However, there is dependably a major hazard that interceptor can be exposed when the database is being used. Estonian Internal Security service decides in yearly survey 2015[19] the most perilous potential nearby dangers that can be an issue outlining database answer for uncommon needs.

In the district the author works, potential dangers incorporate digital harm and impact operations through digital assaults. While access to non–open data is viewed as imperative in digital insight, harm suggests acquiring access to PC frameworks with the sole reason for rendering a PC system or another PC controlled framework broken at a specific minute, or changing or erasing the information being handled inside it. Occasions in Ukrainian energy systems Christmas 2015, when malware was supposedly used to bring about expansive scale power blackouts, have created much exchange. [19, p. 22] Consider hazardous dangers depicted here the author expected to specify that information security is the continuous procedure and that can be enhanced consistently in sliding time window.

7. Database GUI

Graphical Interface shown on the Figure 7 is made simply and clearly so when MS Access is working properly it should be understandable through touch and experiment practice what author like to do most often.

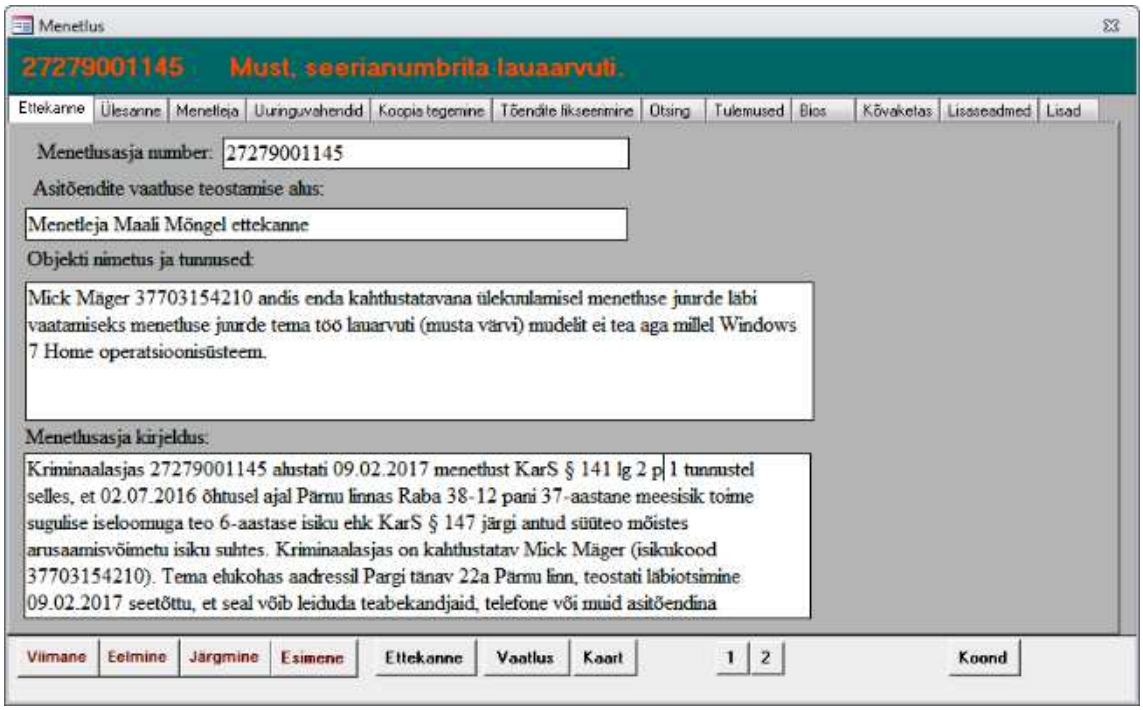

Figure 7. MS Access database GUI

Tabulation makes work with forms comfortable and filling text area give opportunity to generate examination papers more quickly. The buttons with brown writings are used to navigate between different cases. Working reports are examination report and total report.

8. Computer examination

PC examination is preeminent presentation of specialized aptitudes for the examiner. How to introduce the data found so, that a large portion of the general population will comprehend it? It has been dependably a million–dollar question for IT Forensic authorities. There is no straightforward answer or answer for this sort of issue and that is unquestionably one motivation behind why we have to research subjects all things considered. Basic Investigation of Computers electronic crimes program manual [12] characterize essential parts of PC where specialists can discover evidential information Figure 8 [12, p. 9]. This data gives comprehension and thoughts how to apply the subject. Cache and registers triangle portray PC content in point of interest and will help IT forensics expert comprehend what may be expected to seek. Unadulterated specialized methodology does not leave much space for legal interpretation. [4, p. 7] Cache and registers triangle figure 8 is one of the basic things examiner must see and comprehend.

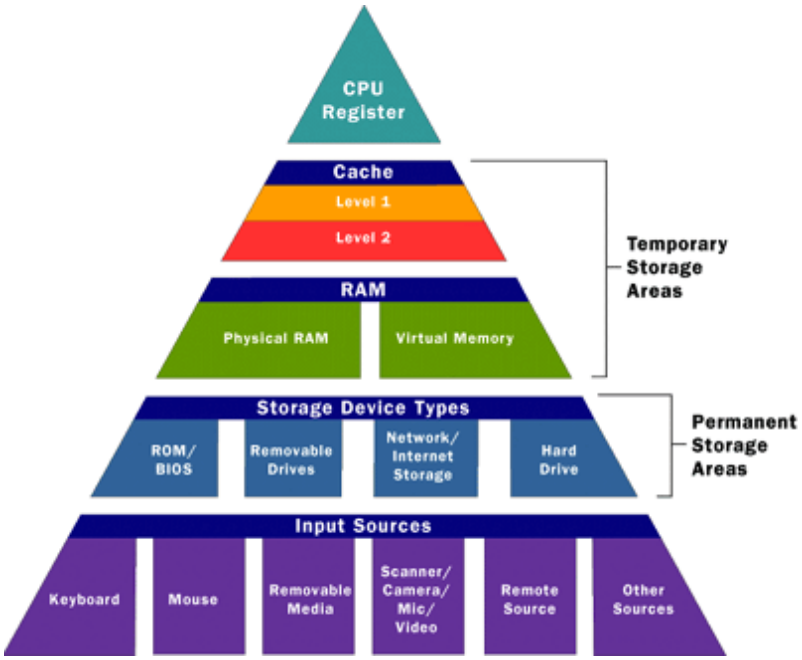

Figure 8. Cache and Registers of personal computer [12, p. 9]

About each desktop PC and server being used today contains one or more hard–plate drives. Each centralized computer and supercomputer is typically associated with several them. You can even discover VCR–sort gadgets and camcorders that utilization hard plates rather than tape. [12, p. 28] There are a lot of devices around us. It is always difficult to understand does particular device contain hard drive or memory that can be copied.

These billions of hard–plates do one thing admirably – they store changing computerized data in a moderately perpetual structure. They give PCs the capacity to remember things when electrical power is lost. [12, p. 28] There is an expanding pattern to firmware devices and all the more regularly a small units taking a shot at the field of IT crime scene investigation. Best performing organizations will work and share skill everywhere throughout the world, shaping great practices in this way. A great case utilizing firmware equipment is physical write blocking device.

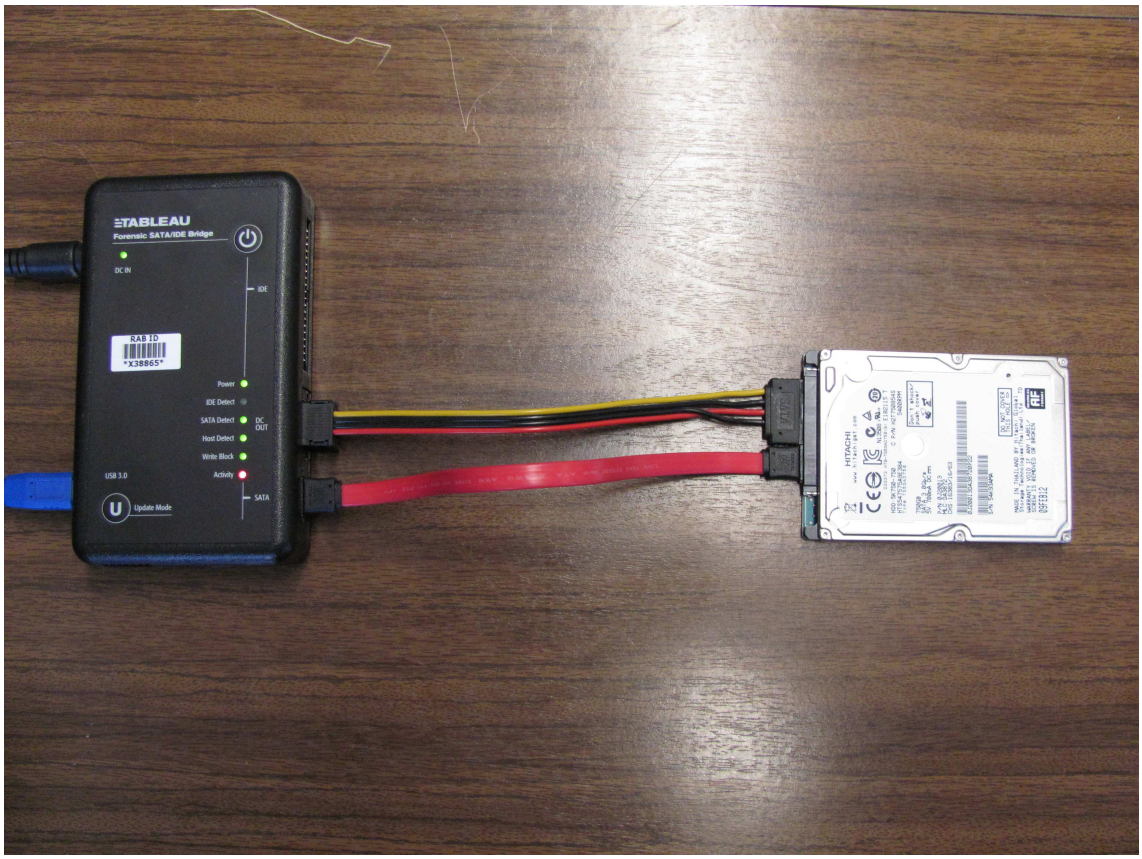

Figure 9. Write-block Tableau Forensic SATA/IDE Bridge Model T35u (by author)

Tableau Forensic SATA/IDE Bridge Model T35u on the figure 9 is working together with Guidance Software PC exploration software Encase Forensic on the figure 10. True is that hardware write blocking devices can usually cooperate with various programs and are able to make indistinguishable duplicate from hard drive. Instead commercial Encase Forensic can be used Accessdata FTK imager. It is best practice and imperative to use for IT scientific examination methods just lawful, legitimate hard– and software from validated sources. Author will bolster this thought since it is moral and IT forensic inspector cannot demean act like a criminal.

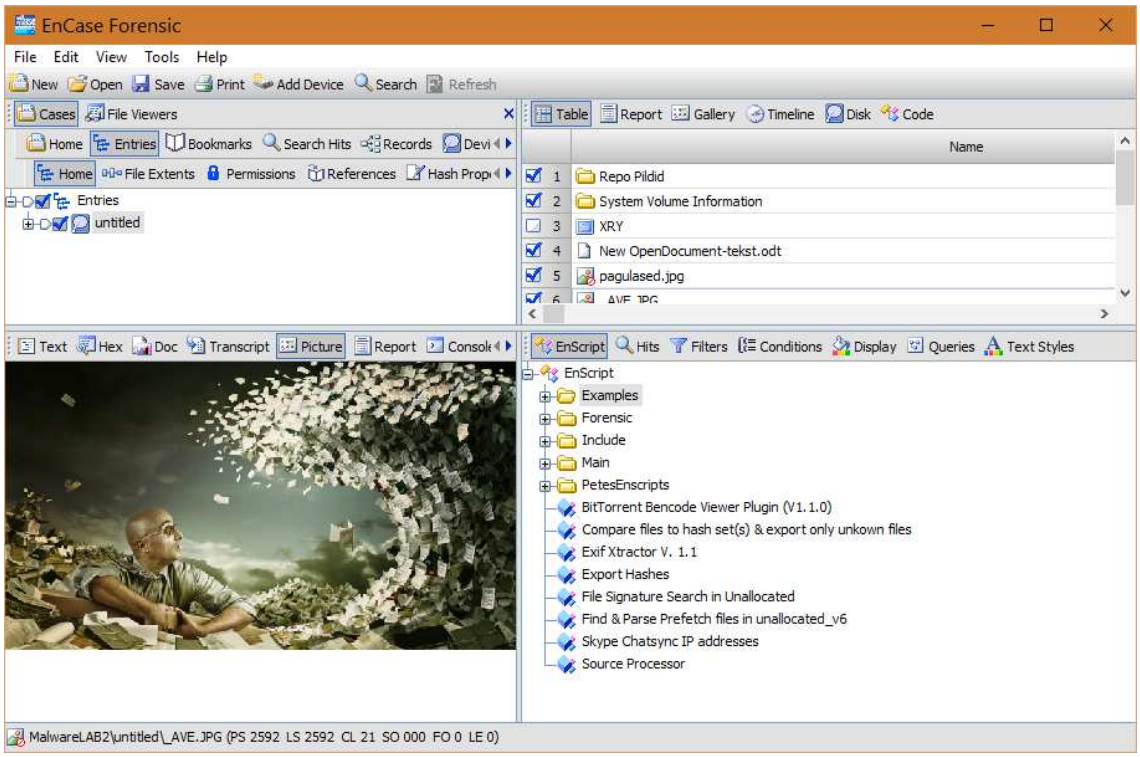

Figure 10. Encase Forensic program view (picture from https://insdrcdn.com/media/attachments/2/d9/1103cad92.jpg)

Tableau write–block device on the figure 9 and Encase computer forensic program on the figure 10 usually work in symbiosis. Computer examination is very important, however according to statistical analysis on Figure 18 there is a big future ahead for mobile forensic people, because for nowadays IT forensic examiners work more with mobile devices than they do computer forensic examinations. How to explore the mobile phone is set out below.

9. Mobile device examination

The accessibility of measurable programming devices for cell phones is impressively unique in relation to that of PCs. While PCs may vary from cell phones from an equipment and programming point of view, their usefulness has turned out to be progressively comparative. In spite of the fact that the majority of cell phone operating systems are open source (i.e., Android), highlight telephone OS's are regularly closed. Closed operating systems make translating their related file system and structure troublesome. Closed operating systems make their associated file system and structure rendering difficult. Numerous cell phones with the same operating system may likewise change broadly in their usage, bringing about a bunch of record framework and structure stages. These structure stage changes make significant difficulties for mobile forensic tool makers and analysts. Comprehension the different sorts of mobile acquisition tools and the information they are equipped for recovery is vital for a mobile forensic examiner. The grouping framework utilized as a part of this segment gives a structure to criminological analysts to look at the extraction techniques utilized by various tools to acquire information. The goal of the instrument characterization framework is to empower an examiner to effortlessly group and analyze the extraction technique for various tools. The tool grouping framework is shown in Figure 11 [22]. As the pyramid is crossed from the base, Level 1, to the top, Level 5, the strategies required in acquisition turn out to be more specialized, intrusive, tedious, and costly. [21, p. 15]

Level 1, Manual Extraction techniques include recording data raised on a cell phone screen while utilizing the UI. Level 2, Logical Extraction strategies are utilized at most and are somewhat specialized, requiring novice level preparing. Strategies for stages 3 to 5 involve extracting and rewriting a duplicate or image of a physical store (e.g., a memory chip), contrasted with the logical acquisitions utilized at level 2 include catching a duplicate of logical storage objects (e.g., catalogs and documents) that live on a logical store (e.g., a file system partition). Level 3, Hex Dumping/JTAG Extraction techniques, involve playing out a "physical acquisition" of cell phone memory in circumstance and require very good preparing. Level 4 Chip–Off strategies include the physical expulsion of memory from a cell phone to extract information, requiring leading–edge preparing in electronic designing and great knowledge of file system artifacts. [21, pp. 15–16]

Figure 11. Sam Brothers cellular phone tool levelling pyramid [22]

Level 5, Micro Read techniques include the utilization of a powerful magnifying microscope to see the physical condition of gates. Level 5 techniques are the most intrusive, refined, specialized, costly, and tedious of the considerable number of methods. [21, pp. 15–16]

There are advantages and disadvantages to performing extraction types at every layer. For instance, hex dumping permits erased objects and any information remainders present to be explored (e.g., in unallocated memory or file system space), which generally would be out of reach using logical acquisition techniques. In any case, the extracted gadget images require parsing, unscrambling and translating. Logical acquisition techniques, however more restricted than Hex Dumping/JTAG strategies, have the favorable position in that the system information structures are at a higher level of abstraction and are ordinarily simpler for an instrument to extract and render. However, the extracted device images require parsing, decryption and decoding. Logical acquisition methods, though more limited than Hex Dumping/JTAG methods, have the advantage in that the system data structures are at a higher level of abstraction and are normally easier for a tool to make excerpt and render. These distinctions are because, of the basic refinement between memory as seen by a process through the operating system aptitude (i.e., a consistent perspective), versus memory as found in crude structure by the processor or another hardware parts (i.e., a physical perspective). [21 p. 16]

Based upon a wide assortment of circumstances (e.g., type of information required, time accessible, priority, accessible tools, and so forth.), an inspector may choose a particular stage to start their examination. It is essential to note that once a level is utilized, other exchange levels may not be conceivable. For instance, after using chip–off (level 4) method lower level methods for device just may not be physically feasible. Forensic analysts ought to know about such effects and perform the suitable level of extraction proportionate with their preparation and experience. [21 p. 16]

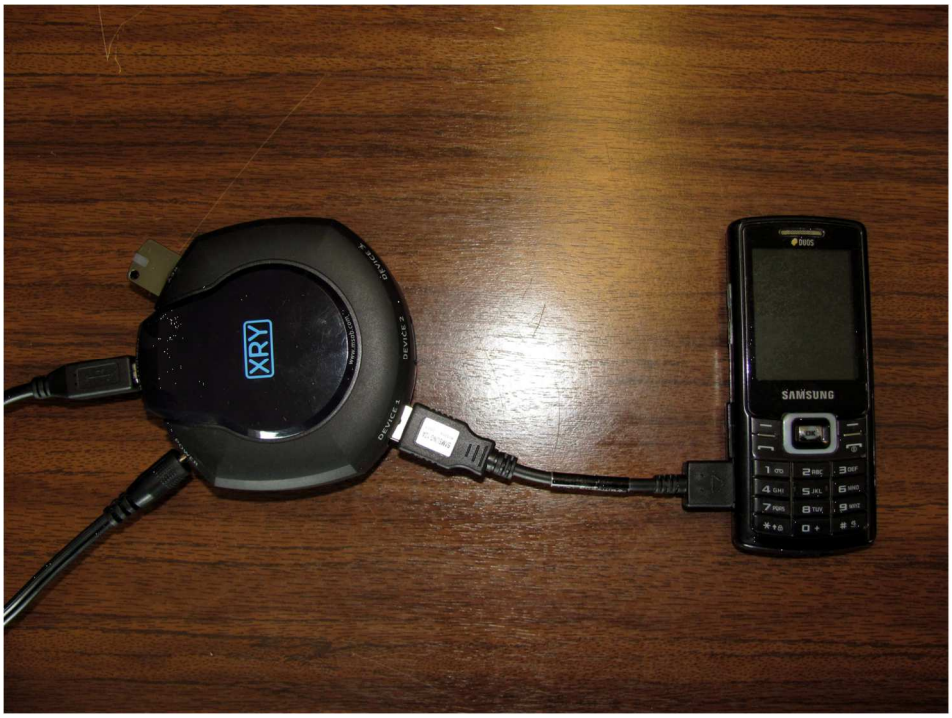

Figure 12. Samsung Duos cellphone connected Micro Systemation XRY tool (by author)

With every approach, information might be completely exterminated or changed if a given device or technique is not used legitimate. The danger of modification and annihilation increments in couple with the stages. Hence, legitimate preparing and tutoring is basic in getting the most considerable achievement rate for information extraction and investigation of the information contained inside cell phones. [21 p. 16] Cell phone information extraction and investigation amid examination is possible with various instruments figure 12 indicate how it's done with Micro Systemation XRY tool.

9.1 Manual extraction

It is the simplest and understandable method of analysis for examiner. If the phone has three digits and two records it is not hard to write these down. A manual observation strategy includes seeing the information content on a cell phone. The substance showed on the LCD screen requires the hand control of the knobs, console or touchscreen to see the substance of the cell phone. Data found might be recorded utilizing an outside photo or video camera. At this level, it is difficult to recoup already erased data. A few devices have been created to furnish the forensic specialist with the capacity to report and sort the data recorded more rapidly. All things considered, if there is a lot of information to be caught, a manual extraction can be exceptionally tedious and the information in the device might be unintentionally changed, erased or overwritten as an aftereffect of the examination. Manual extractions turn out to be progressively troublesome and maybe unachievable while experiencing a broken/missing LCD screen or a harmed/missing console interface. Extra difficulties happen when the device is arranged to show a dialect obscure to the examiner (e.g., Russian, Chinese), this may bring about trouble in effective menu route. [21 p. 17] Linguistic problems can defeat analysis.

9.2 Logical extraction

Availability between a cell phone and the investigation workstation is accomplished with an association utilizing either a wired (e.g., USB or RS–232) or radio (e.g., Wi–Fi, Bluetooth or IrDA) communication. The analyst ought to know about the issues related while selecting a particular network connection technique, as various communication sorts and related conventions may bring about information being altered (e.g., unread SMS) or distinctive sums or sorts of information being extricated. Logical extraction devices start by sending a progression of orders over the set up interface from the PC to the cell phone. The cell phone reacts based upon the summon demand. The reaction (cell phone information) is sent back to the workstation and exhibited to the investigation inspector for reporting purposes. Logical extraction tools begin by sending a series of commands over the established interface from the computer to the mobile device. The mobile device responds based upon the command request. The response (mobile device data) is sent back to the workstation and presented to the forensics examiner for describing purposes to fulfill report. [21 p. 17]

Hex Dumping and JTAG–Hex Dumping and Joint Test Action Group (JTAG) extraction techniques manage the cost of the legal inspector more straightforward access to the raw data saved in flash disk. One test with these extraction techniques is the capacity of an offered instrument to parse and decipher the captured information. [21 pp. 17–18]

Giving the legal analyst a consistent perspective of the file system, and writing about other information leftovers outside the file system that might be available for view are demanding. For instance, all information contained inside a given flash memory chip may not be obtained, a lot of tools, for example, flasher boxes, may just have the capacity to extract particular segments of memory [23]. Techniques utilized at this level require connection (e.g., cable or Wi–Fi) between the cell phone and the research workstation. [21 pp. 17–18]

9.3 Hex Dumping

This strategy is the all the more ordinarily utilized technique by devices at this level. This includes transferring an altered boot loader into a secured range of memory (e.g., RAM) in the gadget. This transfer procedure is proficient by interfacing the cell phone's information port to a flasher box and the flasher box is connected with the research workstation. Different order–requests is sent from the flasher box to the cell phone to place it in a diagnostic mode. Once in indicative mode, the flasher box catches all (or areas) of flash memory and sends it into the research workstation over the same connection utilized for the transfer. [21 p. 18]

Some flasher boxes work along these lines or they may utilize a restrictive interface for memory extractions. Uncommon cases exist where extractions can be proficient utilizing Wi–Fi (i.e., early Jonathan Zdziarski (JZ) Methods) [24]. [21 p. 18] Hex dump is a dump of the data in hexadecimal format. It is a binary information stream where the substance of that stream is possible to observe as the hexadecimal values.

9.4 Joint test action group

Many makers bolster the JTAG standard, which characterizes a typical test interface for processor, memory, and other semiconductor chips. Forensic examiners can connect with a JTAG – consistent segment by using unique reason standalone software programmer gadgets to test characterized test dots [25]. The JTAG testing unit can be utilized to demand memory addresses from the JTAG – corresponding segment and accept the reaction for storage and transfer [26]. [21 p. 18]

JTAG allow forensic masters to have another chance for imaging gadgets that are bolted or gadgets that may have minor harm and can't be appropriately interfaced any other way. This technique includes joining a wire (or wiring tackle) from a workstation to the cell phone's JTAG interface and connect memory through the gadget's micro–process or to create an image [23]. JTAG extractions contrast fundamentally from Hex Dumping because it is obtrusive and as entrance to the connections demand that the investigator disassembling a few of a mobile phone to acquire access to set up the wiring communication interface. [21 p. 18]

Flasher boxes are little gadgets initially outlined with the plan for administration or update cell phones. Copying a physical device as often as possible require the utilization of a flasher box to simplify the mining of information from a cell phone. The flasher box can help the inspector by connecting research computer with the cell phone utilizing diagnostics to contact with the memory chip. This connection may use the cell phone's operating system or may move around it inside and out and convey straightforwardly to the chip [27]. [21 p. 18]

Flasher boxes are often equipped with special programs to simplify the information mining process working in conjunction with the research computer. A lot of flasher box programming bundles give the additional usefulness of retrieval passwords from cell phone memory or some configuration files. Despite the fact that data obtaining techniques contrast between flasher boxes, a general procedure is utilized [23]. [21 p. 18]

Restrictions on the utilization of flasher boxes are as follows:

- Much of the time, a cell phone is required to be started again to force the extraction procedure; it may need authentication components initiate avoiding further investigation. [21 p. 19]
- Many flasher boxes recoup the information only in a scrambled configuration and demand the inspector to either utilize the product given by the flasher box maker to decode the information or may require a reversible design of the information's encryption plan by the examiner. [21 p. 19]
- Numerous telephone models don't leave a possibility of making identical copy of the whole memory range from inside a cell phone. It may happen that certain areas might be accessible for certain cell phones. [21 p. 19]
- The flasher box administration software frequently has a lots of knobs that are called with almost indistinguishable names. This perplexity may effectively even lead to a skillful analyst being misguided to press the wrong button, deleting the substance of the cell phone as opposed to dumping the memory. [21 p. 19]
- Absence of documentation on the utilization of the flasher box instruments is normal. Extraction strategies are regularly distributed on forums upheld by the seller and directed by more prepared clients. Alerts ought to be accepted when guidance is given, as not all the data gave is always right. [21 p. 19]
- Forensic purpose: Almost all flasher boxes were not outlined with a forensic purpose as originally planned reason. Inspectors must be knowledgeable about the utilization of flasher boxes and ought to comprehend the best possible way to utilize and understand behavior of flasher boxes. [21 p. 19]
- In spite of these restrictions, utilization of a flasher box is a feasible alternative for some crime scene investigation cases. Legitimate preparing, knowledge and downplaying of how the devices function after all are the main access to great achievement. [21 p. 19]

An extensive variety of high–tech competence and legitimate preparing is required for extricating and dissecting binary images with these techniques, including finding and interfacing with JTAG ports, making boot loaders and fix up the file systems. [21 p. 19]

9.5 Chip–Off

Chip–Off techniques allude to the obtaining of information entirely from a cell phone's flash memory. This extraction method demands the complete physical removal of the flash memory from circuit board. Chip–Off gives analysts the capacity to make a binary image of the detached chip. Keeping in mind the end goal to give the inspector information in a contiguous binary format file, the wear–leveling algorithm must be reverse engineered. Once finished, the binary image can be examined. This kind of securing is most firmly similar with physical imaging a hard disk drive as in ingrained digital legal sciences. Broad preparing is required so as to effectively perform data mining at this level. Chip–Off extractions are testing in view of a wide assortment of chip sorts, a horde of raw information formats, and the danger of bringing on physical harm to the chip amid the removal procedure. Because of the great complexities identified with Chip–Off method, JTAG extraction is more regular. [21 p. 19]

9.6 Micro Read

A micro read includes recording the physical perception of the gates on a NAND or NOR chip with the utilization of an electron microscope. Because of the amazing amount of high–tech skills and resources included when executing a Micro Read, this level of acquisition just must be endeavored exclusively for prominent cases proportionate to a national security emergency after all other data obtaining strategies have been depleted. Prosperous data obtaining at this level would require a group of specialists, legitimate hardware, and a lot of time and very good understanding of the relevant and proprietary data that is needed. [21 pp. 19–20]

10. Evaluation

Hypotheses used in a wide variety of statistical criteria. Experiments with the choice of the problem are based on the description and characterization of the problem. The hypotheses on the statistical verification concluded that the null hypothesis about setting up 40 hour's limit per computer examination must be rejected. Statistical data show that giving basic framework in electronic evidence examination it is possible to make analysis faster.

Research conducted on IT – Forensic investigators work reports that are collected on month basis during the period 2009 – 2016. First examiner using MS Access program described above other two examiners using their own unique approaches. Represented data cover years 2014–2016 because this period of time is most reliable that then was a certain human resources stability in West prefecture cybercrime unit. Figure 14 show distribution of working time hours during 2014 – 2016. Speeding confirmation is shown on Figure 15 there can be conclude that first examiner will handle situation under control using special tool. There is slight growth in working time hours over the years and that is interesting phenomena for future research. Comparison of working time hours confirm a stable period on Figure 17. By stability, the author means a situation where experts can calmly do their job to get maximum in their results. 841 electronic evidence examinations done during the selected period. Figure 16 will show how much devices was examined by examiner total during the selected period. Digital investigation unit managing instructions give an average time frame for the complete forensic investigation of an estimated time–line 216 hours [28, p. 28]. So statistical analysis and time analysis show that every examiner in West prefecture LAB is a real IT Forensic professional, there is no question about it. However, there is a lack of categorization data because some cases are more difficult than other cases and there are no notes about it in the collected research data. It might be a challenge how to determine a case difficulty level. Author proposes here to select data by 3 level system to low, medium and high by importance of the case. Because it has not been done before it might be difficult to introduce without management support.

11. Conclusion, recommendations and future research

The idea that giving basic framework in electronic evidence examination we can speed up the execution time of process analysis is correct. However, it is sometimes up to the forensic examiner how to organize the job. Recommendation here is that manager need to know what examiner do and how much time is taking certain procedure. Examiners who have organized work methods will tend to work faster. In the longer perspective new examiners once they have become familiar with their jobs will also increase their efficiency in analyzing electronic evidence. During the work the Microsoft Access application was almost developed, that definitely helps an expert to collect observation data. However, it need further development. Suggestion in that development can hopefully move to the direction multi user solution basing on web or cloud technology. Purpose for creating the simple database model was to make reporting quicker and as statistic evaluation shows, it was a good idea. It is clearly another interesting issue out of scope of this work to research how to speed up skilled digital forensic examiners work–flow with already working existent framework. Light growth working time hours over the years might be interesting phenomena for future research.

In the second research discovered that second examiner is trying to bend statistics. Without special tool 10 pages and more long evidence examination protocol take a lot longer to write. Setting up 40–hours limit for creating evidence examination protocol is not appropriate value there is no real ground for that recommendation. 216–hours limit [28, p. 28] is more close to the reality. Author suspect that there is may be connection between Moore's law and examination time growth, because it sounds as a logical conclusion and could be subject for future research.

There is another interesting finding from figure 18 that examiners struggle most of the time with mobile devices instead of computer forensic issues. The problem definitely needs further attention because there are different routines for computer forensic specialists and mobile forensic specialists.

Giving basic framework to electronic evidence examination it is possible to speed up the execution time of the analysis work–flow. Quantitative and qualitative analysis confirm it. Outcomes of usefulness, satisfaction, and ease of use test outcome demonstrate that the subject is important and fascinating to the examiners.

12. References

[1] **Riigikogu**, "Act – Code of Criminal Procedure," in *Riigi Teataja*, 2013. [Online]. Available: https://www.riigiteataja.ee/akt/12849731. Accessed: Apr. 7, 2016.

[2] **Riigikogu**, "Act – Code of Criminal Procedure English translation," in *Riigi Teataja*, 2013. [Online]. Available: Apr. 7, 2016. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/527012016001/consolide. Accessed: Apr. 7, 2016.

[3] **J. I. James, P. Gladyshev**, Digital Forensic Investigation Research Group, and University College Dublin, "Cornell University Library," in *Challenges with Automation in Digital Forensic Investigations*, 2013. [Online]. Available: http://arxiv.org/pdf/1303.4498.pdf. Accessed: Apr. 7, 2016.

[4] **P. Lahesoo**, "Personal Computer as electronic evidence by Estonian law," Research paper, Tallinn, 2016.

[5] **Guidance Software**, "Endpoint data security, eDiscovery, forensics," 1997. [Online]. Available: https://www.guidancesoftware.com/. Accessed: Apr. 7, 2016.

[6] **AccessData**, "E–discovery & computer forensics," AccessData, 2010. [Online]. Available: http://accessdata.com/. Accessed: Apr. 7, 2016.

[7] **B. Carrier**, "The sleuth kit (TSK) & autopsy: Open source digital forensics tools," in *Autopsy*, 2003. [Online]. Available: http://www.sleuthkit.org. Accessed: Apr. 7, 2016.

[8] **Y. Shu, J. James, and P. Gladyshev**, "A CONSISTENCY STUDY OF THE WINDOWS REGISTRY," in *Advances in Digital Forensics VI*, 2010. [Online]. Available: http://opendl.ifip–tc6.org/db/conf/ifip11–9/df2010/ZhuJG10.pdf. Accessed: Apr. 7, 2016.

[9] **AS Andmevara**, "Public information act," in *Riigi Teataja*, 2010. [Online]. Available: https://www.riigiteataja.ee/en/eli/514112013001/consolide. Accessed: Apr. 7, 2016.

[10] **F. Cohen**, "Digital Forensic Evidence Examination," in *fredcohen.net*, 4th Edition ed., 2012. [Online]. Available: http://www.fredcohen.net/Books/2013–DFE– Examination.pdf. Accessed: Apr. 7, 2016.

[11] **O. Olt**, "Sisekaitseakadeemia," (Kriminalistika Ekspertiisid), Tallinn: Paar OÜ, 2013, pp. 387–400. [Online]. Available: http://www.sisekaitse.ee/public/kirjastus/ekspertiisid_sisu_veebi.pdf. Accessed: Mar. 30, 2016.

[12] **Homeland Security**, *Basic Investigation of Computers and Electronic Crimes program*. Budapest: Homeland Security, 2005.

[13] **T. London**, "Infotehnoloogiliste ekspertiiside uuringud," 2008. [Online]. Available: http://www.slideshare.net/krebalo/magistritoo–terry–london–08092008. Accessed: Mar. 30, 2016.

[14] **A. V. Aho and J. D. Ullman**, "Aho/Ullman foundations of computer science," in *Stanford InfoLab*, 1994. [Online]. Available: http://infolab.stanford.edu/~ullman/focs.html. Accessed: Apr. 12, 2016.

[15] **R. Fidel and A. M. Pejtersen**, "From information behaviour research to the design of information systems: The cognitive work analysis framework," in *www.informationr.net*, Professor T.D. Wilson, 2004. [Online]. Available: http://www.informationr.net/ir/10–1 /paper210.html. Accessed: Apr. 13, 2016.

[16] **C. W. Churchman**, *The systems approach.* New York: Dell, 1979.

[17] **D. Johnstone, M. Bonner, and M. Tate**, "Bringing human information behaviour into information systems research: An application of systems modelling," in www.informationr.net, Professor T.D. Wilson, 2004. [Online]. Available: http://www.informationr.net/ir/9–4/paper191.html. Accessed: Apr. 13, 2016.

[18] **Decision Group Inc.**, "Network packet forensics analysis training course," in *Total Solutions for Computer Network Forensic*, 2015. [Online]. Available: http://www.edecision4u.com/network–forensics/NPFAT/npfat.html. Accessed: Apr. 13, 2016.

[19] **Estonian Internal Security Service**, "Annual review 2015," in KAPO, 2016. [Online]. Available: https://www.kapo.ee/sites/default/files/public/content_page/AnnualReview2015.pdf. Accessed: Apr. 13, 2016.

[20] **Politsei– ja Piirivalveamet**, "Politsei– ja Piirivalveameti struktuur," in *PPA*, 2016. [Online]. Available: https://www.politsei.ee/et/organisatsioon/politsei–ja–piirivalveamet/struktuur/. Accessed: Apr. 13, 2016.

[21] **R. Ayers, S. Brothers, W. Jansen**, National Institute of Standards and Technology, and U.S. Department of Commerce, "NIST Special Publication 800 – 101 Revision 1," in *National Institute of Standards and Technology*, 2014. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800–101r1.pdf. Accessed: Apr. 14, 2016.

[22] **Sam Brothers**, How Cell Phone "Forensic" Tools Actually Work – Cell Phone Tool Leveling System, Mobile Forensic World, Chicago, IL, March, 2008.

[23] **Marcel Breeuwsma, Martien de Jongh, Coert Klaver, Ronald van der Knijff, Mark Roeloffs**, Forensic Data Recovery from Flash Memory, Small Scale Digital Device Forensics Journal, Vol. 1, No. 1. [Online]. Available: http://www.ssddfj.org/papers/ssddfj_v1_1_breeuwsma_et_al.pdf. Accessed: Jun. 01, 2007.

[24] **J. Zdziarski**, "iOS Forensic Investigative Methods," in *TECHNICAL DRAFT*, 2012. [Online]. Available: http://www.zdziarski.com/blog/wp–content/uploads/2013/05/iOS– Forensic–Investigative–Methods.pdf. Accessed: Apr. 16, 2016.

[25] **Svein Willassen**, Forensic Analysis of Mobile Phone Internal Memory, IFIP WG 11.9 International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13 – 16, 2005, in Advances in Digital Forensics, Vol. 194, **Pollitt, M.; Shenoi, S.** (Eds.), XVIII, 313 p., 2006.

[26] **M. Breeuwsma**, *Forensic Imaging of Embedded Systems using JTAG (boundary – scan), Digital Investigation*, Netherlands Forensic Institute – NFI, Ed., Volume 3,

Issue 1 ed. The Hague: The International Journal of Digital Forensics & Incident Response, 2006, pp. 32 – 42.

[27] **K. Jonkers**, "The forensic use of mobile phone flasher boxes5, digital investigation 6," 2010, pp. 168 – 178, [Online]. Available: http://www.sciencedirect.com. Accessed: Sep. 09, 2013.

[28] **2CENTRE** Cybercrime Centres of Excellence Network, **R. Genoe, and J. McGourty**, MANAGING A DIGITAL INVESTIGATION UNIT A Handbook for Senior Law Enforcement Officers, 1–st Edition ed. Dublin: University College Dublin Centre for Cybersecurity & Cybercrime Investigation, 2013.

[29] **D. M. Amari**, "CALEA Update Magazine Issue 108," in *Creating a Police Quality Management System*, 2011. [Online]. Available: http://www.calea.org/calea–update– magazine/issue–108/creating–police–quality–management–system–how–surprise–police– depart. Accessed: Apr. 23, 2016.

[30] **The International Organization for Standardization**, "ISO," in *Quality management principles*, 2015. [Online]. Available: http://www.iso.org/iso/pub100080.pdf. Accessed: Apr. 23, 2016.

[31] ***CV Keskus***, 2014. [Online]. Available: http://www.cvkeskus.ee/325614. Accessed: May 30, 2016.

[32] **CV–Online** 1996–2016, "Tööpakkumised," in *CV–Online*, 2016. [Online]. Available: http://www.cv.ee/toopakkumine/politsei–ja–piirivalveamet/kriminaalteabeteenistuse– vanemspetsialist–f3107382.html. Accessed: Jun. 29, 2016.

[33] **K. Kent, S. Chevalier, T. Grance, and H. Dang**, "Guide to Integrating Forensic Techniques into Incident Response," in *Recommendations of the National Institute of Standards and Technology*, 2015. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800–86.pdf. Accessed: Sep. 19, 2016.

[34] **European Comission**, "European Anti–Fraud Office," in *Guidelines on Digital Forensic Procedures for OLAF Staff*, 2016. [Online]. Available: https://ec.europa.eu/anti– fraud/sites/antifraud/files/guidelines_en.pdf. Accessed: Oct. 12, 2016.

[35] **K. Kent, S. Chevalier, T. Grance, H. Dang, and National Institute of Standards and Technoloy**, "Guide to Integrating Forensic Techniques into Incident Response," in *Recommendations of the National Institute of Standards and Technology*, 2006. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800–86.pdf. Accessed: Oct. 12, 2016.

[36] **European Commission**, Basic Computer Forensic Examiner part 1, The International Association of Computer Investigative Specialists, Ed., BCFE 2015 ed. Zagreb: European Union Programme Hercule III, 2015.

[37] **European Commission**, Basic Computer Forensic Examiner part 3, The International Association of Computer Investigative Specialists, Ed., BCFE 2015 ed. Zagreb: European Union Programme Hercule III, 2015.

[38] **A. Lund**, "Measuring usability with the USE questionnaire," in ResearchGate, 2001. [Online]. Available: https://www.researchgate.net/publication/230786746. Accessed: Oct. 13, 2016.

[39] **J. Somer**, *Sündmuskoha vaatlus*, H. Lindmäe, Ed., õppevahend politseikoolile ed. Paikuse: Paikuse Politseikool, 1996.

[40] **B. Angerfelt**, "Examination and analysis report," 2005.

[41] **K. Meikas**, *INFOTEHNOLOOGIAEKSPERTIISIDE METOODIKA (KEKK'i näitel)*, K. Rava, Ed., Diplomitöö ed. TALLINN: TALLINNA TEHNIKAÜLIKOOL, 2006.

[42] **T. Reid and D. D. F. R. S. E**, *Essays on the Intellectual Powers of Man*, University of Glasgow, Ed., VOL. II. ed. Dublin: Printed for L. WHITE, No. 86, DAME–STREET., 1785.

Tables

Table 1. Examiner work–flow data 2014 –2016 (West prefecture)

	A	B	C	D	E
1	From	01.01.2014	Workdays/Holidays	698	24
2	To	06.10.2016	Examiner I	Examiner II	Examiner III
3	Computers	126	31	49	46
4	Copy made	104	24	58	22
5	Other Devices	310	54	134	122
6	Mobiles	405	141	249	15
7	Hours total	11310	2614	4966	3730
8	Percent normal worktime	67,51 %	46,81 %	88,93 %	66,80 %
9	Other technical job (hours)	632	182	188	261
10	Consulting (hours)	423	171	130	71
11	Other activities(hours)	3721	1243	1637	841
12	Hours total	4776	1596	1955	1173
13	Percent normal worktime	28,51 %	28,58 %	35,01 %	21,01 %

Table 2. Devices by years 2014 – 2016 comparison (West prefecture)

	A	B	C	D
1	Year	Computer	Mobile	Other
2	2014	51	154	115
3	2015	54	134	129
4	2016	21	117	66
5	Total:	**126**	**405**	**310**

Table 3. Examiner work–flow data 2016 (West prefecture)

	A	B	C	D	E
1	From	01.01.2016	Workdays/Holidays	195	5
2	To	06.10.2016	Examiner I	Examiner II	Examiner III
3	Computers	21	9	10	2
4	Copy made	18	8	9	1
5	Other Devices	66	11	33	22
6	Mobiles	117	31	86	0
7	Hours total	2298	649	1239	410
8	Percent normal worktime	49,10 %	41,60 %	79,42 %	26,28 %
9	Other technical job (hours)	144	43	99	2
10	Consulting (hours)	33	19	14	0
11	Other activities(hours)	670	26	360	284
12	Hours total	847	88	473	286
13	Percent normal worktime	18,10 %	5,64 %	30,32 %	18,33 %

Table 4. Examiner work–flow data 2015 (West prefecture)

	A	B	C	D	E
1	From	01.01.2015	Workdays/Holidays	252	9
2	To	31.12.2015	Examiner I	Examiner II	Examiner III
3	Computers	54	13	19	22
4	Copy made	38	11	18	9
5	Other Devices	129	21	48	60
6	Mobiles	134	40	91	3
7	Hours total	4631	995	1844	1792
8	Percent normal worktime	76,57 %	49,36 %	91,47 %	88,89 %
9	Other technical job (hours)	108	31	45	32
10	Consulting (hours)	49	28	21	0
11	Other activities(hours)	1306	557	672	77
12	Hours total	1463	616	738	109
13	Percent normal worktime	24,19 %	30,56 %	36,61 %	5,41 %

Table 5. Examiner work–flow data 2014 (West prefecture)

	A	B	C	D	E
1	From	01.01.2014	Workdays/Holidays	251	10
2	To	31.12.2014	Examiner I	Examiner II	Examiner III
3	Computers	51	9	20	22
4	Copy made	48	5	31	12
5	Other Devices	115	22	53	40
6	Mobiles	154	70	72	12
7	Hours total	4381	970	1883	1528
8	Percent normal worktime	72,73 %	48,31 %	93,77 %	76,10 %
9	Other technical job (hours)	380	108	44	227
10	Consulting (hours)	341	124	95	71
11	Other activities(hours)	1745	660	605	480
12	Hours total	2466	892	744	778
13	Percent normal worktime	40,94 %	44,42 %	37,05 %	38,75 %

Table 6. Examinations total by examiner 2014 – 2016 (by author)

	A	B	C	D
1	Total	Examiner I	Examiner II	Examiner III
2	841	226	432	183

Table 7. Descriptive statistics hours by examiner (by author)

	A	B	C	D
1	*Descriptive Statistics*			
2	*Hours*			
3	Variable name	Examiner I	Examiner II	Examiner III
4	Mean	959,74	165,55	561,39
5	Standard Error	404,95	22,12	79,60
6	Median	112	112	444
7	Mode	24	8	8
8	Standard Deviation	2254,65	154,86	539,89
9	Sample Variance	5083466,60	23981,88	291479,62
10	Kurtosis	6,43	–0,56	0,01
11	Skewness	2,77	0,84	0,75
12	Range	8328	488	2168
13	Minimum	8	8	8
14	Maximum	8336	496	2176
15	Sum	29752	8112	25824
16	Count	31	49	46

Table 8. z–Test three samples for means (by author)

	A	B	C	D
1	z–Test: Three Samples for Means			
2		Examiner I	Examiner II	Examiner III
3		*Hours*		
4	Mean	959,7419355	165,5510204	561,3913043
5	Known Variance	5083446,623	23981,6196	291481,2121
6	Observations	31	49	46
7	Hypothesized Mean	40	40	40
8	z	2,271264441	5,675171987	6,549941421
9	P(Z<=z) one–tail	0,011565487	6,927469265	2,877986738
10	z Critical one–tail	1,281551566	1,281551566	1,281551566
11	P(Z<=z) two–tail	0,023130974	1,385493853	5,755973476
12	z Critical two–tail	1,644853627	1,644853627	1,644853627

Table 9. Examiner I six cases time analysis (by author)

	A	B	C	D	E
1	**Examiner I**	Begin time	End time	Workdays	Days
2	Laptop Lenovo T60	06.10.2016 13:00	24.10.2016 16:30	13 days	18 days, 3 hours, 30 minutes
3	Samsung NP–R509	06.10.2016 15:00	27.10.2016 12:15	16 days	20 days, 21 hours, 15 minutes
4	Desktop black	12.02.2016 9:00	23.02.2016 13:30	8 days	11 days, 4 hours, 30 minutes
5	Lenovo Yoga	19.04.2016 8:00	11.05.2016 16:30	17 days	22 days, 8 hours, 30 minutes
6	X–Box 360	20.05.2015 10:00	22.05.2015 16:30	3 days	2 days, 6 hours, 30 minutes
7	Acer Aspire	10.08.2015 10:00	22.12.2015 16:30	97 days	134 days, 6 hours, 30 minutes
8			**Total:**	**154 days**	**156 days, 5 hours, 30 minutes**

Table 10. Examiner II six cases time analysis (by author)

	A	B	C	D	E
1	**Examiner II**	Begin time	End time	Workdays	Days
2	Desktop unknown	12.02.2016 9:00	24.03.2016 14:00	30 days	41 days, 5 hours
3	Laptop HP	01.03.2016 11:45	15.03.2016 13:30	11 days	14 days, 1 hour, 45 minutes
4	Dell Latitude D430	14.06.2016 11:00	30.06.2016 9:30	13 days	15 days, 22 hours, 30 minutes
5	HP Pavilion	09.12.2014 16:00	06.02.2015 13:40	44 days	58 days, 21 hours, 40 minutes
6	Desktop ORDI	04.05.2015 15:00	20.05.2015 13:00	13 days	15 days, 22 hours
7	Toshiba Sattelite	09.12.2014 16:00	06.02.2015 11:30	44 days	58 days, 19 hours, 30 minutes
8			**Total:**	**155 days**	**158 days, 20 hours, 25 minutes**

Table 11. Examiner III six cases time analysis (by author)

	A	B	C	D	E
1	**Examiner III**	Begin time	End time	Workdays	Days
2	HP Compaq	15.07.2015 9:00	21.12.2015 10:00	114 days	159 days, 1 hour
3	Fujitsu Siemens	31.03.2014 9:30	27.06.2014 12:00	65 days	88 days, 2 hours, 30 minutes
4	Ordi tower	22.07.2014 8:30	28.07.2014 16:15	5 days	6 days, 7 hours, 45 minutes
5	HP Compaq	14.04.2015 14:00	18.06.2015 12:00	48 days	64 days, 22 hours
6	HP Pavilion dv6500	15.01.2015 10:00	04.03.2015 13:00	35 days	48 days, 3 hours
7	HDD Seagate	17.09.2014 17:00	21.01.2015 15:00	91 days	125 days, 22 hours
8			**Total:**	**358 days**	**360 days, 10 hours, 15 minutes**

Table 12. Examination pages by six cases analysis of variance (by author)

Anova: Single Factor

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Examiner I	6	64	10,66666667	1,066666667
Examiner II	6	16	2,666666667	0,266666667
Examiner III	6	61	10,16666667	61,36666667

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P–value*	*F crit*
Between Groups	241	2	120,5	5,765550239	0,013884	3,68232
Within Groups	313,5	15	20,9			
Total	554,5	17				

Table 13. Six cases hours by examiner (by author)

	A	B	C
1	Hours		
2	Examiner I	Examiner II	Examiner III
3	107,5	245	913
4	165,25	89,75	522,5
5	68,5	126,5	47,75
6	144,5	373,66	406
7	30,5	126	283
8	782,5	371,5	750

Table 14. Six cases examination times analysis of variance (by author)

Anova: Single Factor

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Examiner I	6	1298,75	216,4583333	79309,51042
Examiner II	6	1332,41	222,0683333	16341,25802
Examiner III	6	2922,25	487,0416667	98604,56042

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P–value*	*F crit*
Between Groups	286915,3595	2	143457,6798	2,215501844	0,143539089	3,682320344
Within Groups	971276,6443	15	64751,77628			
Total	1258192,004	17				

Table 15. Measuring Usability with the USE Questionnaire analysis usefulness (by author)

USEFULNESS		DISAGREE	2	3	4	5	6	AGREE	N/A
1	It helps me be more effective.					1	2	1	1
2	It helps me be more productive.					2	2	1	
3	It is useful.						4	1	
4	It gives me more control over the activities in my life.					1	3	1	
5	It makes the things I want to accomplish easier to get done.					1	3	1	
6	*It saves me time when I use it.*						4	1	
7	*It meets my needs.*				1	2	1	1	
8	*It does everything I would expect it to do.*					3	1	1	

Table 16. Measuring Usability with the USE Questionnaire analysis ease of use (by author)

EASE OF USE		DISAGREE	2	3	4	5	6	AGREE	N/A
9	It is easy to use.				1		3	1	
10	It is simple to use.					1	3	1	
11	It is user friendly.					2	2	1	
12	It requires the fewest steps possible to accomplish what I want to do with it.					1	2	2	
13	*It is flexible.*					3	1	1	
14	*Using it is effortless.*				1	3		1	
15	*I can use it without written instructions.*					2	1	2	
16	*I don't notice any inconsistencies as I use it.*				1		3	1	
17	*Both occasional and regular users would like it.*					2	2	1	
18	*I can recover from mistakes quickly and easily.*					1	1	3	
19	*I can use it successfully every time.*					2	2	1	

Table 17. Measuring Usability with the USE Questionnaire analysis ease of learning (by author)

EASE OF LEARNING		DISAGREE	2	3	4	5	6	AGREE	N/A
20	I learned to use it quickly.						3	2	
21	I easily remember how to use it.					1	3	1	
22	It is easy to learn to use it.						4	1	
23	*I quickly became skillful with it.*						3	2	

Table 18. Measuring Usability with the USE Questionnaire analysis satisfaction (by author)

SATISFACTION		DISAGREE	2	3	4	5	6	AGREE	N/A
24	I am satisfied with it.					1	1	3	
25	I would recommend it to a friend.						4	1	
26	It is fun to use.						3	2	
27	It works the way I want it to work.					2	2	1	
28	It is wonderful.				1	1	2	1	
29	*I feel I need to have it.*					1	2	2	
30	*It is pleasant to use.*					1	1	3	

Figures

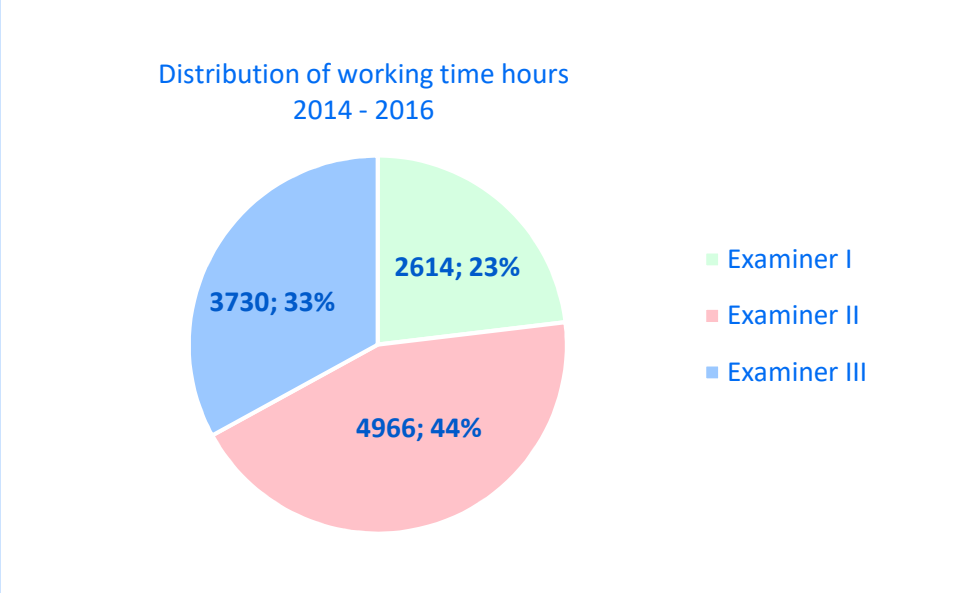

Figure 13. Distribution of working time hours 2014 – 2016

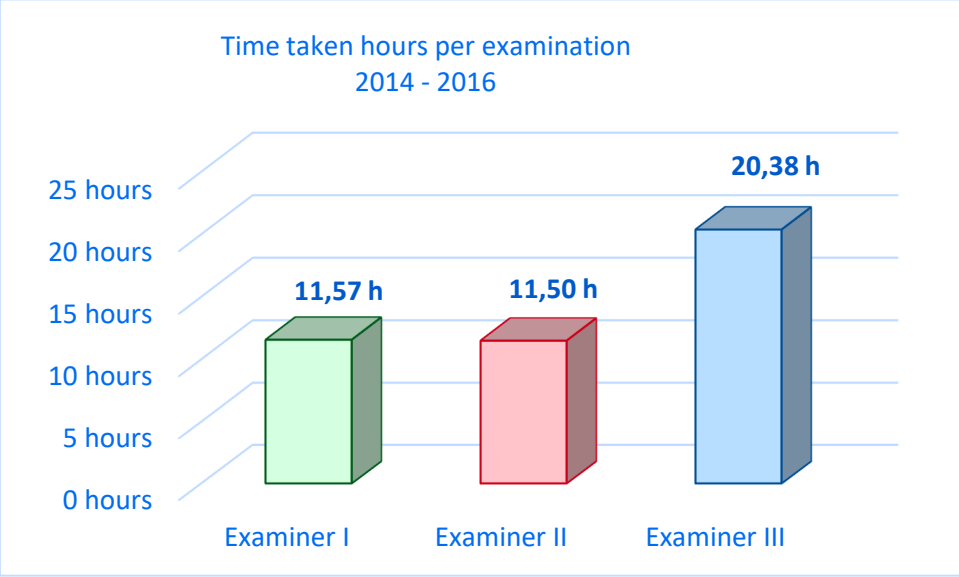

Figure 14. Time taken hours per examination 2014 – 2016

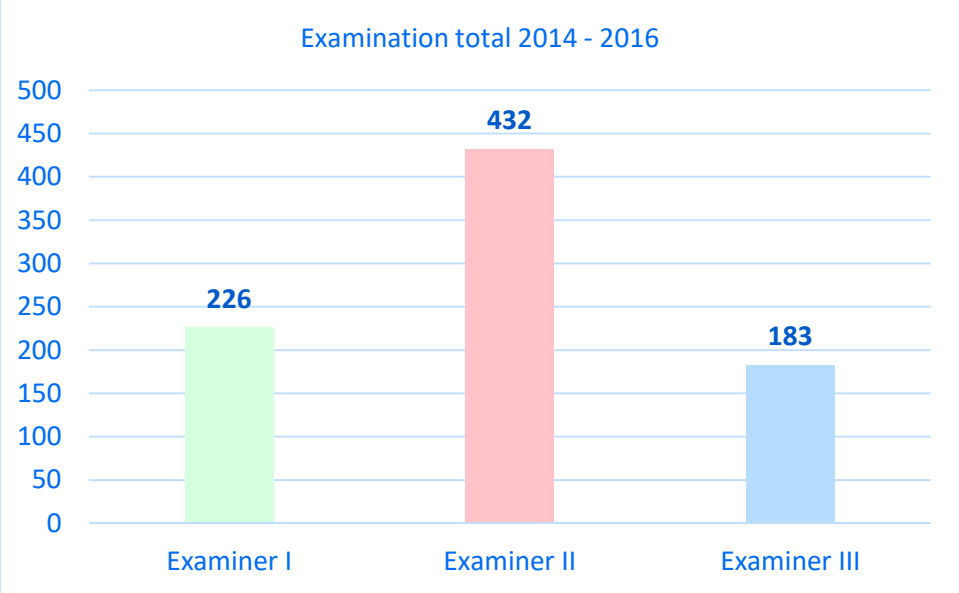

Figure 15. Examinations by examiner total during 2014 – 2016

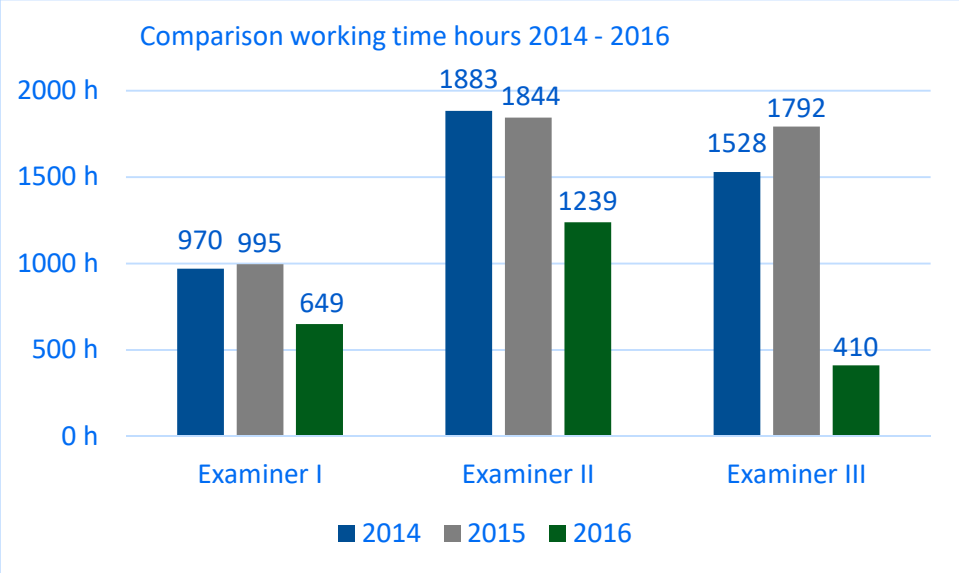

Figure 16. Comparison working time hours 2014 – 2016

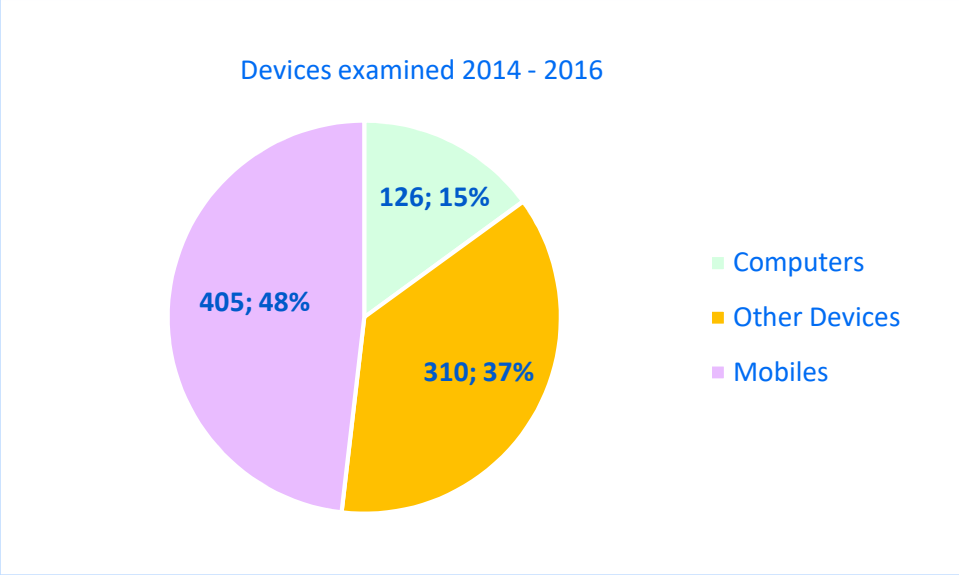

Figure 17. Examined devices 2014 – 2016

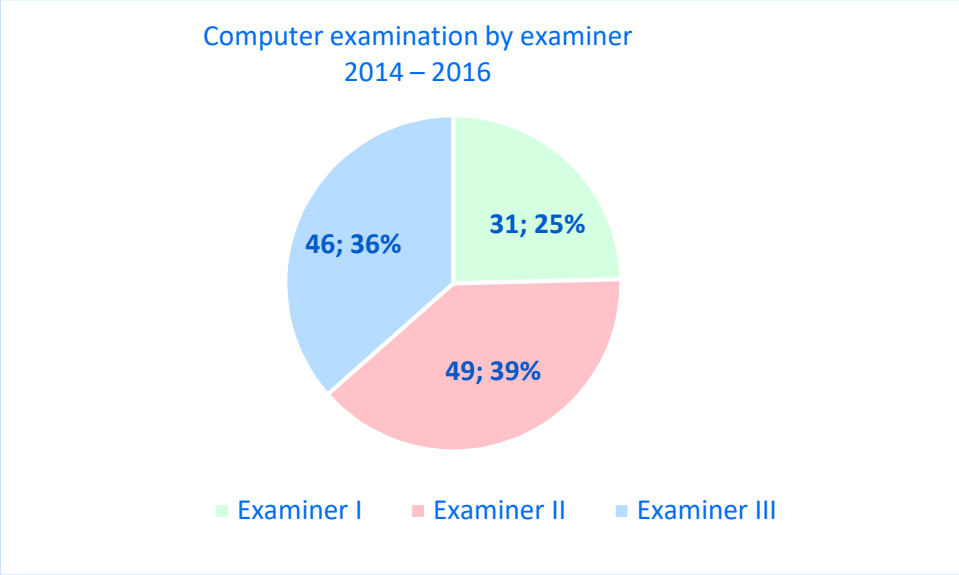

Figure 18. Computer examination by examiner 2014 – 2016

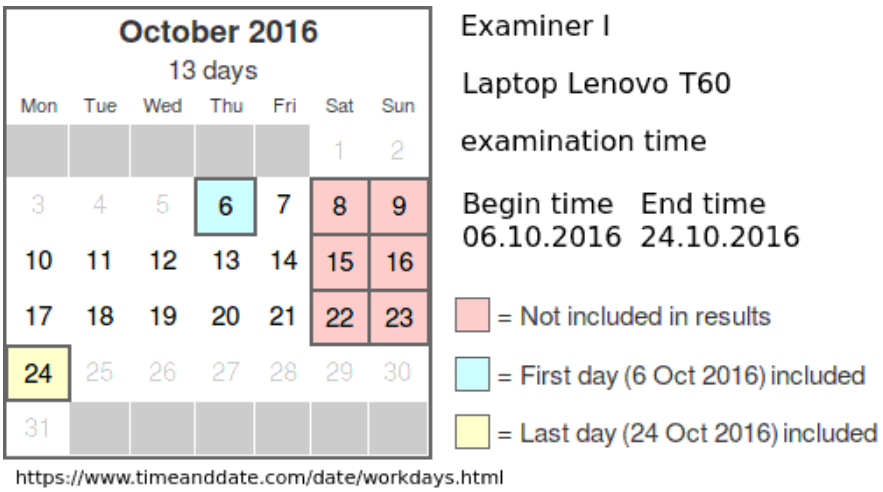

Figure 19. Examiner I time analysis example

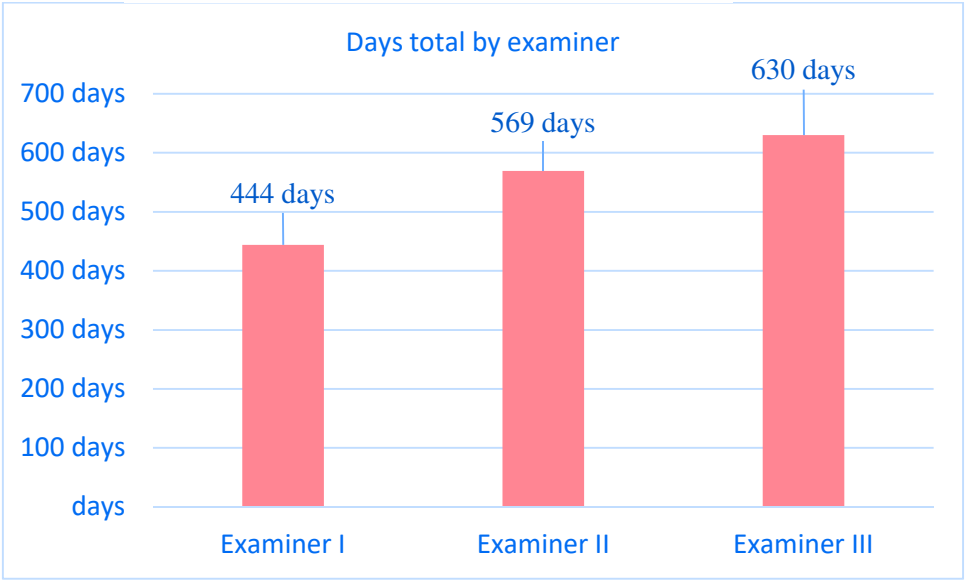

Figure 20. Six cases analysis days total by examiner

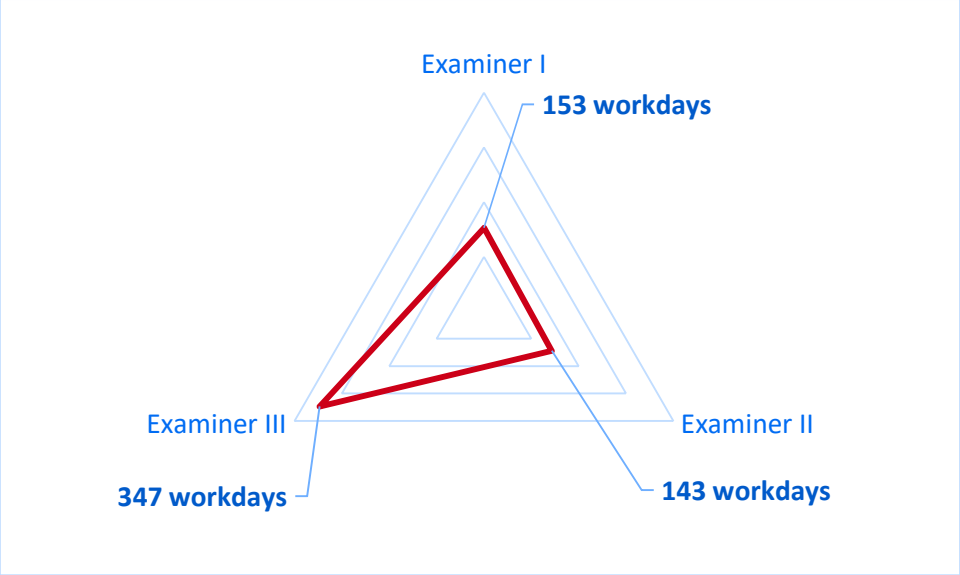

Figure 21. Six cases weakest link analysis

IV. License

Non–exclusive licence to reproduce thesis and make thesis public

I, **Priit Lahesoo**,

(*author's name*)

1. herewith grant the University of Tartu a free permit (non–exclusive licence) to:

   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

The electronic evidence examination reporting system by the example of West prefecture,

(title of thesis)

supervised by Truls Ringkjob, Raimundas Matulevičius

(supervisor's name)

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non–exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **06.01.2017**