universität wien

DISSERTATION

Titel der Dissertation

„Presentation & Argumentation Support for IT Forensics Case Preparation“

Verfasser

Mag. Maximilian Bielecki Bakk.

angestrebter akademischer Grad

Doktor der technischen Wissenschaften (Dr. techn.)

Wien, April 2014

Studienkennzahl lt. Studienblatt:	A 786 175
Dissertationsgebiet lt. Studienblatt:	Dr.-Studium der technischen Wissenschaften Wirtschaftsinformatik UG2002
Betreuerin / Betreuer:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

Abstract

This thesis discusses the development of a novel forensics support concept to automatically analyse malicious software and identify potential criminals. Furthermore it generates an automated argumentation strategy, which can be used within court cases. To evaluate the performance of this novel approach a prototype system has been developed and tested. The results and outcome thereof are discussed in detail within this research project.

This research study was conducted over 6 years with all discussed technologies constantly evolving. Although some technical solutions changed in the meantime, the basic fundamentals and ideas still remained valid. It is necessary to fully understand the basic technological concepts and ideas, which are necessary for a valid computer forensic investigation.

This research thesis is divided into four different core elements. First there is an extensive literature review that discusses novel computer forensic approaches and studies. The following chapter discusses in details the research methodology which was used to conduct this research project. This also includes the research idea, the research question and the research approach in more general. Another crucial part is the “Concept and Model” part which discusses the current situation that includes three different views (legal, organisational and technical), the defined requirements and the conceptual model itself. Another essential element of this research work is the technical implementation of the conceptual model which leads to the prototype development. This prototype was used for evaluating the research question in a more measurable way. This research thesis concludes with a theoretical case study and an extensive discussion of the gathered results and the outcome.

The results of this research project illustrate explicitly that there is urgent need for novel computer forensic approaches and concepts that can support and accelerate the investigative process.

Deutsche Zusammenfassung

Diese wissenschaftliche Arbeit diskutiert die Ansätze und Entwicklung eines neuartigen forensischen Konzeptes, für die automatisierte Analyse von Schadsoftware, umgangssprachlich genannt „Malware“ und die eindeutige Täteridentifikation. Zusätzlich generiert es eine automatisierte Argumentationsstrategie, welche in Gerichtsverhandlungen eingesetzt werden kann. Um die Leistung und Einsatzfähigkeit dieses Ansatzes wissenschaftlich evaluieren zu können, wurde ein technischer Prototyp entwickelt und ausgiebig getestet. Die Ergebnisse und daraus auffallenden Besonderheiten werden im Detail im weiteren Verlauf dieser wissenschaftlichen Dissertation diskutiert.

Dieses Forschungsprojekt wurde über einen Gesamtzeitraum von 6 Jahren betrieben, wodurch sich die teilweise eingesetzten Technologien und Ansätze mit der Zeit weiterentwickelt haben. Obwohl sich manche technische Lösungen im Laufe der Zeit verändert oder angepasst haben, blieb das Grundgerüst für die Forschungsarbeit die ganze Zeit überhin gültig. Diesbezüglich ist es unbedingt notwendig, die ganzen Grundtechnologien und Ansätze im Kern zu verstehen, die für eine erfolgreiche computerforensische Untersuchung erforderlich sind.

Diese wissenschaftliche Arbeit besteht aus vier Themenschwerpunkten. Zuerst erfolgt eine tiefergehende Literaturanalyse, in der aktuelle computerforensische Forschungsarbeiten im Detail vorgestellt werden. Der nächste Abschnitt beschreibt die Forschungsmethodik, die in diesem Projekt angewendet wurde. Diese beinhaltet die Forschungsidee, die zentralen Forschungsfragen und den generellen Forschungsansatz. Ein weiteres zentrales Thema dieser Arbeit ist der Abschnitt „Konzept und Modell“, in dem detailliert auf die Ausgangssituation, die Anforderungen und schlussendlich dem konzeptuellen Modell eingegangen wird. Der nächste Themenschwerpunkt dieser Arbeit befasst sich mit der technische Umsetzung und der Umwandlung des theoretischen Modells in einen einsetzbaren Prototypen, anhand dessen die allgemeine Evaluierung der Forschungsidee erfolgte. Abschließend wird noch

eine theoretische Fallstudie des Prototypens und eine ergiebige Analyse der erzielten Forschungsziele behandelt. Zusätzlich werden auch notwendige Einschränkungen diskutiert, die definiert werden mussten, damit das Forschungsprojekt überhaupt umgesetzt werden konnte.

Die Ergebnisse dieser wissenschaftlichen Arbeit verdeutlichen eindeutig den Bedarf an neuartigen computerforensischen Ansätzen und Lösungen, damit der investigative Prozess beschleunigt und unterstützt werden kann.

Acknowledgments

This research project is dedicated to my wife Anna, for her love, inspiration and never-ending support and encouragement to complete this thesis even during personally challenging times for us, when starting a family and building our careers.

I gratefully acknowledge the extensive support and assistance of my PhD supervisor, Univ.-Prof. Dipl.-Ing. Dr. Dr. Gerald Quirchmayr from the University of Vienna, Austria. Without his constant guidance and words of encouragement and support throughout my research this thesis would have never been finished.

I would also like to acknowledge the support and commitment of my family in particular my parents to help me finish this research project. All the never-ending discussions and ideas we had will always be remembered.

In addition I would like to thank all colleagues who I had the opportunity to meet during this research study. The list would be far too long to name everyone here but I am very thankful for all conversations, chats and discussions we had subjecting this project.

Finally, I would like to thank all reviewers from the following Boards and Committees:

- BILETA 2010, British & Irish Law, Education and Technology Association (Vienna, Austria, 2010)
- TRUSTBUS 2010, Conference on Trust, Privacy and Security in Digital Business (Bilbao, Spain, 2010)
- ARES 2010, The International Dependability Conference on Availability, Reliability and Security (Cracow, Poland, 2010)
- WDFIA 2009, International Annual Workshop on Digital Forensics & Incident Analysis (Athens, Greece, 2009)

- IPICS 2006, European Intensive Programme on Information Security Management and Technology (Taivalkoski, Finland, 2006)

who have provided valuable feedback on published papers relating to this research project.

The major institution I would like to acknowledge is the University of Vienna which proved several times that it provides the best possible support for young scientists. In conjunction I have to mention and thank for the experience I gained during my Erasmus exchange study at Royal Holloway, University of London.

Without all this support and experience I would have never been able to finish this life-fulfilling research project.

Thank you all for your continuous support.

Table of Contents

List of tables and figures

List of abbreviations

ACTA	Anti-Counterfeiting Trade Agreement (ACTA)
API	Application Programming Interface
AJAX	Asynchronous JavaScript and XML
BT	Bluetooth
CD	Compact Disc
CERT	Computer Emergency Response Team
CFAA	Computer Forensic Analyser and Advisor
DDoS	Distributed Denial of Service
DNSSEC	Domain Name System Security Extensions
DVD	Digital Versatile Disc
EU	European Union
FTK	Forensic Software ToolKit
GUI	Graphical User Interface
ICANN	Internet Corporation for Assigned Names and Numbers
ICG	Incident Cause Graph
IETF	Internet Engineering Task Force
IP	Internet Protocol
HDD	Hard disk drive
HTML	Hypertext Markup Language
MP3	MPEG Audio Layer III
MPAA	Motion Picture Association of America
MySQL	MySQL is a relational database management system and very common for use in web applications
NAS	Network Attached Storage device
NIST	National Institute of Standards and Technology
OS	Operating System
PCI	Peripheral Component Interconnect
PCI-X	Peripheral Component Interconnect Extend
PHP	PHP: Hypertext Pre-processor
PIN	Personal Identification Number
PIPA	Protect IP Act
RAM	Random Access Memory

SOPA	Stop Online Piracy Act
StGB	Strafgesetzbuch (= Austrian Criminal Code)
SQL	Standard Query Language (used for databases)
TAN	Transaction authentication number
WEP	Wired Equivalent Privacy (outdated wireless network encryption standard)
WiFI	Wireless Fidelity (802.11 stands for wireless network)
WPA (2)	Wi-Fi Protected Access (current wireless network encryption standard – WPA2)

1. Introduction

Computer forensics is a modern alteration of classic forensic science used for more than hundreds of years by law enforcement institutions worldwide. With the development and appearance of novel technologies, new forensic methods and approaches had to be developed or adopted. The “old forensic process” which worked flawless for the past years suddenly turned out to be useless to deal with this new threat scenario of computer crimes.

There is the necessity to adapt the old techniques and processes to handle the changed current situation. The fast growth of the internet and the worldwide connection of different networks and computer systems have increased the demand of forensic experts and computer investigations.

Modern computer systems have become so powerful that can be used in many different manners. On one hand these systems enable committing crimes, but on the other they might be used to solve crimes and prevent criminal activities. These systems provide powerful and strong tools within the forensic toolkit on which forensic investigators rely heavily.

The change of the current culture from an old-styled society based on the provision of services to a society that mainly focuses on available information increased the need for computer forensic experts and technologies due to the drastic growth of criminal activities within this field of science. Highly qualified computer forensic experts are needed for on-going investigations and their knowledge is mandatory for professional analysis which are required for court proceedings.

One of the most difficult aspects for computer forensic experts is to stay always ahead of possible criminal minds in respect of technology and techniques. The modern generation of forensic experts needs constant training and practice due to the fast implementation and development of novel technologies. Operating

systems, computer hardware, network technologies and other software solutions are constantly evolving therefore investigators spend a lot of their time constantly educating and improving their knowledge. In the event of forensic investigators falling behind the skill levels of criminals in terms of technological understanding, the criminals will win the “final race”.

The main idea behind this research project is, upon analysing the current situation, to define a theoretical model which can support forensic investigators during their computer analysis process. The main research question which has to be answered is whether there is a possibility to increase the time-efficiency of criminal forensic investigations by developing new forensic software solutions for automated analysis. Another essential part of this project focuses on the legal situation and other issues closely related to forensic investigations.

The outcome of this research project will be discussed within the following chapters and paragraphs.

1.1. Computer Forensics

The main idea behind the field of science called “Computer Forensic” is to obtain and analyse digital information for use as evidence in civil, criminal or administrative court proceedings. The roots of computer forensics can be found within the old-fashioned approach of criminal investigations. The main goal of those investigations is to identify the five key questions related to a crime: What, Where, When, How and Who. Every conducted investigation is based on these questions. What criminal act happened? Where did it take place? When did it occur? How was the crime committed? Who is responsible for the criminal act? These questions remain valid for computer forensic investigations as well; however they require a small adjustment.

Currently there are several different regulations that define in detail the preference of digital evidence and additional traces which have to be considered.

Computer forensic investigations are mainly conducted by law enforcement institutions which often have legal authority to commence forensic investigations. These days there are also some privately owned companies initiating forensic analyses on behalf of their customers but their actions are strictly regulated by legal regulations[1]. Nevertheless digital evidences which will be collected and gathered can be very crucial for possible upcoming court cases.

This field of investigation is closely related to different types of law and regulations which have to be obeyed in every detail. For instance it is illegal to break into another computer system without any legal permit, even in terms of an investigation. Another issue closely related thereto is data privacy and data protection. During computer forensic analyses investigators walk on a “tight path” that determines which actions comply with current regulations and which are prohibited.

One other issue about computer forensics which should be emphasized is that although the term “computer” is used within the title of this field of science it is not only limited to computer devices. Currently modern mp3 players and smartphones have so much computing power and memory built-in that they can also store crucial evidence data.

To fully understand the term computer forensics, it is important to discuss and highlight the difference between computer forensics and data recovery. Data recovery focuses mainly on techniques and technologies which try to recover information that was lost or deleted from a computer system. Computer forensics instead utilises the techniques of data recovery but with the focus on data which was deliberately hidden or deleted, with the purpose of ensuring that the restored data is valid and can be used as digital evidence. Another closely connected field of science is a “disaster recovery” which uses some of the

[1] Follow this link for additional information about Texas law requiring computer forensic investigators to get licensed http://legal-beagle.typepad.com/wrights_legal_beagle/2008/12/e-discovery-forensics-private-investigator-license-for-computer-data-collection-and-assessment.html

computer forensic techniques and concepts to recover lost or manipulated data and restore functionality.

It is very important for this research project to fully understand the terminology and idea behind computer forensics and all included limitations.

This thesis focuses on exploring the technical, legal and organisational challenges of modern computer forensic investigations and the implications of their relationships as responses to criminal, illegal and inappropriate on-line behaviours.

This perception allows us to generate a true and accurate picture of activities, timelines and events that have occurred on hosts, networks and running applications, to be in a position to validate whether criminal, illegal or other inappropriate on-line behaviour has occurred[2].

The following three subsections provide a brief introduction into the three main areas of challenges closely examined by this research project.

1.1.1. Technical Area

Computer crime incidents are often considered to be problems of general computer security, military intelligence and IT experts. The constant growth in the number of incidents and the increase of novel technological approaches have led to an explosion of concerns within this field of science. How shall the IT world react appropriately to deal with these new circumstances? Cybercriminals commit computer crimes in a more professional manner which can be observed over the past few years but the technological solutions for those kinds of threats are still missing[3].

As a result of this dramatic development, IT companies and experts try to adapt their well-established solutions by implementing additional routines and

[2] Citied from (Boucek, 2009)
[3] See (McAfee, 2012) for more information

extending their verified processes. It has to be noted that research and commercial companies focus their efforts on completely opposite directions. Whereas researchers try to establish and create novel approaches and concepts, commercial operators mainly stick to their current product portfolio and propose some additional functionality. Although new concepts and products emerged on the market, most commercial vendors appear to behave reactively to problems rather than proactively[4]. They provide solutions for existent problems instead of developing solutions that could handle such threat autonomously.

Moreover it appears that improvements in these technical areas focus on improving technical capabilities and performance issues instead of investigating the root of these problems.

A fundamental problem with this new threat scenario is that it cannot be solved exclusively with a technical solution. Novel and appropriate concepts that can change the current situation are still missing.

1.1.2. Legal Area

While comparing the developments between the technical and legal area, this research study comes to the conclusion that it is much easier and faster to develop a complicated technical solution instead of establishing and adopting new legal approaches and regulations. The legal area remains a relatively slow and tradition bound sector where changes of the current legislation require a big amount of discussions and thus time. While national and international frameworks do exist to address some of the challenges posed by modern computer crimes committed over the Internet, the practice of law within the national court systems exhibit considerable variation. Even countries of the European Union, which ratified similar European laws and regulations, have different approaches towards computer crime incidents. Austria and Germany

[4] For more information follow (Steinberger, 2012) or (Socialweb, 2013)

for instance focuses on data-privacy and data-safety, whereas Anglo-Saxon countries concentrate on data control and user-access control.

Another fundamental problem within the legal sector is the lack of legal professionals with the extended understanding of modern computer systems and technologies. Modern digital solutions introduce a completely new set of challenges, like digital evidence or a different chain of custody which has to be adopted to comply with current legislations.

Apart from these basic problems the legal area faces another issue which has to be addressed in more detail. Laws and regulations are often closely related and connected with each other. One minor change in one regulation can have a big impact and completely change the meaning of another one. Therefore they have to be considered very wisely and adopted appropriately. All corresponding consequences have to be taken into consideration to avoid situations where one novel law forbids a particular activity but correspondingly allows committing another crime.

Another side effect of the current democratic system is that governments are generally elected only for four or five years. Often these governments lack a possible outlook of all their legislative actions and they prefer only to adjust already proven laws instead of introducing new ones. This approach limits and hinders the adjustment of the legal system towards novel crime scenarios.

1.1.3. Organisational Area

Modern technologies like the development of the Internet created a new subcategory of trading companies based on electronic commerce. Companies quickly realised that with the proper use of these new technologies and concepts their revenues can be easily increased in combination with limited costs and extended market presence. Nevertheless most of them were aware of possible risks posed by criminal or inappropriate behaviours, but only a few installed appropriate security systems and procedures to avoid them. In

particular, organisations remained more concerned about fraud, defamation, loss of reputation, financial loss and the loss of a competitive advantage instead of dealing more cautiously with private user information and payment data for instance.

This lack of appropriate risk and management analysis lead to situations and problems that many companies face right now. They realise that there is a risk being always connected to the Internet with all their shop systems and involved database systems but instead of installing proper security systems, they assume that they will never become a potential target for any criminal actions[5].

The possible difficulties and risks are roughly known but due to the lack of proper legal regulations, companies are not forced to install appropriate security measures. In some countries companies are only advised but no official legal steps can be taken before such incidents happen[6]. Legal actions will be considered only when a computer crime is committed, which is in most cases too late to save any crucial information (private user information that is stolen for instance).

Novel European regulations that try to change this current situation are slowly being introduced that. At this point the “E-Privacy Directive” has to be discussed. It was issued in July 2002 and fully implemented in 2003 in all member states of the European Union. It describes data protection and data privacy from the user’s perspective in particular. This directive started a rethinking process about security measures within big ecommerce companies that have to comply with this new regulation[7].

Apart from the legal situation, another difficulty within the organisational area is the tendency of companies to “pull-the-plug” and turn all affected systems immediately off instead of properly investigating any occurring problems. This

[5] For more information see (Privacy and security concerns as major barriers for e-commerce: a survey study, 2001)
[6] See the “Competitive analysis of the UK cyber security sector” for more information (Department for Business, Innovation and Skills, 2013)
[7] For more information about this directive see (European Parliament, Council , 2002)

circumstance makes it extremely difficult for law enforcement units to investigate such incidents extensively.

As a response to such negligent behaviour even the “Computer Emergency Response Team” (CERT[8]) prepared a short report on the implications of computer crimes for modern companies to increase the consciousness for this kind of topic[9].

Companies with such mentality often misinterpret and take the threat of computer crimes not seriously enough. Instead of financing a highly-skilled team of in-house IT-professionals, these companies prefer to pretend that nothing will ever happen and assume that they are not at risk.

These entities often face dramatic situations that can lead to complete shutdowns of entire companies because of the lack of proper preparation.

Modern companies should have the appropriate strategies and concepts in place to be fully prepared for unpredictable situations and worst case scenarios like disaster recoveries.

1.2. The Research Problem

As already discussed within the last paragraphs novel technologies and concepts reveal potential risk scenarios that have become the focus of interest for technical, legal and organisational areas. While each field of science independently would require a full research project, the main problem can be only addressed with a combined approach. The above mentioned areas are so deeply connected and related that it makes no sense to solely focus on one field only.

[8] Computer Emergency Response Team (CERT) is a group of highly skilled experts that handle computer security incidents worldwide. Almost every country maintains his local CERT response team which are often supported by domestic universities.
[9] See (Team, 2002) for more information

Computer forensic demands a multidisciplinary approach that has to be supported by legal, technical and organisational solutions and new models. Different concepts and models have been developed by several different research projects, for example by the "First Digital Forensic Research Workshop"[10] and the CTOSE project funded by the European Union[11]. These models and definitions also reflect the on-going discussions inherent within the root disciplines that contribute to the multidisciplinary nature of this field of science.

Figure 1, Related areas of this research project

Most significantly, the computer forensic perspective allows for an examination of each specific area in more detail and its response to problematic criminal incidents as well as providing a conceptual framework within which the implications of their connected relationships are explored. The lack of coordination and fragmentation that appears evidently is caused by the fact that each area is struggling with its own problems, issues and challenges. The

[10] See (Palmer, 2001) for more information

[11] CTOSE stands for Cyber Tools On-Line Search for Evidence and is an EU project to establish a methodology to collect digital evidence.

researchers and practitioners in each of these areas attempt to address these challenges and solve these problems separately. Unfortunately, by making improvements in one area, another area may be negatively affected and suffer significantly, diminishing thereby the overall effectiveness of the responses.

1.2.1. The Research Question

To address the research problem discussed in paragraph 1.2, one complementary research question has to be defined:

> How can the efficiency of Computer Forensic investigations be improved by a better integration of standardised tools in the forensic analysis process, especially regarding the preparation of evidence for presentation in court?

To answer this research question in a complete manner and satisfy the research objectives defined within the next paragraph, the scope of this research project starts with an extensive literature research to investigate the current developments within the novel field of computer forensics.

As a next step the research methodology has to be defined and explained to underline the designated research approach.

The following section of this thesis introduces a novel concept and approach to enhance current computer forensic investigations including the identification of possible limitations which have to be clearly defined first. The concept and approach will be discussed in more detail, explaining all relevant connections between all three areas of interest. Based on the outcome of this discussion a practical model will be developed and introduced. This model will be further used for practical implementation to verify the newly established concept.

1.2.2. The Research Objectives

The following chapter will discuss current scientific and commercial work based on some novel computer forensic concepts that were evaluated during an extensive literature research during this research project. It clearly reveals that almost all concepts try to focus on one specific issue instead of dealing with all faced problems in a more general approach. Another challenge for this research project in particular was that there are almost no scientific publications that discuss a scientific approach with all related consequences within the three discussed areas. Technical solutions for instance can have explicit influence on the organisational layer and all of its relations but these are often not investigated or considered.

Trying to answer the defined research questions in paragraph 1.2.1, this research project tries to achieve the following research objectives:

- Analyse the current standardised computer forensic procedure
- Determine possible limitations of current investigations
- Develop novel model to enhance computer forensic investigations
- Identify legal requirements for generating results useable within court cases.

1.3. Chapter Descriptions

Chapter 2 presents a review of existing literature relevant to the research project. This chapter will discuss publications and concepts that come from various directions. Some will focus on technical solutions whereas other will discuss legal and organisational adjustments. All have in common that they are settled in the science spectrum of computer forensics.

Chapter 3 of this project defines the used research methodology which was used during this research project. The methodological framework underpinning this exploratory research is called the “Design Research” methodology. The

research strategy involves the development of a practical prototype based on the newly created concept and model. The main idea behind the prototype is to determine and verify the efficiency of this new approach.

Chapter 4 introduces the newly developed concept and model and discusses possible limitations to achieve all designated research goals. The results of this chapter lead directly to the practical implementation to verify the expected outcome.

Chapter 5 describes the practical implementation of the newly established concept and model. The product is a functional prototype which will be used to verify that the specified research objectives were achieved. This section of the research project includes a detailed description of the technical solution created to achieve the designated target.

Chapter 6 provides a theoretical case study in conjunction with a realistic scenario. It illustrates the efficiency of the novel forensic approach and the prototype functionality.

Chapter 7 discusses the collected results and outcome of this research project. It defines also possible limitations of the new concept and analyses the impact thereof on all three specified research areas. In addition it includes a synthesis of the main findings of the research, along with a brief discussion of the limitations of this study.

Chapter 8 provides the conclusion of this research project. At the end of this project an outline for future research work is given.

2. Related Work

2.1. Selected Publications

This chapter provides an overview of publications and articles relevant to this research project. The research was conducted between 2009 and 2011. It focused on novel computer forensic approaches and concepts that will be discussed in the following paragraphs.

The computer forensic science is still a novel field of science, which reflects the different variants of forensic approaches. One of the most common approaches is to adopt the current traditional criminal forensic process. Nevertheless computer forensic is mainly based on computer systems which requires different approaches and concepts. Another advantage of this novel field of science is the use of modern technological solutions which provide access to innovative solutions.

To secure a broad scope for the literature overview seven very interesting and promising computer forensic researches were chosen which will be discussed in more detail. These concepts and models include all different variants of novel approaches and solutions. One publication describes the development of a pattern matching board that improves the digital forensic performance. Whereas another one describes the global needs of a general approach of information security for the modern information society.

At this stage it has to be reminded that analysis and discussion of all modern approaches would exceed the scope of this research project therefore it will be limited. Nevertheless this literature overview provides a general overview of current developments and research projects found within the field of computer forensic.

The first publication describes the need of new memory analysing forensic techniques to collect important digital evidence, which could be lost or destroyed by incautious behaviour. It describes also the possible advantages that can be gained through additional information by breaking encryption keys.

The next paper discusses a very promising approach to increase the efficiency of computer forensic investigations by using additional hardware components. The authors achieve an impressive acceleration for forensic analyses by installing a special extension board called Tarari.

The third paper introduces a new concept to enhance computer forensic analysis by using visualisation and data exploitation. The authors discuss a very useful approach to support forensic investigations by visualising gathered evidence and creating links between all incidents.

The fourth describes a post-mortem incident modelling method with a novel point of view for an investigation.

The fifth publication deals with a very general discussion about computer forensic and the needs of information security. It points out that the currently changing society requires new solutions and new guardians to protect them.

The sixth paper analyses the current hacking trends related to cybercrime incidents. It provides an interesting overview to the actual hacking scene and compares the different techniques used by Asian and European hackers.

The last paper describes a very important part of forensic investigations: Forensic Evidence Management. It provides some novel concepts and discusses current limitations and bottle-necks.

2.2. Enhancement of Forensic Computing Investigations through Memory Forensic Techniques

Authors: Matthew Simon and Jill Slay

This paper highlights the need of advanced memory forensic methods and techniques. It demonstrates also the weaknesses in conventional forensic methodologies, tools and techniques. Memory forensic techniques have a potential to recover digital evidence where conventional static-media based techniques fail. Due to the constant digital evolution the number of novel challenges during an investigation especially in the collection and analysis of technical devices is increasing. Computer Forensic needs to meet these challenges with novel tools, techniques and processes to understand the potential of digital evidence and also to provide means to detect and analyse systems where these evidences are utilised.

According to the authors the memory forensic techniques prove to have the required potential to overcome all new challenges and issues by extending the manner of gathering digital evidences. Physical memory can provide a source of evidence to analyse the previous and current state of an investigated system. This kind of information can be decisive for the entire investigation. It can also contain remnant data of network applications within the volatile memory store, allowing investigators a deeper and wider view of the scene. Anti-forensic measures such as encryption software may also be defeated by recovery of encryption keys and passwords.

The conclusion of this paper summarises the need of further research into memory forensic techniques focusing in particular on the application level data. The current development aims primarily on data that is stored physically on hard drives or other storage devices excluding the volatile data stored within the memory. The research need is for tools and techniques that can extract high level data stored within applications and technologies that are problematic for

conventional forensic computing methodologies. Furthermore the research has to address two different areas: firstly a greater use and understanding of physical memory as a standalone source of evidence and secondly the use of physical memory in combination with other conventional sources of evidence as a mean of providing greater understanding than possible from one single source. The additional use of physical memory can influence the outcome of an entire investigation[12].

2.3. Improving Performance in Digital Forensics by using Pattern matching Board

Authors: Jooyoung Lee, Sungkyung Un and Dowon Hong

This paper focuses on the acceleration of digital forensic investigations. It demonstrates a novel approach to use a so called Tarari calculation board for pattern matching analyses. Figure 2 illustrates a Tarari expansion board which can be used in every PCI and PCI-X slot (commonly available expansion slots).

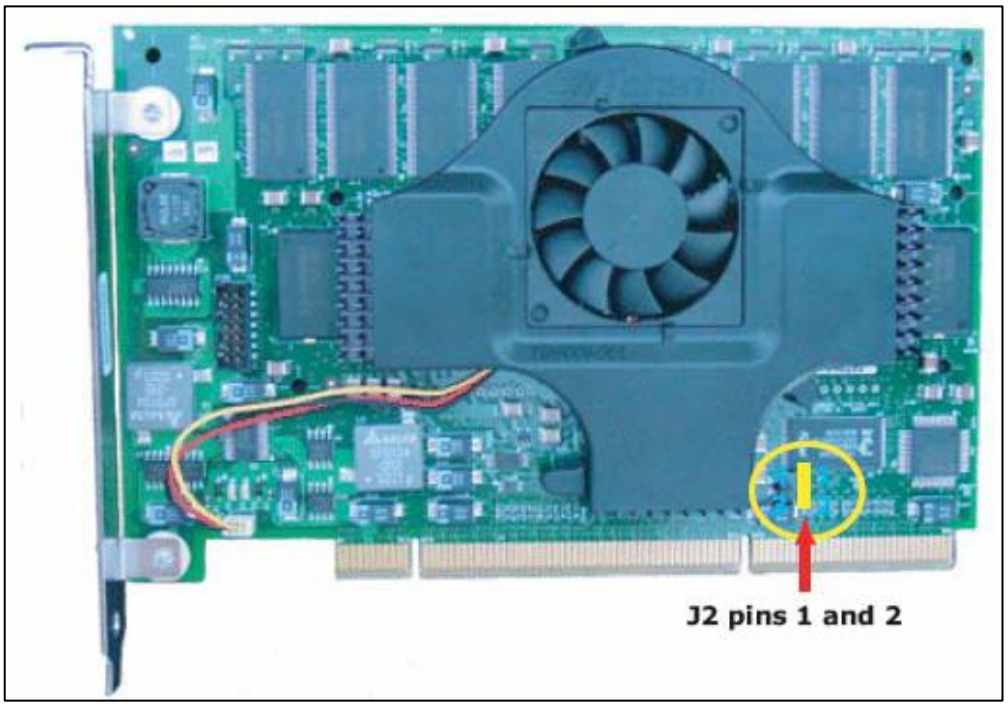


Figure 2, Tarari expansion board

[12] See (Simon, et al., 2009) for additional information

To present the success of this approach the results gained by this new device where compared with the gathered results of the commercialised forensic tool called EnCase. The Tarari board proved to be 5 times faster during an average keyword search. Another advantage is that it analyses connected hard drives entirely including even non-allocated areas. Moreover it demonstrates how easily it can be implemented into an existing forensic environment without exceeding any cost limits.

The main aim of this expansion board is to increase the efficiency of the forensic analysis and investigation process. Additionally it proves that novel hardware devices can be easily adopted and implemented into working environments. The only main drawback of this approach, which actually proves to be the most interesting part of this research project, is the Tarari board itself. Due to the lack of mass production and expectable high development costs it will be mainly limited to institutions and foundations with generous financial resources such as military or intelligence agencies.

Nevertheless this paper points into an interesting area of developing novel devices for successful computer forensic analyses. Besides it shows that the goal should be to increase the efficiency and speed of investigations which can finally result in reducing additional costs[13].

2.4. Enhancing Computer Forensics Investigation through Visualisation and Data Exploitation

Authors: Grant Osborne and Benjamin Turnbull

This research focuses on establishing a need for new architectures to build visualisation systems that enhance computer forensic investigations of digital evidence. One big challenge today is the proper visualisation of all gathered evidences and information. It can provide an additional support during an investigation and point into the right direction. This paper suggests that there is need for new techniques that display data in easy understandable visual forms

[13] See (Lee, et al., 2009) for additional information

that “facilitate efficient insight gaining into digital evidence” [14] . These visualisation techniques demand source data that contains additional context relevant information which can be useful during an investigation.

The primary focus of visualisation systems is to enable users to navigate through data structures and focus on information that is consequential to them with the relative ease and familiarity. If all digital evidence can be extracted from all involved devices and stored in a way that they are comparable and represented in a visual form that is understandable, current digital forensic investigations can be radically enhanced. Apart from that this research project discusses the separated approach of data analysis and visualisation. Instead of combining both technologies to create a visualisation presentation layer above the data processing layer that would provide additional support for the investigators, the current research focuses mainly on data analysis. The constant visual representation of the data enhances an investigator’s understanding of the related data set.

Additionally this research introduces the notion of data exploitation which mentions a way to describe techniques that provide opportunistic data analysis across multiple sources of digital evidence. “Data exploitation techniques shall provide normalisation techniques, event correlation, relationship extraction and investigative domain knowledge processing across a set of evidence”[15]. Data exploitation aims to look beyond easily accessible information such as modification, access and creation information embedded in every file, as well as simple file type analysis, drawing on data mining and event correlation techniques.

Visualisation proves to be an interesting research area which can provide additional and helpful information for investigators. One of the biggest challenges seems to be the extraction and appropriate visualisation of all gathered evidence and data. There must be some kind of Meta level which stores additional information required for an intelligent presentation. This

[14] Taken from (Osborne, et al., 2009; Osborne, et al., 2009)
[15] Taken from (Osborne, et al., 2009; Osborne, et al., 2009)

request demands novel techniques and approaches for a successful visualisation and data exploitation of related gathered evidence[16].

2.5. A Post-Mortem Incident Modelling Method

Authors: Shanai Ardi and Nahid Shahmehri

This paper presents a structured method to perform the post-mortem analysis and to model the causes of an incident visually in a graph structure. The goal of modelling incidents is to develop an understanding of what could have caused the security incident or computer crime and how its recurrence can be prevented in the future. From the forensic point of view this approach can help to reconstruct exactly the latest process and actions before a computer system was attacked.

The general process for performing an incident post-mortem analysis is divided into four different steps:

1. Collecting every log file that can be useful in identifying how the incident happened
2. Collecting a set of incident hypotheses, conducting interviews of all involved parties and accepting or rejecting the hypothesis
3. Refining hypotheses by rejecting those not supported by facts
4. Finalising the proposed theories and suggesting countermeasures.

The novel proposed approach now presents four adopted steps supported by a structured modelling method:

1. Listing all gathered evidence about the incident and reports
2. Incident hypothesis is generated by answering a set of questions which creates an incident scenario:
    a. What was the incident type (according to NIST)?
    b. What was the incident indication?
    c. What security measures were applied?
    d. What detection measures were applied?

[16] See (Osborne, et al., 2009; Osborne, et al., 2009) for more information

3. Generating the Incident Cause Graph (ICG) based on the gathered hypothesis
4. The resulting graph is used to generate a set of lessons learned and to identify effective countermeasures

Figure 3 illustrates an entire ICD graph for a simple Half-Life case study.

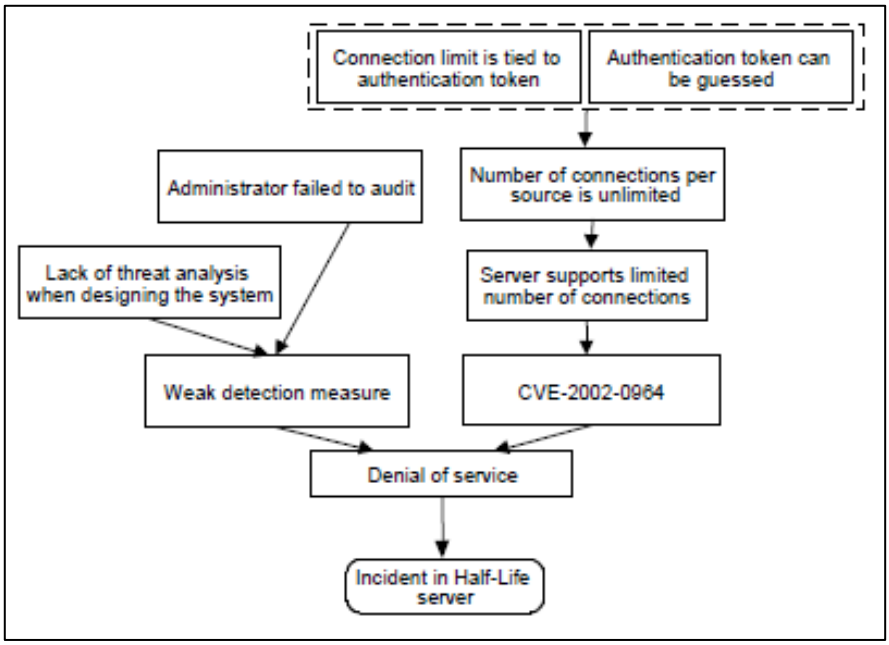


Figure 3, typical ICG (in this example for a Half-Life case study)

The ICG is built by identifying its cause nodes and their relationships. For the successful generation of an ICG there is a need of detailed knowledge about the system architecture, organizational policy and corresponding risks and threats. This requires a highly skilled professional who is fully trained and used to such analysis.

Comprehensive analysis of incidents should constitute a part of the incident response process. In order to ensure the long-term prevention of incidents, the incident response team must understand the root cause of incidents and address it with proper countermeasures.

Although this paper is not directly related to computer forensic it proves to have the same core aim to reduce the criminal impact of computer crimes. Looking

closer at the process to create an ICG graph it shows evident similarity with the forensic investigation. It demonstrates a simple approach to visualise an occurred incident and to finally derivate some successful countermeasures thereof[17].

2.6. An inclusive Information Society needs a Global Approach of Information Security

Authors: Solange Ghernaouti-Hélie

This paper tries to discuss the topic of information security in a more general and philosophic way. It analyses and postulates the hypothesis that the global information society and knowledge economy are both constrained by the development and overall acceptance of an international cyber security framework. The validity of such a framework or model requires a challenging multidimensional cyber security approach for everyone – from individuals to organizations and states. A future culture of cyber security contributes to a safe and secure information society. Currently most efforts are focused on awareness which is appropriate and mandatory but not sufficient. In fact, education should be effective and available for each kind of stakeholders (policy makers, justice, managers, end-users...).

"Mastering information risks through information security could help to strengthen confidence in the electronic marketplace and all other e-commerce system. There is no real technological obstacle to further development of information security but the scope of deployment of effective security measures is very complex and related costs are not minor. Private and public partnership is desirable, at national and international levels, to integrate security into infrastructure and to promote a security culture, behaviour and tools. Financial, procedural and organizational resources are to be found to support effective deployment of security that could be of benefit to everyone"[18].

[17] See (Ardi, et al., 2009; Ardi, et al., 2009) for additional information
[18] Cited from (Ghernaouti-Hélie, 2009; Ghernaouti-Hélie, 2009)

This paper discusses in general a very interesting topic about the evolution of current society and the need of cyber security. Due to the fact that the influence of the internet on the average life is constantly growing there is urgent demand for a cyber-police institution. The challenge now is to convince society about this need which comes together with novel security technologies. These new techniques can have a huge impact on every human being because they can, if the development goes into the wrong direction, degrade the “holy” status of privacy which is a fundamental right within modern society.

This paper shows that there is a need of discussion on a higher political layer about the evolution of society in a more philosophic way. This could have a tremendous impact on the entire forensic science by changing the fundamental circumstances[19].

2.7. Peter the Great vs Sun Tzu

Author: Tom Kellermann

The main aim of this publication is to give a short overview of the current hacking scene and provide a comparison of the different techniques used in Eastern Europe and Asia.

The author analyses the completely different strategies which both hacker scenes follow. East Asian hackers, located mainly at the chines coastline, tend to use more simple approaches. They prefer to gain as much data as possible during their attacks and make use of massively available free-hosting systems. In comparison Eastern European hackers, located at the former Soviet bloc, use much more sophisticated and complex techniques. Due to their extended maths and logical skills (a gift from the former soviet educational system) the involved algorithms are much more precise and include as little code as necessary. Even the infrastructure used for cybercrimes is different.

[19] See (Ghernaouti-Hélie, 2009) for more information

"Eastern European hackers tend to develop their own infrastructure specifically designated for their own use in attacks. They tend to be in control of their entire infrastructure and will routinely set up their own servers for use in attacks as well as to develop their own Domain Name System (DNS) servers to route traffic and create sophisticated traffic directional systems for attacks."[20]

The author investigates also actual malware attacks like "Tinba" [21] and "Luckycat"[22] and compares the different techniques and approaches.

The conclusion of this research is that both hacker groups have completely different strategies and techniques. Whereas the East Asian groups try to achieve as much harm as fast as possible, Eastern European hackers focus on specific designated targets. In addition Eastern European hackers develop and implement much more-sophisticated programs which guarantee a higher-level of success.

[20] Taken from (Kellermann, 2012)

[21] "Tinba" is an extremely well written malware program which has an extraordinarily small size – approximately 20 kilobytes. Its main purpose is for information-stealing especially in the financial sector. Main attack location was Turkey. Currently there are around 60,000 infections in Turkey. Follow (Trend Micro, 2012) to find more information about Tinba.

[22] The „Luckycat" campaign mainly targeted the aerospace, energy and engineering industry. The attack was designated against companies in India and Japan and conducted with the help of malware software which exploited vulnerabilities in popular software. The entire campaign started in June 2011 and has been linked to more than 90 attacks. Main elements of this campaign could be tracked to hackers based in China. See (Trend Micro, 2012) for more information.

Hackers	East Europe	East Asia
Patriotic hackers **Goal:** Support their homeland	Website defacement; ability to conduct large-scale DDoS attacks; coordination with military operations (RU-GE War)	Website defacement; ability to conduct large-scale DDoS attacks
Criminal hackers **Goal:** Generate profit	Profitable operations with affiliate model distribution and active underground economy; professional malware development; professional exploit pack development; global distribution and mass targeting	Profitable operations with "cell" structure and active underground economy; primarily focuses on China
Espionage hackers **Goal:** Steal intellectual property	Still not well-known; possible operation leveraging criminal tools and infrastructure (ZeuS/ Kneber); possible "APT-style" operations emerging with good operational security	Development and use of advanced exploits, including zero days; highly targeted attacks; low-quality malware or use of publicly available malware (RATs); persistent operations with low operational security

Figure 4, Tactical Comparison of East European and East Asian[23]

It is interesting to investigate the cultural differences and motivations of committing computer crimes. The used technologies and involved organisational structures are completely different which is caused by different cultural circumstances.

2.8. A Tactical Management Model of Forensic Evidence Processes

Author: Colin Armstrong

This thesis discusses the development of a tactical management model of forensic evidence processes. It investigates the question of not standardised evidence processing and different approaches. It analyses the different points of view for law enforcers, forensic scientists and the local judiciary. Each view requires a different approach for successful investigations.

The main aim of this research project is to generate a novel framework for building better forensic evidence solutions. During the conducted research

[23] Taken from (Kellermann, 2012)

a preliminary model was established which led directly to the development of a functional meta- model.

The resulting meta-model and all constituent parts address challenges to tactical management of forensic evidence processes that provides a holistic management tool[24].

The established meta-model provides a framework for six component models addressing the perspective and reason for the intervention, building of evidence knowledge, analysis of the relationships between evidence items, building forensic evidence networks of investigated cases, an evidence resource library and finally evidence classification schemes.

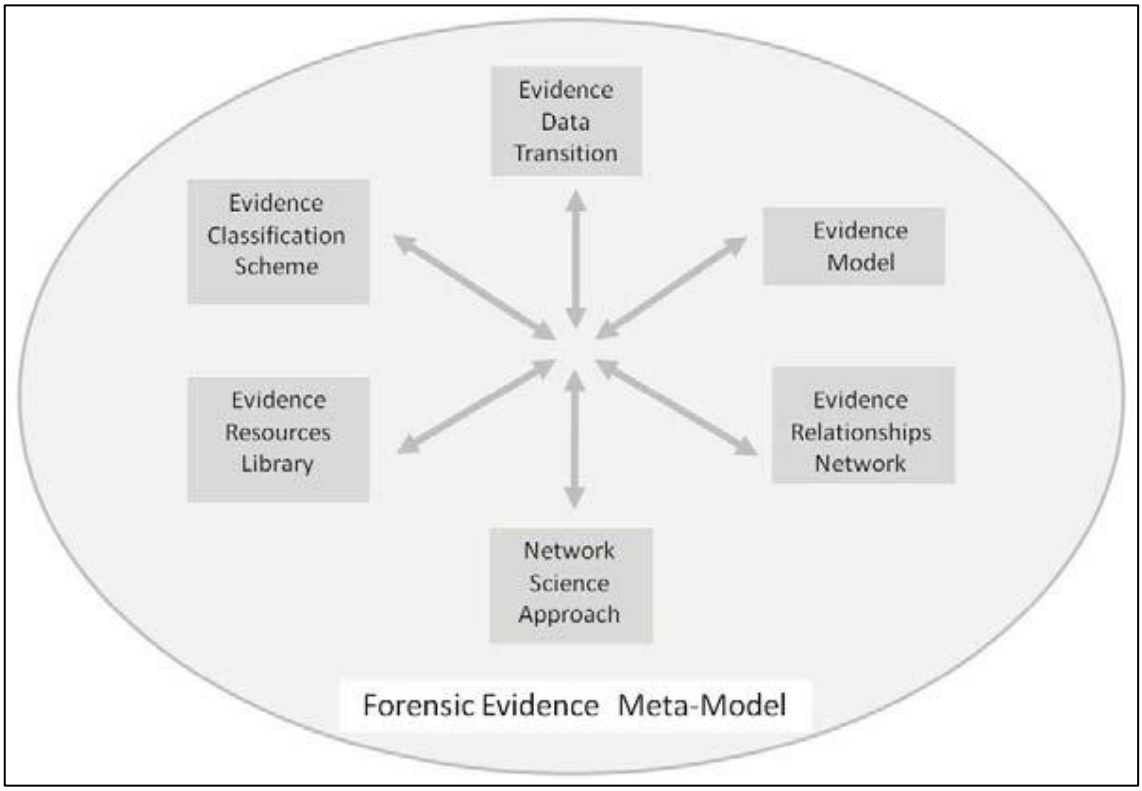


Figure 5, the Forensic Evidence Meta Model[25]

The discussed results were gathered and collected through extensive interviews with forensic experts and law enforcement agencies. The outcome represents

[24] Cited from (Armstrong, 2010)
[25] Picture taken from (Armstrong, 2010)

an impressive framework which can provide a standardised approach for further forensic investigations.

2.9. Summary

The number of computer crime incidents is constantly evolving and threatening every networked computer system. It is difficult to find one general approach which fits for every aspect during an investigation. Nevertheless those presented research projects present an advanced novel concept which can enhance the outcome of almost any forensic investigation.

Another very important aspect which is closely related to computer crimes and especially to computer forensics is the collection and handling of digital evidence. Digital evidence of a computer crime scene can be found in almost any digital device. It is not only limited to dedicated computer or server systems. Due to the fact that modern MP3 players and mobile smartphones often have sufficient computing storage and power, they can keep information that can be crucial for the entire investigation. It is very important to remember that digital evidence which is gathered during an investigation has to be well documented and should always be collected in a systematic way. This process guarantees a neutral and objective investigation which can be very helpful during court proceedings. Besides sealing typical hard drives, it should be taken into consideration that computer systems do not include only hard drives. All connected peripherals have to be investigated as well because they can provide valuable information. Apart from attached devices it is also very important to understand the different volatility levels of data which have to be handled in a different way.

Computer forensic is a very novel and constantly developing field of science. There are many different research projects which share the same goal: to increase the efficiency of forensic investigations. A successful computer forensic investigation still takes too much time so that today's legal institutions do not have the capabilities to commence a computer forensic investigation for every computer incident. There is a fundamental lack of highly educated staff,

adequate soft- and hardware and finally appropriate concepts and strategies. On the other hand there are so many different ways and cases of computer crimes that it is illusive to search for a general strategy or solution.

Due to the advanced scientific results gathered within this research project, it will be used as the argumentation strategy framework for the on-going scientific work within this thesis.

This research project will make use of all gathered results and create a novel concept tested with a technological prototype which will be presented in the following chapters.

3. Research Methodology

3.1. Introduction

This chapter discusses the research methodology which was used to conduct this scientific project.

The methodological framework is based on the “Design Research” methodology which was used during this research study. The research strategy tries to identify the technical, legal and organisational challenges related to computer forensics. The interpretation and discussion assumes a forensic perspective to analyse and discuss the relations across these three different areas and to explore the resulting implications.

This research section intends to identify all possible challenges and relations which will be used as a basis for a novel concept and model in chapter 4.

The first section discusses the selected research philosophy. The second part explains the research strategy in more detail. The last section of this chapter provides details on the selected approach which leads to the extensive interpretation and discussion.

The “Design Research” steps are mainly based on a publication written by A. Duffy and F. O’Donnell[26].

3.2. Design Research Approach

The “Design Research” as a fully defined concept was introduced in the early 60s[27] although it combined the ideas and concepts of already established research approaches. The main idea behind this research philosophy is to shift

[26] Follow (A Design Research Approach, 1998) for more information
[27] See (Collins, i inni, 2004) for more information

the research phase directly into the design phase. It might sound surprising to conduct a technological research during the design stage, however it finally provides essential advantages and helps to identify achieved research goals.

The idea behind this research philosophy is to investigate "the process of designing in all its many fields"[28]. Designing proves to be a creative act, common to many disciplines. It is closely related to theoretical research work as it gives the possibility to create and validate any conceptual model. In addition it supports advancing the theory and practise of design[29].

Soon the "Design Research" approach was established as a well-defined and validated research strategy which is known to researches worldwide.

Figure 6, Design Research Process

The appropriate research process can be divided into 5 main sections which will be discussed in more detail within the following paragraphs.

- Research Idea
- Needs Analysis
- Research Framework
- Research Approach
- Validation.

[28] Cited from (Society)
[29] Based on (Society)

3.2.1. Research Idea

The “Research Idea” summarises the overall motivation and inspiration behind the research project. It combines the area of interest together with the research activity. For this project the motivation was obvious. Due to the advanced interest within the field of computer forensic, the idea was born to support forensic investigators. Besides, novel technologies involved in this field of science will see an enormous increase of demand. The demand of knowledge and expertise will grow dramatically, almost with the same speed as the number of computer crimes committed worldwide.

3.2.2. Needs Analysis

After identifying the research mission, a needs analysis has to be conducted. The results of this analysis are necessary to examine if there is any need for a novel technical solution based on a new conceptual model. In reality this research project shows that forensic investigators have a huge lack of a structured approach. It illustrates that investigators often have an extensive toolkit (e.g. forensic software) ready for user but without a proper guidance it is almost impossible to utilise all functionalities.

The outcome of this research phase leads to the key research areas which has to be identified. Because of the “Design Research” approach it also has influence on the theoretical and practical model. The identified key target areas result in the design process improvement and the corresponding research areas.

3.2.3. Research Framework

Due to the close relation between the design phase and the research phase the “Research Framework” plays a very crucial role. Modern design processes are closely related and linked to computational design tools and data models. This proves also to be one of the biggest advantages of this concept. Technological

solutions combined with human interactions allow the design phase to be more accurate and effective.

In this research project the “Research Framework” is based on the assumption that any developed technological solution will make impact on the design stage itself. This guarantees that the “Design Research” approach is constantly refining itself and generates more accurate results. The outcome of the design phase relates closely to the research phase which again influences the design phase. Figure 7 illustrates the constant redefining mechanism of this approach.

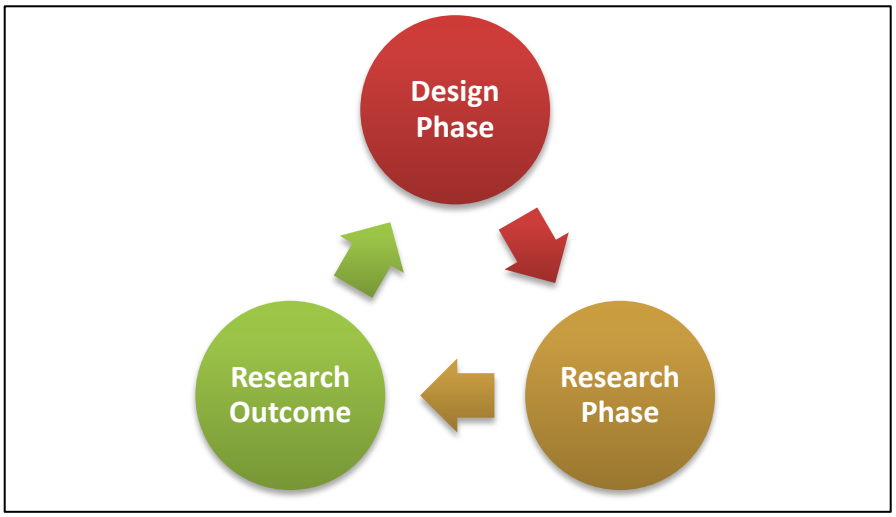


Figure 7, Research Framework

Based upon prior work the scientist Venable established a more detailed cyclic model[30] for the “Design research” methodology as illustrated in the following Figure 8. Solution technology invention is the end product of “Design Research”, where technology design/invention encompasses design (based upon theory), development or building, plus functional testing of a proposed solution technology. It is understood that the technology design/invention includes design that is based upon theory and conceptual models. “Technology” in this context includes systems, methods, algorithms, technological solutions, practices, in addition to a product and other appropriate means of problem solving. For solution invention to take place, a conceptualization or theory of the creation needs to be formed, even if still fuzzy and not properly defined.

[30] See (Venable, 2006) for more information

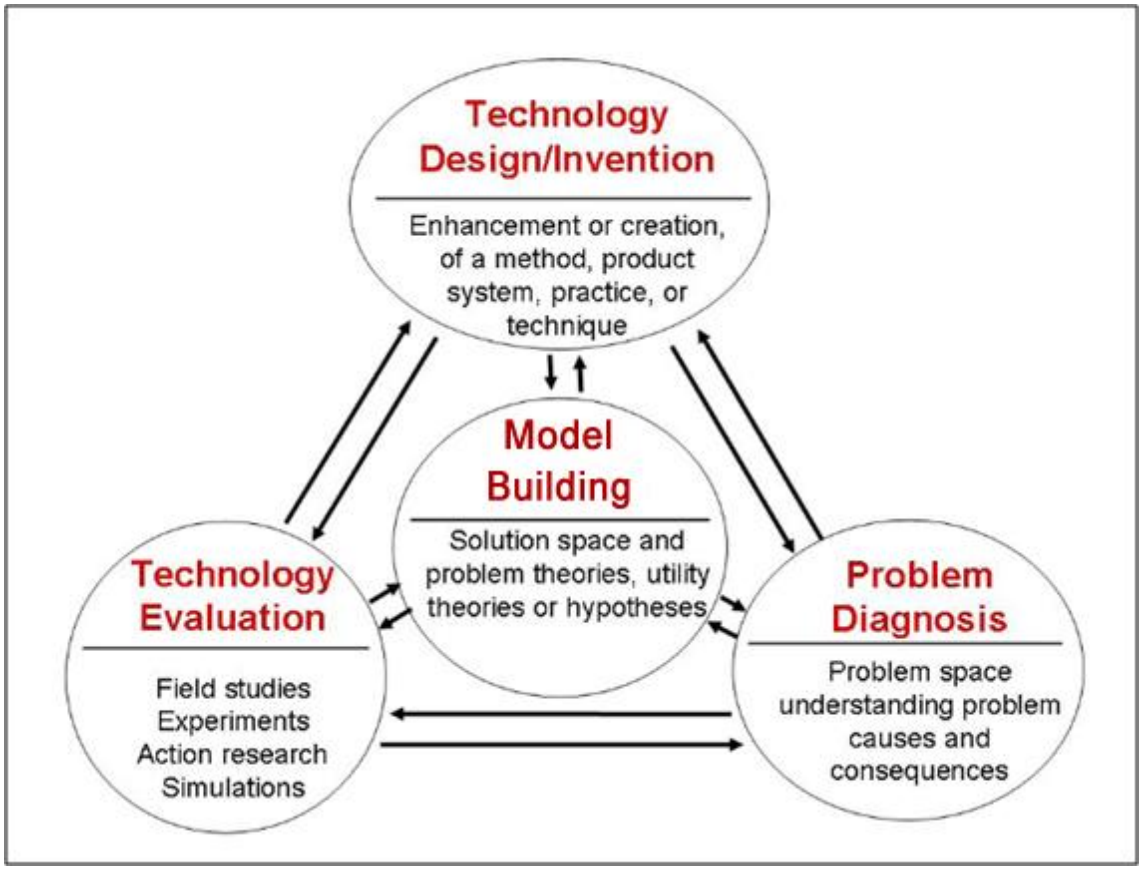


Figure 8, Modified Design Research Framework

As “Design Research” in general is focused on building solutions to address a given problem space, the “Problem Diagnosis” phase provides a solid foundation for solution design. The “Problem Diagnosis” phase involves gaining the understanding of the problem situation and investigating the causes and the impact of the problem. The definition of the term problem is “the difference between perceived reality and perceived expectation for that reality, together with a desire to make the perceived expectation become reality[31]”.

If the desired state and the current state are the same then there is no problem. The problem analysis is the full understanding of the question space. This knowledge must include both, the desired state and the current state. In Venable’s “Design Research“ approach the main phase is called “Model Building” where the analyses of the solution space is carried out, theories are built and novel concepts established. The “Technology Design/Invention” phase

[31] Quoted from (Jayaratna, 1994)

includes the creation of a system, method or technique to provide a solution for the specified problem.

This solution technology is expected to assist in eliminating or reducing one or more of the identified problems.

The “Technology Design/Invention” stage is a solution design set of activities rather than a technological design that as a technological resolution may not always be the best fit to the problem. Similarly, the “Technology Evaluation” stage is a solution evaluation pursuit in this context. The “Technology Evaluation” phase involves the application of research methods and instruments to evaluate the goodness of fit of the solution to the problem space.

The “Design Research“ is able to offer a structured, yet flexible approach to the process of designing solutions for systems-related problems and the association application of technology to those solutions. The “Design Research“ is the ideal methodology for the development of theories and designs for the related solutions.

The main advantage of the Venable “Design Research“ model is the flexibility and integration of all phases within the approach. Although Venable’s focuses on the format of representation, called the “Model Building” phase, the central activity creates the possibility for an adaptable approach to be included in the general research process.

Research involving methods, such as action research and prototyping, can be more readily incorporated into the research process configured in this way. The ability to move back and forth in cycles amongst the phases is an additional benefit which leaves researchers the chance to adapt their approaches. This means that modifications and enhancements can be made during the research project to support the research outcome[32].

[32] General description cited from (Armstrong, 2010)

3.2.4. Research Approach

The “Research Approach” acts generally as an overall guide to implement the research thesis. The design problem is redefined and a possible hypothesis of how-to better support design is proposed based upon an analysis or understanding of the design. This hypothesis is formulated into a research problem within the field of interest.

Afterwards a possible solution for this approach is realised, evaluated and the overall results and appropriate documentation generated.

Within this thesis this stage can be compared to the prototype development. The CFAA prototype represents a technical solution based on the defined conceptual model. The model itself was adapted several times to generate a more accurate solution.

3.2.5. Research Validation

The validation phase represents the last stage of this “Research Approach”. All generated models and results have to be evaluated in a scientific way to guarantee valid results. There are many different approaches and strategies to generate the best validation process but in general every hypothesis, concept and solution has to be argued upon other theories and models.

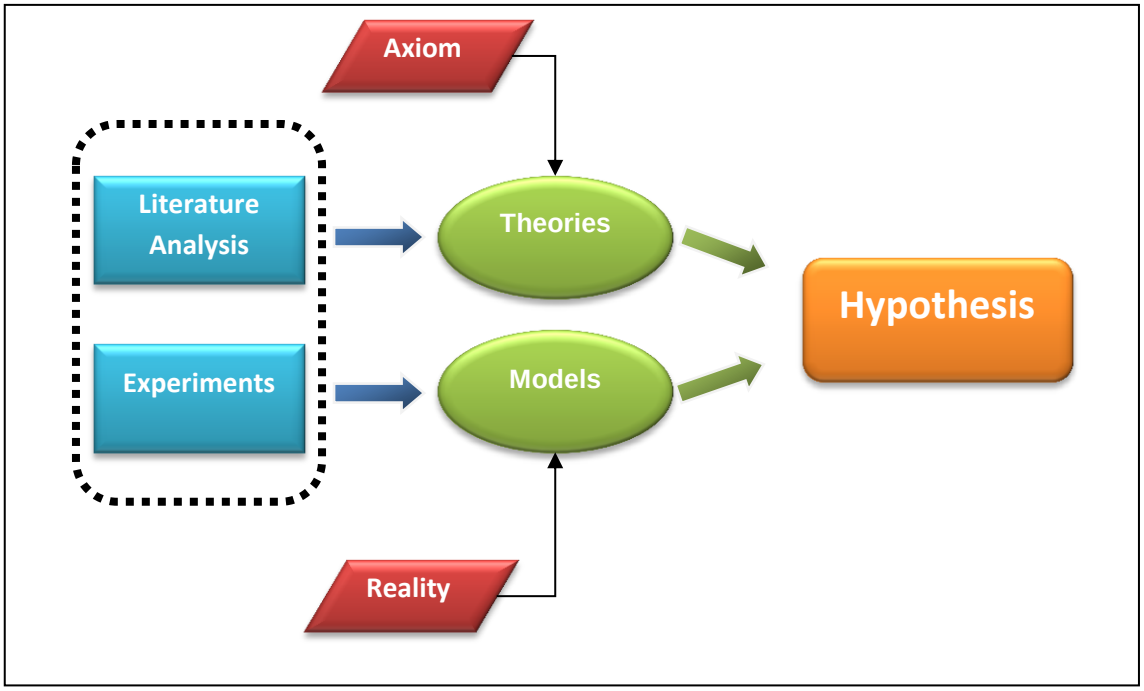


Figure 9, Validation Template

Theories which are built upon a combination of known axioms and a fundamental literature analysis conclude with the hypothesis in the same way as models. Models are the result of experiments and literature, as same as the reality. These two parts define a hypothesis. To validate this hypothesis all established theories and models have to be evaluated. Only in the case they pass the evaluation process, the hypothesis itself can be validated otherwise the entire hypothesis cannot be valid.

In addition there are several different evaluation techniques which can be used for such verification:

- Case studies - particular instances of design are studied and analysed.
- Experiments - predefined criteria and methods of evaluation are established and artificial scenarios are constructed. Design experiments are artificial in nature whereas the other methods are more closely based on actual design practice.
- Industrial studies - actual design practice is studied and analysed through a variety of techniques, e.g. interviews, protocol analysis, methods study, etc.
- Protocol analysis - records of design practice or experiments, using audio/video tapes or other means, are analysed.

- Worked examples - similar to case studies, scenarios of particular design problems are simulated and analysed.

3.3. Design Research approach for this project

The research strategy for this project was as followed. The basis for the technical prototype was established by defining a conceptual model first. The first model illustrated a simple and raw start for this research project. It clearly defined however the first steps and pointed the direction of this research. Based on this first model a state-of-the-art analysis was initiated. First was the broad idea to support computer forensics in general. However subsequently the question was narrowed down into how can investigators in particular be supported.

What are the main challenges? Afterwards the overall-picture became much clearer. Investigators spend a lot of time going through manually different search scenarios. No common and extensive approach could be identified or defined. Due to different legal situations it was nearly impossible to define an all-valid solution for every possible situation.

As a next step the research question was readjusted again. If there is no chance to help the investigators with a general solution, there must be a more in-depth approach to support them. One special field of forensic investigations was identified and newly investigated. The focus shifted to the science field of malware identification. Computer forensic experts have advanced technological tools which can investigate different areas of computer systems. However a common problem is that a standardised approach is missing. Some investigators focus on network protocols whereas others verify software vulnerabilities. The same problem is with malware software itself. IT experts know that this kind of software can provide crucial evidence for committed computer crimes but in most cases their appearance is disregarded as deep investigations often lead to possible dead-ends. Therefore the idea for this research had to be narrowed down once again. How can the process of

malware identification be supported? Is there any chance of increasing the efficiency overall?

Meanwhile the designing process was running as well to support the research approach. How should the technical prototype be defined to achieve the designated research goals? This step finally determined the conceptual model and the related research strategy.

In the end the technical design helped to define the theoretical model in more detail and vice-versa. As a result of this strategy the conceptual model became more accurate as same as the prototype development because of the advanced design stage.

This research approach visualised the beauty of the “Design Research” strategy. Due to the novel model and concept development a scientific prototype could be developed but the final version thereof once more adjusted the defined models and concepts.

The “Design Research” methodology provided the flexibility to outcome several problems during this research project whereas it also strictly limited the possible boundaries and guaranteed the focus on the research task.

3.4. Summary and Reflection

This chapter describes a very crucial part of this research project. One of the first steps was to define a possible research methodology to generate appropriate and accurate results. The “Design Research” approach proved to be the most efficient approach method and increased incidentally the efficiency of the outcome by shifting the research phase into the design phase.

The details analysis of the Design Research approach showed the complexity of this methodology and underlined the advantages which were the main causes for selection.

The following chapter 4 presents the novel concept and the according model. It will describe a new approach for an automated forensic investigation tool.

4. Concept and Model

This chapter analyses and discusses all relevant topics and key areas for creating a novel concept and model solution for this research project. The main idea behind this research project is to create a new approach for computer forensic investigations combined with an automated forensics case preparation system. To achieve this goal a new conceptual model has to be developed which deals with all requirements to fulfil this target. All requirements and possible aspects have to be analysed and discussed in every detail to guarantee the completeness of this approach. In addition the feasibility of this proposed solution has to be verified and tested and possible limitations identified.

All analysed and discussed issues together form the conceptual model which is needed before the prototype solution can be approached.

This chapter is divided into five different parts and finishes with a short summary. The first section describes the actual situation of a computer forensic investigation and the possible transition into a court case. The next paragraph tries to identify all possible requirements and analyses, the three main key aspects in more detail. The third section analyses the feasibility of the proposed solution which concludes in possible limitations within the next section. The forth part describes the entire conceptual model including all aspects. The last paragraph of this chapter summarises all sections.

4.1. Current Situation

This section gives an overview of the current situation during a computer forensic investigation. It analyses three main areas which will help to identify the current requirements.

The first section describes a typical forensic investigation with all involved steps. The second part discusses the current legal framework and all appropriate laws and regulations. The next paragraph analyses the organisational setting and structure which is mandatory for a successful investigation. The last section deals with the technological environment.

4.1.1. The Typical Digital Forensic Process

Computer forensic investigations facilitate the core techniques of traditional forensic approaches. Generally speaking, forensic science is the application of science to the law – any scientific principle or technique that can be applied to identifying, recovering, reconstructing, or analysing evidence during a criminal investigation is part of forensic science[33]. The scientific principles behind evidence collecting are well-established and commonly used.

One fundamental principle which is also valid for computer forensic analyses is the Locard's exchange principle which defines that "anyone, or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they depart"[34]. In the physical world an offender may leave some DNA evidence like a hair or a fingerprint at the crime scene. In addition he can accidently take a feather or a fibre from the scene. This kind of evidence can prove a possible connection between the crime scene and the possible criminal.

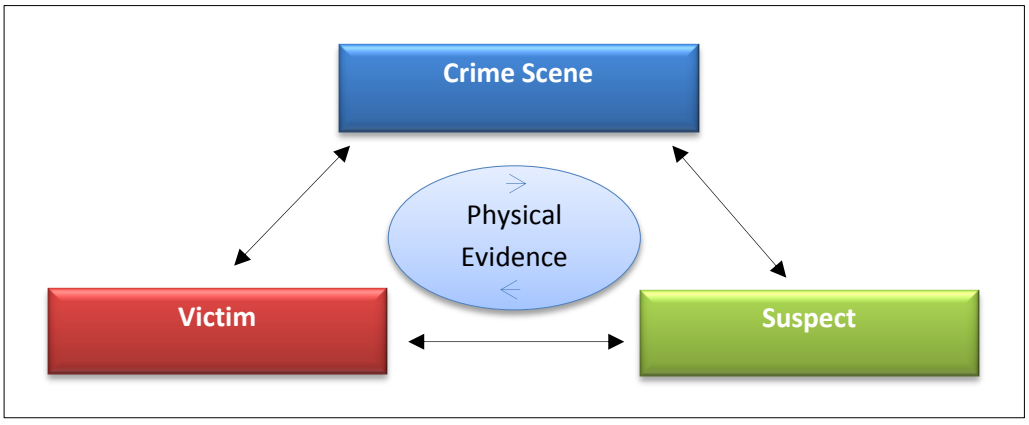


Figure 10, Locard's Exchange Principle

[33] Cited from (Casey, 2000) page 3, second paragraph
[34] Cited from (Casey, 2000) page 4, first paragraph

Digital evidence is a special type of physical evidence. Although it follows the same rules the digital evidence is harder to collect. Whereas physical evidence can be gathered by standardised approaches and techniques (e.g. collecting fingerprints and DNA samples,…), digital evidence requires novel concepts and methods. Investigators need the right tools at their disposal otherwise it will not be possible to gather and collect valid digital evidence.

According to scientist Casey[35], digital evidence has the following advantages over old-fashioned evidence:

- Digital evidence can be exactly duplicated and the copy can be examined as if it was the original.
- With the right tools it is very easy to determine whether digital evidence has been modified or manipulated by comparing with the original source.
- It is relatively difficult to destroy digital evidence. On some computer systems deleted data can be recovered from even overwritten storage devices.
- In the event criminals try to destroy digital evidence, copies can be sometimes obtained from systems which they are not aware of such as smartphones or other network devices.

Based on Professor David L. Carter[36], a valid categorisation of different types of cybercrime was established to efficiently separate different sorts of computer crime:

- Computer as the designated target (e.g. Computer intrusion)
- Computer used as criminal tool of the crime (e.g. credit card fraud)
- Computer as incidental to other crimes (e.g. child pornography or money laundering)
- Crimes associated with the prevalence of computers (e.g. copyright violation).

A typical computer forensic investigation follows in general always the same course of action. A computer crime incident happens and the local authorities

[35] Based on (Casey, 2000), page 4, last paragraph
[36] See (Carter, 1995) for more information

are informed and notified thereof. There can be a difference if the computer crime was committed against a computer system maintained by local authorities or if the incident was directed against a corporate system. In almost all of these situations the local authorities have to be informed that such a computer crime attack occurred[37]. In general computer forensic investigators (depends on the financial situation and organisational structure of law enforcement units) immediately commence their investigations to collect as much digital evidence and to limit the potential damage. Depending on the computer crime incident there are several different procedures how to perform such a computer forensic investigation properly.

The standard procedure normally referred to is the so-called SAP model. **SAP** stands for **S**ecure, **A**nalyse and **P**resent. The first step in a computer crime investigation is to seal all available digital evidence directly at the crime scene. The most important and valuable part (in terms of forensic investigations) of an affected computer system is the hard drive or any other storage device. Forensic investigators normally take a bit-stream copy of the affected HDD to exactly duplicate the running computer system. Because of the volatile memory of a computer system, often called RAM or cache, the affected machine should be never turned off as this could lead to the loss of crucial evidence.

Currently there are several forensic tools available which can easily make sealed and verified copies of working HDDs (i.e. EnCase, Ftk, Sleuth kit,...) and the corresponding memory data. This step in general is called the “Secure” part because all digital evidence is gathered and secured. Due to novel technological approaches this part is not very time-consuming. Although it still has to be performed by specialists to guarantee that all possible evidence was collected properly. It should be reminded that evidence does not only have to be located at the affected system but it can be often found within other peripherals as connected routers or NAS devices.

[37] For more information how to file a complaint follow this website: http://www.ic3.gov/complaint/default.aspx

The following “Analyse” section represents the most time-intensive part of a computer forensic investigation. Verification of the collected data can take more than several days and eventually it can occur that an investigator was looking for the wrong parameters which would result in repeating the entire process. Irrespective of the time-consuming process it also takes a highly educated expert to fulfil this step. Not only the investigator needs to have a broad knowledge about computer crimes, hacker attacks and software tools but he also needs to be familiar with hardware structure, system architectures and peripherals and all their related functionalities. A typical computer crime investigator has a much broader sense of computer science than an average computer specialist. The investigator cannot specialise in only one field of computer science, he has to be an expert in almost every field which makes it so difficult to recruit appropriate personnel.

In addition the investigator has to deal with another time-consuming process during this step: documentation. Documentation of evidence and all involved investigative steps is essential for a number of reasons. Especially for court cases the famous “chain of custody” has to be established whenever evidence is gathered or collected. If the documentation of an investigation is incomplete or includes logical errors the collected evidence may not be used within court proceedings. The documentation has to include all serial numbers and other technical details that can be used to specifically identify each item of evidence. Pictures of investigated computer system proved to be very useful especially for forensic investigations that take over a longer time period. In addition every access to collected digital evidence has to be recorded to eliminate the risks of losing or unintentional manipulating collected data.

In some cases digital evidence cannot be found directly within the computer system. In such situations investigators have to use all of their knowledge to retrieve and reconstruct data which was possibly destroyed or deleted. There are advanced techniques and technologies available which can achieve such objectives. Nevertheless the possible “hiding spots” for such data can be numerous, especially in terms of novel HDDs with several TB of disk space or other network attached storage devices. Another emerging challenge for

investigators is the recovery of encrypted digital evidence. Encryption software became more advanced over the last years so that law enforcement authorities do not have any chance to recover encrypted materials. TrueCrypt for instance is an open-source software that creates and maintains fully encrypted data containers which cannot be decrypted without the appropriate password key[38]. Another advantage of TrueCrypt is that it utilises different encryption algorithms at the same time to masquerade the content of a data container. Even entire HDDs with full operating systems can be easily encrypted by selecting the appropriate options. The only approach to successfully break such an encryption is the famous brute-force attack which will systematically try every possible password combination until the correct key is found. This approach starts to get more time-consuming with the difficulty and length of the designated password and the corresponding algorithms.

As the last step of the entire "Analysis" process is the full reconstruction of the "computer crime". All gathered and derived evidences support the reconstruction process. The ultimate goal for an investigator is to establish what happened and when precisely the crime occurred. Reconstructing all details surrounding the incident or break-in are often essential to understand what occurred, who caused the events, when, where, how and why[39].

The last step of a typical computer forensic investigation is called the "Present" phase. After successful identification and analysis of the computer crime incident the investigator has to present his results in an understandable way. Although this step of the process seems to be very simple and easy to accomplish, it still encounters a lot of difficulties. Due to the fact that investigators are highly trained and used to novel technologies, they often lack the ability of explaining technical findings and results in an plausible way. If for instance the collected evidence of an investigation leads to court proceedings all gathered information has to be presented in an understandable way for the

[38] Even the FBI was not able to break the encryption of a TrueCrypt volume after one year – follow the link for more information
http://www.webcitation.org/query?url=g1.globo.com/English/noticia/2010/06/not-even-fbi-can-de-crypt-files-daniel-dantas.html

[39] Based on (Casey, 2000) page 64, last paragraph

unskilled judge and jury. Technicians often face the problem that they cannot describe and explain technical approaches in such a clear way that non-technicians can follow.

Apart from this fundamental problem of understanding there is another problem of legislation. Every country in the world has its own legislation and jurisdiction. The problem for investigators is that computer crimes that are forbidden and prosecuted in one country can be completely legal in other one. Due to the fact that the internet represents an universal network without borders and boundaries many computer crime investigations end up with results which do not lead to a successful prosecution in court because of local and legal constrains.

4.1.2. Preparations for a Forensic Investigation

The preparations for a computer forensic investigation can influence the investigative outcome. The following tasks have to be conducted before even digital evidence is collected. Sometimes it can be very helpful to find possible answers from the victim himself (e.g. system administrator,…) or in general from a person of interest to the investigation[40].

The first task starts with “Identifying the Nature of the Case”. This includes whether the computer crime was conducted against computer systems within the private or the public sector. The nature of the case defines the following steps of the investigation process and types of resources and tools that are needed.

This leads directly to the next step, which aims to “Identify the type of computer system”. This step is necessary to recognise the affected computer system and determines the appropriate tools. Windows machines need a different set of investigative tools than UNIX systems for instance.

[40] Based on (Nelson, et al., 2006) page 159

Another important question is handled within the next step, which discusses whether the computer system can be seized or not. The ideal situation for forensic investigations is that all involved machines and systems can be seized at once and analysed within a laboratory environment. In most cases, machines cannot be removed from the crime scene as it would irreparably harm the running business or disrupt entire institutions. In such cases investigators have to create exact system copies of the affected machines that will be further processed and analysed.

Furthermore they have to investigate all other connected network devices that can possibly provide additional information about the computer crime. This can be a very time-consuming process depending on the size of the network and the amount of devices.

Another good strategy is to collect all possible log files in particular from root network devices such as routers, access points or firewalls. They can include crucial digital evidence which can lead the investigators directly to the responsible criminals.

4.1.3. Legal Framework

Before any formal models or any technical solutions can be discussed, an explicit border line has to be drawn. Within this paper only current Austrian regulations will be discussed and taken into consideration, as even the continental European diversity would exceed the scope of this research project.

According to the Austrian criminal procedure code ("Strafprozessordnung"[41]) during a court case there are several important steps that have to be taken into consideration. The first step is to identify the involved parties ("legal persons") and the competent court. There are several different types of courts in Austria which all have different authorities. Additionally, the main problem is to identify all involved people within legal proceedings, in particular in computer crime

[41] referenced to (Strafprozeßordnung, 2009)

cases. Very often it is extremely difficult to find the explicit offender, as novel techniques obstruct successful investigations.

The next important aspect for a successful court case is the law of evidence. The gathered evidence has to provide the necessary information to prove that a criminal act has occurred and who exactly committed the crime. Within computer crime cases it is often difficult to secure the evidence in an enduring way and avoid additional, mostly unintended manipulation of data. One common approach for this problem is to confiscate and seal all involved technical devices. However in cases where entire server farms are involved, it is impossible to shut down the entire system and transfer it to an examination site.

Digital evidence is fundamentally different to old-fashioned evidence like fingerprints or DNA. Digital evidence may be copied many times and computer science methods can prove that the copies are exactly the same as the original evidence through hashing techniques. How can a digital copy be used in court where original evidence is mandatory?

Smith and Bace[42] discuss in more detail court proceedings that questioned the authenticity of digital evidence which had been created, manipulated and stored on different types of computing systems, pointing out that more than 90% of today's information is created and stored in computer systems. Investigators of traditional crimes, homicide and child pornography are finding evidence secreted on computing devices. In those instances of physical crime, often information about the crime is recorded on the offender's computer. Computer data is readily replicated and many exact copies of the evidence may be preserved[43].

There is a clear lack of a more effective way to deal with this problem of evidence management. Except for the common problem of avoiding the manipulation of evidence, there must be a closed chain of evidence. A detailed log has to be administrated to confirm what happened to all systems and data,

[42] See (Bace, 2003) for more information
[43] Cited from (Armstrong, 2010)

who had access and could manipulate them or who could accidently have changed any information.

Additionally, the law of evidence takes testimonies into account and even deals with automated data analysis (“Rasterfahndung”), monitoring of telecommunication networks and even optical and acoustic observation of potential criminals using technical devices (“Lauschangriff”). All these legal actions can be initiated as a matter to secure the crime scene for possible investigations.

The final criminal proceedings are based on two different investigations. First, there is a preparatory proceeding before the entire case even gets to court. In Austria there is the possibility that the preparatory proceedings are initiated against an unknown offender. The aim is to identify all involved parties within such a case. As a next step, a preliminary hearing takes place to decide whether the investigated offenders can be accused or not. Only in the situation that such a hearing ends successfully, a court case will be commenced.

The detailed steps during a court case are very similar to other European countries and will therefore not be discussed in detail.

Another important note about the current legal framework in Austria is the constant evolution of classic computer crime legislation. In the early stages of computer crime legislation the main focus was on classical burglary or damage of property, such as the destruction of computers. With novel technological solutions and the broad acceptance of the internet, a completely new area of computer crime incidents evolved. Therefore the legal regulations had to be adapted to deal with these new circumstances. There were incidents where computers suddenly were misused by criminals and participated in global criminal acts. Who is responsible in the end? Is it possible to find the offenders or is it just the owner of the machine who is responsible? Legal systems had to deal with this new situation and novel laws were introduced.

For instance, before 1987 the intentional deletion of computer software by a third party was not an illegal act in Austria, as the full device that stored the program was not irrevocably destroyed. To solve this problem, the Austrian legislation enacted new provisions of law in 2002. New acts of crime were defined or modified within the Austrian criminal code ("Strafgesetzbuch - StGB"):

- The act on data corruption (§126a - "Datenbeschädigung")
- The act on fraudulent data misuse (§148a - "betrügerische Datenverarbeitung")
- The act on illegal access to computer systems (§118a - "Widerrechtlicher Zugriff auf ein Computersystem")
- The act on violating the telecommunication law (§119 - "Verletzung des Telekommunikationsgeheimnisses")
- The act on illegal eavesdropping (§119a - "Missbräuchliches Abfangen von Daten")
- The act on manipulating a computer system (§126b – „Störung der Funktionsfähigkeit eines Computersystems")
- The act on data misuse and illegal access (§126c - „Missbrauch von Computerprogrammen oder Zugangsdaten")
- The act on falsification of data (§225a "Datenfälschung").

In the following paragraphs the current Austrian provisions of law will be discussed in more detail which is necessary to fully understand the current legal framework.

4.1.3.1 The act on data corruption (§126a - "Datenbeschädigung")

Original law provision from the Austrian criminal code:

"§ 126a. (1) Wer einen anderen dadurch schädigt, dass er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst

unbrauchbar macht oder unterdrückt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer durch die Tat an den Daten einen 3 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen, wer einen 50 000 Euro übersteigenden Schaden herbeiführt, mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.“[44]

Translation found at the webpage of the European council’s initiative to fight cybercrime[45]:

“Section 126a (1) A person who causes damage to another person by altering, erasing or otherwise rendering useless or suppressing automation-aided processed, transmitted or entrusted data without being authorised to dispose of the data or to dispose of them alone, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

(2) A person who causes damage exceeding 2,000 Euro by the offence is to be sentenced to imprisonment up to two years or to pay a fine up to 360 day-fines; a person who causes damage exceeding 40,000 Euro is to be sentenced to imprisonment from 6 months to five years.

Description:
This law describes in detail what happens to a criminal that causes damage to another computer system. It does not only focus on the term damage but it also includes other related tasks which can result in damaged data like altering or erasing data.

4.1.3.2 The act on fraudulent data misuse (§148a - “betrügerische Datenverarbeitung”)

Original law provision from the Austrian criminal code:

[44] Taken from the Austrian criminal code (StGB)
[45] For more information follow (Seger, 2007)

"§ 148a. (1) Wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern, einen anderen dadurch am Vermögen schädigt, dass er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflusst, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer die Tat gewerbsmäßig begeht oder durch die Tat einen 3 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu drei Jahren, wer durch die Tat einen 50 000 Euro übersteigenden Schaden herbeiführt, mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen."

Translation found at the webpage of the European council's initiative to fight cybercrime[46]:

Section 148a (1) A person who, with the intent to enrich himself or a third person unlawfully, causes economic damage to another's property by influencing the result of automation-aided data processing through arrangement of the program, input, alteration or erasure of data (sect. 126a par. 2) or through other interference with the course of data processing, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

(2) A person who commits this offence professionally or causes damage exceeding 2,000 Euro is to be sentenced to imprisonment up to three years, a person who causes damage by committing the offence exceeding 40,000 Euro is to be sentenced to imprisonment from one year to ten years.

Description:
This act describes in detail the consequences of an illegal and fraudulent misuse of data processing.

[46] For more information follow (Seger, 2007)

4.1.3.3 The act on illegal access to computer systems (§118a - "Widerrechtlicher Zugriff auf ein Computersystem")

Original law provision from the Austrian criminal code:

„§ 118a. (1) Wer sich in der Absicht, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem verletzt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen."

Translation found at the webpage of the European council's initiative to fight cybercrime[47]:

Section 118a (1) A person who, with the intent to obtain information on data for himself or for another unauthorised person, which are stored in a computer system not being destined for him, and to make them available to another person for whom they are not destined by using them or making them public, and to procure in this way an economic gain for himself or another person or causing a disadvantage for another person, obtains the access to a computer system or to a part of such a system for which he is not permitted to dispose or not to dispose alone, by violating specific safety precautions within the computer system, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

[47] For more information follow (Seger, 2007)

(2) The offender is to be prosecuted only with the consent of the aggrieved party.

Description:

This law handles all illegal computer access which often occurs during hacking attempts. It describes in detail how an unlawful access looks like and what general conditions have to be met.

4.1.3.4 The act on violating the telecommunication law (§119 - "Verletzung des Telekommunikationsgeheimnisses")

Original law provision from the Austrian criminal code:

„§ 119. (1) Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen."

Translation found at the webpage of the European council's initiative to fight cybercrime[48]:

Section 119 (1) A person who, with the intent to obtain information not being destined for himself on communications transmitted through a telecommunication sect. 3 n.13 of the Telecommunication Act) or a computer system for himself or for another unauthorised person, attaches technical

[48] For more information follow (Seger, 2007)

means to the telecommunication device or the computer system or otherwise prepares such means to receive information and makes use of them, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

(2) The offender is to be prosecuted only with the consent of the aggrieved party.

Description:

This legislation describes the consequences of violating the strict Austrian telecommunication act. In terms of computer crimes all network attached devices and systems are protected by the Austrian telecommunication act as they interact all together over a connected communication line although the entire communication is conducted automatically.

4.1.3.5 The act on illegal eavesdropping (§119a - "Missbräuchliches Abfangen von Daten")

Original law provision from the Austrian criminal code:

„§ 119a. (1) Wer in der Absicht, sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, ist, wenn die Tat nicht nach § 119 mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen."

Translation found at the webpage of the European council's initiative to fight cybercrime[49]:

Section 119a (1) A person who, with the intent to obtain information on data for himself or for another unauthorised person, which are transmitted by a computer system not destined for him, and to make them available to another person for whom they are not destined by using them or making them public, and to procure in this way an economic gain for himself or another person or causing a disadvantage for another person, attaches technical means to the computer system or otherwise prepares such means to receive information and makes use of them, or intercepts the electromagnetic radiation of a computer system, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

(2) The offender is to be prosecuted only with the consent of the aggrieved party.

Description:
This act constitutes an extension of section 119. It describes the unlawful interception of data and the resulting consequences thereof. Computer hackers often try to eavesdrop a possible victim first, to find possible weaknesses within the communication system and to identify the designated target.

4.1.3.6 The act on manipulating a computer system (§126b – „Störung der Funktionsfähigkeit eines Computersystems")

Original provision from the Austrian criminal code:

„§ 126b. Wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt, ist, wenn die Tat nicht nach § 126a mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen."

[49] For more information follow (Seger, 2007)

Translation found at the webpage of the European council's initiative to fight cybercrime[50]:

Section 126b A person who interferes seriously with the functioning of a computer system for which he is not permitted to dispose or to dispose alone by feeding or transmitting data is to be sentenced, in case the offence is not punishable under section 126a, to imprisonment up to six months or to pay a fine up to 360 day-fines.

Description:
This act constitutes an extension of section 126 and deals with hacker attacks and computer crimes that mainly focus on disrupting computer systems (i.e. DDoS attacks).

4.1.3.7 The act of data misuse and illegal access (§126c - „Missbrauch von Computerprogrammen oder Zugangsdaten")

Original law provision from the Austrian criminal code:

„§ 126c. (1) Wer ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sich verschafft oder besitzt oder sonst zugänglich macht, dass sie zur Begehung einer der in Z 1 genannten strafbaren

[50] For more information follow (Seger, 2007)

Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
(2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig verhindert, dass das in Abs. 1 genannte Computerprogramm oder die damit vergleichbare Vorrichtung oder das Passwort, der Zugangscode oder die damit vergleichbaren Daten in der in den §§ 118a, 119, 119a, 126a, 126b oder 148a bezeichneten Weise gebraucht werden. Besteht die Gefahr eines solchen Gebrauches nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen."

Translation found at the webpage of the European council's initiative to fight cybercrime[51]:

Section 126c (1) Whoever produces, introduces, distributes, sells or otherwise makes accessible:

1. a computer program or a comparable equipment which has been obviously created or adapted due to its particular nature to commit an unlawful access to a computer system (sect. 118a), an infringement of the secrecy of telecommunications (sect. 119), an unlawful interception of data (sect. 119a), a damaging of data (sect. 126a) or an interference with the functioning of a computer system (sect. 126b), or
2. a computer pass word, an access code or comparable data rendering possible the access to a computer system or a part of it, with the intent that they will be used for the commitment of any criminal offence mentioned in para.1, is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

(2) A person shall not be punished under paragraph 1 who prevents voluntarily that the computer program mentioned in paragraph 1 or the comparable equipment or the pass word, the access code or the comparable data will not be used in a way mentioned in sections 118a, 119, 119a, 126a or 126b. If there is no danger of such a use or if it has been removed without an activity of the

[51] For more information follow (Seger, 2007)

offender, he shall not be punished in case he, unaware of that fact, makes voluntarily and seriously an effort to remove it.

Description:

This act constitutes an extensive addition to section 126 and deals with the misuse of computer programs and illegal access data. It describes typical virus incidents where the creator of the virus has to bear the consequences. It defines also access data like secret passwords or passphrases as old fashioned keys which guarantee that only authorised and legitimate users have access. Breaking those keys and gaining illegal access is comparable to breaking into someone's home or car.

4.1.3.8 The act on falsification of data (§225a "Datenfälschung")

Original law provision from the Austrian criminal code:

§ 225a. Wer durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten mit dem Vorsatz herstellt oder echte Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

Translation found at the webpage of the European council's initiative to fight cybercrime[52]:

Section 225a A person who produces false data by input, alteration, erasure or suppression of data or falsifies authentic data with the intent for using them legally as evidence of a right, legal relationship or fact is to be sentenced to imprisonment up to one year.

[52] For more information follow (Seger, 2007)

Description:

This law describes the act of falsification of data and all related consequences to this illegal act.

4.1.4. European Convention on Cybercrime

Figure 11, Official logo of the European Convention on Cybercrime

The European Union (EU) initiated in 2001 a convention on cybercrime which represents the first international treaty to fight with computer crimes committed via the Internet. All European member states agreed and signed this convention and commenced the ratification process which requires an adaption of the national binding law provisions.

"Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.[53]"

This convention was adopted not only by European experts but also with assistance of specialists from the United States of America, Canada, Japan and several other countries not located in Europe. The convention includes 48 articles which define all related aspects of cybercrime[54]. Currently 52 states signed this convention but only 30 countries already ratified it[55].It is very

[53] Taken from (Council of Europe, 2004)
[54] See (Seger, 2007) for more information
[55] Numbers taken from:
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

interesting to see that even countries outside Europe already ratified this convention like the USA or Japan. It has to be mentioned that almost every country has included its own reservations towards this convention to defend their national interests. For example the USA do not agree on the extradition of American criminals to other countries involved in a cybercrime attack clearly specified within the convention.

These national reservations form a legal threat to the whole convention as they can create legal loopholes which can be misused by criminals.

This convention is also used by a large number of countries worldwide as a guideline or model solution for extending local and national cybercrime legislations.

The first phase of this convention preparation was conducted in the timeframe between September 2006 and February 2009 where the main goal was to support countries worldwide in the implementation of the convention. The project was even supported by commercially oriented companies like Microsoft and McAfee.

During this timeframe the convention was established as the primary reference standard for Cybercrime legislation and created various cooperations at all levels including law enforcement institutions like Interpol or national police departments.

The second phase of this convention was started in March 2009 and aims to build on the momentum created during the first stage and to support more non-European countries with their cybercrime legislations.

It would expand the scope of this research project to analysis all countries who signed and ratified the convention and their correlating cybercrime regulations in detail but the following link leads to an informative overview for all participating countries:

http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp

4.1.5. Organisational Setting

The following paragraph analyses the current organisational setting in matters of “Computer Forensic” investigations.

Computer forensic investigations are mainly conducted by law enforcement institutions which examine computers and all connected peripherals to gather possible evidence and reconstruct the committed computer crime. In most cases the attacker uses sophisticated attack schemes to camouflage his real identity but in some incidents a computer forensic investigation ends up with the arrest of a potential criminal.

What are the several steps to achieve this goal?

Firstly a legal investigation has to be initiated before an investigator can even start his analysis. This step has to be authorised by legal authorities which eventually start an enormous bureaucratic mechanism. This process represents a very time-consuming and non-efficient step which is needed to fulfil all legal requirements. In the event there are any mistakes or errors at the beginning, the entire forensic investigation may be compromised and the gathered evidence subsequently rejected.

After the commencement of the process the investigators collect all computerised evidence at the crime scene and prepare a detailed documentation on all investigated items, including a list of other storage media, like CDs, DVDs and pen drives. They also have to create notes about the current circumstances, i.e. whether a computer or the monitor output was running when they discovered it. This procedure can be very crucial for the

whole investigation because it can contain explicit evidence about the computer crime.

The US “Department of Justice” prepared a document describing the proper acquisition of electronic evidence especially as a first responder. It is mainly intended for law enforcement departments and first responders at computer crime scenes. It discusses also in detail possible risks and procedures to successfully collect digital evidence[56].

As a following step a detailed forensic investigation is conducted on the gathered digital systems. Possible risks and obstacles which can influence the outcome of the investigation have to be identified and determined. In addition a forensic strategy has to be established, listing all steps needed to fulfil the investigation process.

To successfully examine possible evidence data, computer forensic examiners need well-equipped data laboratories which provide the facility and technological solutions required for forensic investigations. Due to the fact that there are several different combinations of possible computer systems, like different OS, technological interfaces or network connections it is very difficult to keep pace with novel technological changes. Therefore these laboratories are often owned and funded by legal departments as the costs for a private laboratory would be tremendous. Although it should be stressed that there are private owned laboratories which try to specialise in a particular field of forensic science like data recovery for instance[57].

After collecting data and gathering important digital evidence, a detailed case report has to be generated to summarise all findings. This information is decisive for other legal proceedings and can lead to a possible court case.

This overview of a typical forensic strategy describes properly the organisational setting. On one hand there is the need of highly trained and qualified

[56] See (US. Department of Justice, 2008) for more information
[57] Example of such privately-owned laboratory in the UK - http://www.disklabs.com

investigators who hold the knowledge how to collect evidence in the right way. On the other hand a well-equipped tech laboratory which provides the optimal environment for a computer forensic investigation is mandatory. The maintenance costs of such a tech laboratory are constantly growing due to the fact of the instant growth of novel technological solutions.

4.1.6. Technological Environment

After discussing the legal and organisation areas this subchapter will analyse the current technological environment.

Due to the fact that there many different computer systems and combinations of OS systems and developments, it is nearly impossible to have an ultimate software toolkit which can analyse and identify automatically every computer crime. In a perfect world this would represent the best and easiest way to deal with computer crimes. The current reality however is completely different.

The entire problem gets even more complicated when digital evidence has to be identified and examined. Due to the technological evolution, digital data can be found not only in obvious computer or server systems parts. Digital evidence can be stored in the following locations:

- Hardware
  - Mainboards
  - Hard drives
  - RAM modules
  - PCMCIA cards
  - Chip cards
- Entire systems
  - Client / Server / Middleware/ Host
  - Transaction servers
  - Backup devices
  - CCTV systems
  - Copying devices
  - Fax machines

  - Access devices (especially log files)
  - Mobile phones
  - Music players
- Peripherals
  - Printer
  - Scanner
- Phone systems (PBX)
  - Log files of dial numbers
- Mobile devices
  - PDAs
  - Mobile phones
  - Smartphones
- Date storage devices
  - Floppies
  - CDs /DVDs
  - Dongles
  - Pen drives
  - USB storage devices
- Client software
  - Email client
  - Office data
  - Internet browser
  - System logs
  - Dongles
- Server software
  - Services, Applications
  - Databases
  - Gateways
  - Domain Controllers
  - Log files
  - Access points

Computer data and digital evidence are usually very sensitive, that is why it is important to classify the different types of data first:

1. Volatile data:

Volatile data is information that will be lost after a system shuts down. It contains cache values, logs of the current network connections, all running processes and information about logged users.

2. Fragile data:

Fragile data contains information that is stored on a hard drive but changes its condition when it is accessed directly.

3. Temporary data:

Temporary data persists of information stored on a hard drive that can only be accessed under special conditions e.g. during the runtime of a program.

There are approaches to provide investigators software tools that can automatically investigate certain parts of a computer system. The following sections will present the most popular forensic computer programs that are used by law enforcement departments to support and accelerate computer forensic investigations.

4.1.6.1 EnCase by Guidance Software

Figure 12, official "EnCase" logo

EnCase is a computer forensics product produced by Guidance Software used to analyse digital media (for example in civil/criminal investigations, network investigations, data compliance and electronic discovery). The software is available to law enforcement agencies and corporations and is generally considered the de facto standard for criminal digital forensics evidence collection.

EnCase includes tools for data acquisition, file recovery, indexing/search and file parsing[58].

Encase represents the current state-of-the-art software toolkit for computer forensic investigations. It provides advanced search options, instant message and mail analysis, a special programming language called EnScript and extensive system file support[59]. In addition it includes a full set of different analysis and reporting features which support investigators during their inspections. Reporting and case management is implemented in EnCase as well as special acquisition and restoration functionalities.

Another huge advantage of EnCase is the standardised and well-documented software core which guarantees court acceptance of all gathered evidences. It can be crucial for court cases to provide certificates for all used software tools.

4.1.6.2 Forensics Toolkit by AccessData

Figure 13, screenshot of FTK 3.0 installer[60]

The Forensic Toolkit developed by AccessData is the other major tool within the forensic community. It provides similar search algorithm like EnCase but has less reporting functionalities. One huge advantage over Encase is the "Password Recovery Toolkit" which provides easy manner to use utility on any encrypted files.

[58] Cited from (Wikipedia)
[59] See (Guidance Software) for more information
[60] Screenshot taken from official brochure found at
http://accessdata.com/downloads/media/FTK3_QuickInstall.pdf

This toolkit is certified and the gathered evidence has court acceptance which makes this tool interesting for law enforcement authorities. One important drawback is the lack of any scripting language. It is not possible within FTK to prepare own scripts like complex search strings.

One big advantage of FTK is a more user-friendly GUI and the higher usability in comparison to EnCase. It provides a simpler user interface and has more static templates for typical investigations.

FTK represents a court-validated investigation tool which means that all generated results can be used in a court case.

4.1.6.3 Sleuth kit – Open Source Software

Figure 14, official Sleuth Kit logo

The Sleuth Kit is written in the programing language C and contains a library and collection of command line file and volume system forensic analysis tools. These tools allow examining the file systems of a suspect computer in a non-intrusive manner because they do not rely on the operating system. This forensic toolkit was developed for Windows and Unix platforms.

The volume system (media management) tools allow to examine the layout of disks and other media. The Sleuth Kit supports DOS partitions, BSD partitions (disk labels), Mac partitions, Sun slices (Volume Table of Contents), and GPT

disks. With these tools, it is possible to identify the exact locations of system partitions and extract them so that they can be analysed with an appropriate file system analysis tools[61].

The Sleuth Kit represents an open-source software toolkit that provides all needed components for a successful forensic investigation. Its main strength lies within the high compatibility of different file formats and the constant development of the open-source community. It is very common in use with privately owned companies because it is distributed under the "Common Public License"[62] which grants the permission to use it free of charge.

This software toolkit can extract information from different file systems like NTFS, FAT, ext2, ext3, UFS1 and UFS2. In addition there is an HTML-frontend called "Autopsy" which provides a graphical user interface to the command line investigation tools.

4.1.6.4 Summary of the technical environment

Currently there are hundreds of different forensic toolkits available on the market. In the end most of them provide similar functionalities but with different strengths and weaknesses. One program has a scripting compiler included, whereas the other one focuses on password recovery. Finally it always depends on the forensic investigation and the computer crime that defines the most suitable toolkit.

Another important point is the available support and involved community behind an available toolkit. The number of computer crimes is constantly evolving and the criminal attacks are getting more and more sophisticated. The investigators and tools used thereby always have to stay a step ahead of the activity of criminals. This is the biggest strength of the open-source solution described in section 4.1.6.3 because with a strong community the toolkit is constantly enhanced and refined which leads to faster updates and novel solutions.

[61] Taken from (The Sleuth Kit)
[62] See (The Opensource Inititative) for more information

4.2. Requirements

The following section analyses and discusses all relevant requirements for the conceptual model. Based on the finding in the last section all requirements will be specified and discussed. According to the actual situation the requirements will be analysed from three different points of view.

Firstly the legal requirements have to be discussed. In comparison to other European countries in terms of computer crimes and forensic the current legal framework in Austria is advanced. According to the Austrian criminal code several different computer crimes are already implemented within the laws and regulations. Nevertheless there are still some situations where the current law system is overstrained and the applicable law is not explicit enough. Another important challenge for the current law framework is the European diversification. Instead of defining the same laws and regulations for the entire European Union every country prepares its own set of laws. This leads to the difficult situation that some computer crimes are legal in some countries and illegal in other ones. Sweden for instance has different regulations for file sharing than England. Bittorrent-pages like thepiratebay.org would be immediately banned in the United Kingdom, while in contradiction in Sweden it is treated as a legitimate site although the legal status is a bit unclear[63]. This complex circumstance requires a big change within the European legal system.

In respect to this publication, all legal requirements are identified and have to be fulfilled. The current Austrian system allows forensic investigations with court-validated forensic tools. The adapted legal system guarantees that all gathered digital evidence can lead to court case with a prosecution of possible criminals.

The organisational requirements which have to be discussed are much more difficult to identify and not as obvious as the legal requirements for instance. On one hand it is rather clear that there is a need of a skilled and trained

[63] Follow this German Link - http://www.heise.de/newsticker/meldung/Schwedische-Piratenpartei-nimmt-The-Pirate-Bay-unter-ihre-Fittiche-1032801.html - for more information about the Pirate Bay.

professional who can conduct forensic investigations. Even with most advanced technological solutions, there must be a human investigator who is defining the investigation strategy and all other relevant processes.

What kinds of skills are needed for the investigator?

There is no general answer to this question because every computer crime is different and includes different technologies. There are computer crimes based on network technologies whereas others use flaws or errors within operating systems. A forensic investigator has to be trained in almost every area of computer science which makes it very difficult to find real experts. Another approach to support investigators will be the development of easy-to-use software toolkits which will require low technological skills. Nevertheless investigators and even judges in court still need the understanding of modern computer systems and technologies. Without this knowledge no satisfactory report can be generated and no criminals prosecuted.

These points lead to another organisational requirement to fully accomplish this research project. Judges and all involved personnel need to have the fundamental understanding of computer science and technologies. In addition there has to be the possibility to present all forensic findings during a court proceeding. There are enough examples in Germany for instance, where judges misunderstood technological solutions and declared illegal actions as legitimate [64]. Besides court cases, forensic investigators need appropriate environments where they can efficiently conduct their forensic analyses.

The last important requirement for this research project is located within the tech sector. As already analysed, there are several different forensic toolkits available. Some solutions are open-source, others are licensed which require a usage fee. However all programs have in common that a user has to be specially trained and instructed to achieve optimal results. Due to the high complexity of computer crimes and the following investigations, these

[64] See (Korosides, 2009) for more information

technological solutions are too complicate for average users. There is need for a simple and easy-to-use technical solution to support investigators in an easy and efficient way.

4.3. Conceptual Model

After analysing and discussing the actual situation, focusing on the legal, organizational and technological areas and defining the current requirements, the actual concept of this research project has to be presented and described in detail.

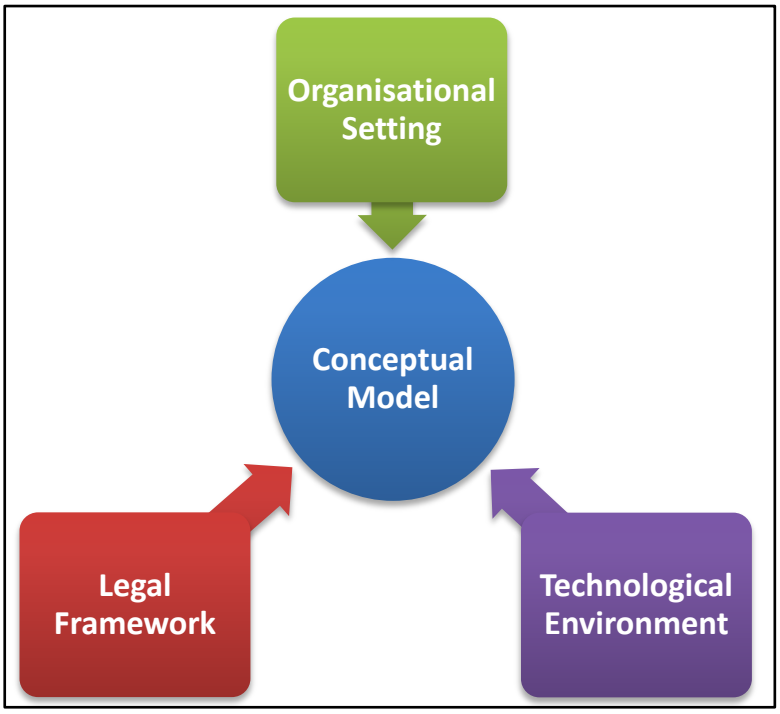


Figure 15, Components Relations

Modern criminal organizations have started to focus their current activities on novel digital technologies and have shifted their illegal actions into a virtual area. Several new different forms of threats have therefore evolved and finally legal authorities started slowly to adapt to this new situation. New police departments were founded (which are mainly focused on computer crime cases), new laws were introduced and special investigations initiated. The main drawback behind this adaptation process was and still is the legal system in

general (especially procedural rules) which overall remained untouched. Hackers, crackers and all kinds of digital criminals still have to stand up in court in front of a judge to finally get convicted. Technology in combination with these fundamental basics of executing the law has led to several new challenges.

First of all, the question is how to identify people who commit a crime or an illegal action within a virtual world. This problem was addressed by introducing the novel science of IT forensics. Specialists are trained to determine what kind of computer crime occurred, which actions were performed and most important who is responsible. Such information can be gathered through specialised software tools such as EnCase, FTK or SleuthKit[65].

The information overload resulting from the current analysis practice and the components in use, demand a tool supporting the process to overcome the obvious problems associated with the way in which information is provided by most of the current forensic analysis software. Besides analysing the digital evidence, there is need for a solution that generates results which can be used in legal court proceedings. Additionally, the tool support has to provide a goal-driven argumentation strategy to verify the gathered digital evidence.

To increase the efficiency of an automated solution, a positive step forward would be to establish a classification of possible cybercriminals. If it is possible to evaluate the level of experience of an attacker during an on-going investigation, maybe the entire analysis process could be finished faster and potentially also with more accurate results.

The main aim of this research project is to increase the efficiency and the quality of forensic investigations by providing an automated software tool to support investigators. Apart from the technological solution, examiners will be assisted with possible legal conjunctions to prepare a forensic case including an argumentation strategy for court proceedings.

[65] See chapter 4.1.6 for more information

The idea behind the conceptual model is to guide research by providing a visual representation of theoretical constructs (and variables) of interest[66].

The visual model is based on the extensive literature review and the desired research questions. The resulting objectives define the conceptual model. It cannot be assessed empirically, because it forms the basis of the research hypothesis.

In this research project the conceptual model consists of the three previously described areas which all define the required model. Based on the evaluation of these, the final model can be established.

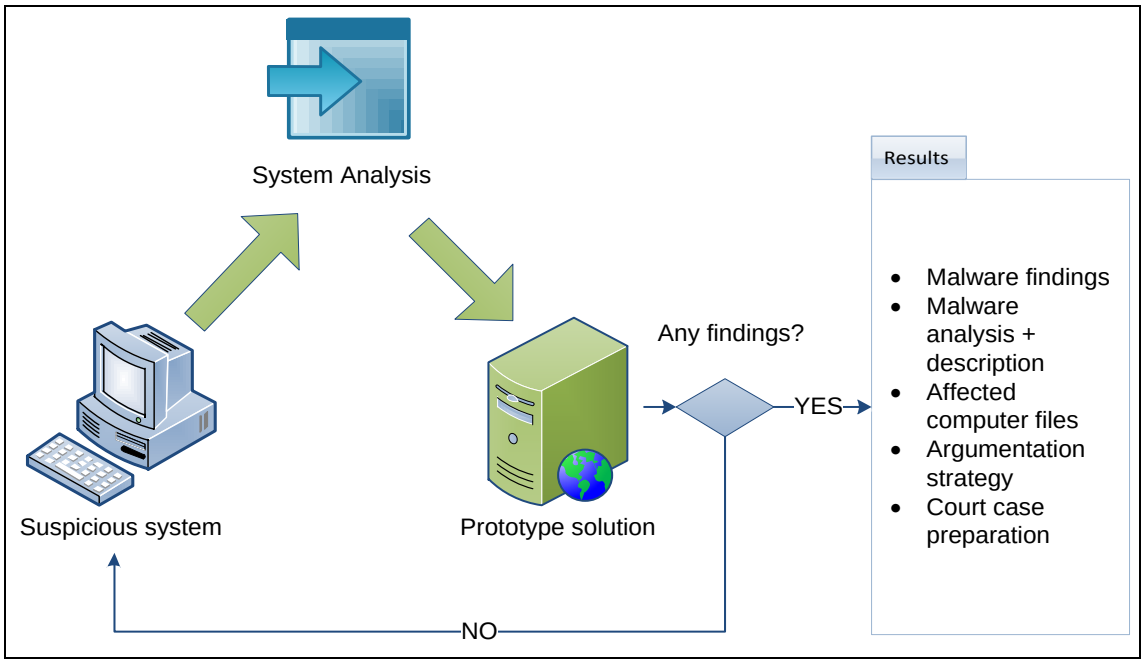


Figure 16, Conceptual Model

The conceptual model presented in Figure 16 visualises the research approach. Based on the organisational and legal situation an affected computer system can be identified. Although this appears to be a simple task, it already includes extensive scientific work to identify a specific system.

[66] Cited from „Conceptual Models“ – University of Stanford http://www.stanford.edu/group/ncpi/unspecified/student_assess_toolkit/conceptualModels.html#templates

There are several different intrusion detection systems that can filter and monitor network or computer attacks[67].

As a following step an automated system analysis has to be conducted. Forensic specialists are highly trained to investigate computer systems in order to conserve the running machine and not to manipulate possible crime evidence.

This step guarantees that the collected evidence and generated results will be valid and approved for a court case. EnCase for instance would be a best-practise solution which is widely used by law-enforcement units. In addition EnCase uses a well-formed scripting language which enhances the core with automated processes called EnScript.

These systems analyse hundreds of various generated information and form the basis for any on-going forensic investigation. The main problem for computer forensic experts is to identify the valuable information out of these result files, which will explain the type of infection and solve the committed computer criminal case.

To achieve such a goal an automated software solution is needed which will extract the important information and evaluate the outcome. In addition it should analyse the collected file list and identify possible malware infections.

At this point it is obvious that there must be some limitations of the functionality otherwise this research project will extend the defined scope. In the first phase only malware programs will be analysed but the prototype will have a modular structure which can be easily extendable.

Apart from the above the prototype will also identify possible infected system files and prepare an argumentation strategy that can be used within possible court cases.

[67] See (Whitman, et al., 2012) for more information

Short summary of the results which the prototype has to generate out of the system files:

- List of all affected system files
- Malware analysis of affected system files
- Additional description of malware infection
- Evaluating possible threat level (based on risk evaluation)
- Preparing argumentation strategy
- Gathering and presenting results as evidence for court cases.

All these steps and approaches define the conceptual model of this research project.

4.3.1. Argumentation Strategy

Considering that it would extend the scope of this research project to analyse the complete argumentation strategy for this thesis in every detail, a conjunction will be made to a very comprehensive analysis conducted by Colin James Armstrong BSc. MIS at the University of West Australia.

Mr Armstrong gathered advanced knowledge in the field of police investigations and computer forensic investigations which resulted in a highly advanced thesis called “A tactical management model of forensic evidence processes”[68]. This research project will be used as a framework to extend the collected ideas and results with the use of a technological prototype.

The author presents an extensive overview of current forensic strategies and techniques which will be referred in the following chapters.

Besides the different forensic approaches he develops a forensic investigation meta-model which is very valuable for the current research project. This meta-model will be used as the fundamental basis for the on-going research study.

[68] See (Armstrong, 2010) for more information

"The Forensic Evidence Meta Model (FEMM) is a representation of a holistic approach to the management of forensic evidence. Management of forensic evidence requires accommodating its many and varied aspects into a single model enabling a better understanding of the meanings derived from evidence, and the development of integrated systems for maintaining all of the special requirements for the safe preservation, storage and management of forensic evidence. [69]"

Apart from this advanced meta-model approach the author presents six disparate systems which have to be integrated to generate optimal results.

This research project was conducted with the same research methodology called "design research methodology" which provided the flexibility to adjust adequately the problem space, the solution approach and the design space according to the research project.

It has to be mentioned that the author conducted a very exhaustive interview session with three different perspectives groups (law enforcement group, followed by forensic scientists and then the judiciary group) to guarantee the completeness of his research. The progressive feedback provided effective means of evaluating drafts of the models as the project progressed. With immediate evaluation feedback by participating forensic evidence practitioners, prompt modifications and adjustments to the introduced model were possible.

4.4. Feasibility and Limitations

The feasibility of this research project is closely related to possible limitations of this study. It is one of the central questions which have to be addressed at the beginning of the project. Is it possible and feasible to generate the proposed approach?

[69] Quoted from (Armstrong, 2010)

The main problem with this approach can be divided into two separate sections. On one hand there is a technological implementation that faces several various difficulties. First of all it has to be identified how a computer forensic investigation can be accelerated. Every computer forensic examination is completely different. Due to the huge amount of different technologies involved and alternative computer crime incidents the investigation strategy looks different. It is not possible and technologically not feasible to develop a concept for each case. Therefore it was necessary to narrow down this research project which had to be more focused on special incidents and investigations. After identifying and analysing the main strategies and proceedings of common computer investigations the most interesting and promising area, appeared to be located in the field of malware programs[70].

Malware is a category of malicious code that includes viruses, worms and Trojan horses. Destructive malware will utilise popular communication tools to spread, including worms sent through email and instant messages, Trojan horses dropped from web sites and virus-infected files downloaded from peer-to-peer connections. Malware will also seek to exploit existing vulnerabilities on systems making their entry quiet and easy[71].

Malware is the general term of a wide range of malicious software that can infect and disturb the functionality of computers. They are often distributed by mail attachments or web applications that install local programs on the HDDs. The operating mode of malware programs is similar to known computer viruses. They can include Trojan programs (also known as Trojan horses) which seem to be legitimate programs at the first sight. However after direct inspection and analysis an illegitimate and harmful code can be identified which main aim is to damage the running computer system. Besides that, malware files can contain backdoor programs that enable security vulnerabilities to bypass normal authentication methods and to gain unrestricted access. Another type of dangerous packet load for malware programs can be identified and called as rootkits. The concept behind rootkits is to masquerade the real existence of any

[70] For more information see (Aquilina, et al., 2008)
[71] Citied from (Symantec)

dangerous code from the user. This is achieved by modifying the running OS system and changing the direct link paths of typically used computer programs by pointing to the malicious code first. This step guarantees that the malicious code is executed every time when the OS is booted up[72].

What is the motivation behind creating a malware program?

This is a difficult question which would require additional psychological knowledge to fully answer it. One of the most obvious causes is possible profit which can be made through malware programs by creators and hackers. Malware code can be either used as a spyware program to collect restricted data by possible key-logging programs which can record all keystrokes and send them back to the attacker. Another possibility is to activate possible backdoor exits of the affected victim computer that can finally turn this computer into a zombie machine. A zombie machine is a computer system which is controlled by an illegitimate user who is in full control of the computer system. This step is similar to a remote access but with the difference that the aim behind it, is to make use thereof in a criminal way. Zombie machines can be used for many different illegal computer crimes like spamming or participating in botnets that are conducting “Distributed Denial of Service” attacks[73]. All this activities have one major point in common: to generate as much profit as possible. For the completeness of this answer it has to be noted that there are several different types of hackers who have different motivations for their tasks. There are two main groups. On one hand there is the white-hat hacker group. They actually form the minority of hackers and try to identify possible security vulnerabilities and flaws. They create programs which are often called “Proof of Concepts”. These programs are often misinterpreted by the local media which presents those programs as new viruses or malwares. Instead the idea behind such proof-of-concepts is to demonstrate that there are accessible vulnerabilities within common computer systems and that there is need for a new solution or software update.

[72] For more information check (Skoudis, 2004)
[73] For more information see (Bielecki, 2007)

On the other hand the other group can be classified as black-hat hacker. These are the real criminals that try to exploit the technological vulnerabilities for their own advantage and profit[74].

How can be malware programs identified?

As already discussed in an earlier paragraph, malware programs completely masquerade their real purpose by pretending some other functionalities (e.g. browser extension, search helper,..). In the end it depends on the payload and functionality. In addition they can have several different stealth techniques to successfully masquerade themselves. This problem is similar to a typical virus infection scenario. How to identify this virtual plague?[75] The most common and practical approach is to identify possible signatures. These signatures provide the possibility to easily identify virus code and possible derivatives thereof. Almost every modern anti-virus scanner uses this mechanism and technique to analyse every executed program code on a computer system. The same approach is suitable for identifying potential malware programs. By checking and verifying possible signatures malware code can be analysed and identified.

How to get a list of signatures of known malware programs?

To answer this question it is important to understand the technology behind it. A signature of a malware program or worm has to be a very specific and definite data which can be used for identification. The problem is how to get a full and complete list of all malware programs. In a realistic approach it has to be admitted that it is impossible to create such an extensive list by a single person. In the scope of this research project there was a solution evaluated to solve this problem. There is an open-source community which is collecting signatures and typical file names of known malware programs. This list is constantly updated and available as a download file[76]. It provides detailed and well explained information about all known malware programs and their functionalities.

[74] For more information see (Harris, et al., 2008)
[75] For more information see (Szor, 2005)
[76] Data available at following link (Collins, et al.)

Nevertheless it also leads directly to another limitation of this research project. The collected file signatures are only valid for Windows OS machines. Other operating systems have different signatures and are not compatible with this list.

After identifying all technological requirements and limitations there is still another problem unsolved: the legal framework. The current European legal system is completely divided into different national aspects. Every country has its own legal and judicial system which is often incompatible with the system of a neighbouring country. There is no global European or world-wide judicial system which every country has to obey. Therefore this research has to introduce some local constrains. Due to local factors this research will mainly discuss and analyse only Austrian law. All legal aspects will be described and explained according to the Austrian jurisdiction.

4.5. Summary

This chapter started with the actual and current situation related with computer forensic investigations. It analysed a typical forensic process and the current Austrian legal framework. In addition the Austrian jurisdiction was explained in more detail and the most appropriate laws identified. Besides the legal position there was an overview of the current organisational and technological environment which included a list of current forensic solutions.

Additionally all requirements were investigated and a conceptual model was defined and presented. To achieve all predefined research goals a feasibility study was conducted which identified possible limitations discussed within this chapter. These had to be analysed and recognised to guarantee the success of this research project.

Finally this conceptual model will be used as a framework to build a technological prototype for further examination of the complete research idea.

5. Prototype Development

This chapter describes the technological solution developed for this research project. As already identified in chapter 4.1.6 there is need for an automated system which is capable to support a computer forensic investigation.

The following paragraphs will describe the functionality of this prototype in more detail. Besides it will discuss the legal aspects, the technical realization and related use-case diagrams. At the end of this paragraph a novel extension which was developed to support investigators during analysing and evaluating results will be introduced.

5.1. Introduction

As already specified in several chapters before the main idea behind this research project is to verify and to create an automated solution to support computer forensic investigators. The outcome of this project is a prototype application called “CFAA” (“Computer Forensic Analyser and Advisor”) which analyses the generated output of EnCase investigations and checks for a possible malware infection by comparing the investigated system files with a complete malware list. The generated results are prepared and formatted in an easy-to-understand way that even people who are not familiar with computer systems can understand. In addition it prepares an automated argumentation strategy according to the Austrian law.

The results generated by EnCase are needed to guarantee the completeness of the system scan. There are many different file scanners[77] available but none of them has the advanced scanning technology included in EnCase. EnCase has the capability of identifying data files that are protected or even hidden in a not

[77] See http://www.kaspersky.com/scanforvirus or http://www.virustotal.com/

partitioned area of HDDs[78]. With this advanced searching capabilities every file found on the analysed machine can be located and secured. The gathered results can be exported through a standardised interface into the CFAA application and used for further investigations.

Currently the prototype focuses mainly on the identification of possible malware programs which can infect a running computer system. Due to the modular structure of this prototype, additional improvements and advanced developments can be added easily to adjust to novel crime scenarios.

In addition to the technical implementation there is a need to classify a typical hacker and the possible threat level of an attack. Details about this classification will be discussed at the end of this chapter which will include an overview of the current hacker motivation. The last paragraph will introduce a novel extension already implemented within the CFAA prototype to support investigators during their analyses.

5.2. Legal Aspects

Before the technical implementation will be addressed all legal aspects have to be clarified first. According to the Austrian criminal code every procedure of taking evidence needs to identify five different main points:

- WHAT was the computer crime incident?
- WHERE did the computer crime incident occur?
- WHEN did the computer crime incident occur?
- HOW was the computer crime committed?
- WHO committed the computer crime?

All five key questions have to be answered to identify and possibly convict a criminal. In the following paragraph all five questions will be discussed in more detail to identify possible drawbacks.

[78] Follow link http://www.guidancesoftware.com/WorkArea/DownloadAsset.aspx?id=671 for more information

5.2.1. Procedure of Taking Evidence

As already identified in the paragraph before five main questions have to be addressed to end up with a successful court case in Austria. First there must be an identification of a computer crime incident. This seems to be a simple and straight forward task but novel computer crimes are masqueraded in such sophisticated ways that even system administrators do not recognise them. There are attempts which try to disguise these incidents as average tasks on a system platform[79]. Those occurrences make it very difficult for investigators because they do not have a starting point to look at. This analysis goes hand-in-hand with the definition of the crime scene (which answers the WHAT & WHERE question!).

After identifying the possible computer crime scene the exact timestamp has to be specified. Due to fact that modern computer systems work with their own system clocks it has to be verified at what exact moment (timestamp) the incident occurred. In addition all related system clocks have to be checked and verified that their functionality was not manipulated[80].

The next step is to identify how the computer crime occurred. This requires the entire reconstruction of the computer crime incident by a forensic expert. The investigator has to identify the type of attack, all involved tools and techniques used during the committed crime and the possible damage caused by the criminal. From the forensic point of view, this is the most time-consuming step. Due to the huge amount of different types of computer crime attacks the investigator has to check all different possibilities. Every detail can be crucial for the outcome of a court case and has to be identified precisely.

The last step within preparing a court case and collecting all evidence is to identify the suspicious criminal who is responsible for the entire computer crime occurrence. From the computer forensic perspective this is a very difficult

[79] For more information see (Casey, 2002)
[80] See (Vacca, 2005) for more information

question to answer. The main difference between traditional criminal incidents and computer crimes is the trace left by a criminal at the crime scene. The major evidence within the computerised world is not an old-fashioned "fingerprint" but a possible IP address which is still in the end nothing more like a telephone number. It can be registered to a real physical person (in a lucky situation) but it still provides no information about the person behind the IP address/computer responsible for the computer crime.

A legal case is a dispute between opposing parties resolved in court by a judge or jury[81]. The Austrian court system works exactly the same. On one side there is a defendant and on the other an accuser. Within a criminal case the situation is slightly different. Instead of a private accuser the defendant is charged by a governmental officer called prosecutor who is using all collected evidence (5 main questions). The main problem is to identify a physical human being who can be held reliable and judged for the committed crimes. According to the Austrian jurisdiction there is a requirement that the defendant has to be a natural person. In case of a legal person it is in general represented by an appropriate natural person authorised to its representation. Looking now at computer forensic investigations it is impossible to sue just an IP address or the owner of the address (who in most cases does not even know that his internet access or computer system was misused to commit a computer crime). Locating an exact person is one of the most challenging parts.

The next step is to see whether the person can be prosecuted in his own country or if he has to be transferred to the location where the computer crime was committed. The normal procedure is to accuse someone where the crime happened but how should this be possible if the computer criminal sits thousands of kilometres away from the crime scene? Another problem with such a situation is that almost every country in the world has its own jurisdiction system. This can lead to the obscure situation that illegal computer crimes committed in one country are completely legal in another one[82]. Modern computer crimes do not know any country borders or other geographical

[81] Cited from http://en.wikipedia.org/wiki/Legal_case
[82] See (Pontell, et al., 2007) for more information

limitations. In most cases it is enough to be connected to the internet which makes the computer system reachable for cybercriminals.

In the end all five main questions (What, Where, When, How & Who) have to be addressed and answered before any court proceedings can be initiated. What are the possible allegations that can be charged by a governmental prosecutor?

In chapter 4.1.3 the Austrian criminal code and the related laws are already discussed in detail. These laws are also appropriate for computer crimes committed through automated malware programs. The following elements of crime can apply to possible malware attacks:

- §118a – Illegal access to computer systems[83] → Backdoor functionality
- §119a – Illegal eavesdropping →Keylogger Programs
- §126a – Data corruption →Damaging running computer system (malicious code)
- §126b – Computer malfunctioning →Changing algorithms or runtime environments on a running computer system (malicious code)
- §126c – Data misuse → Keylogger Programs
- §225a – Data falsification → Changing computer data (malicious code)

In the end it is necessary for a court proceeding to identify the corresponding laws and regulations according to the investigated computer crime.

How should such a technological solution look like that could be capable of answering all these questions automatically? The answer for this question will be investigated within the following paragraph.

[83] See section 4.1.3.3 for more information

5.3. System Design

Before any advanced technical implementation can be started, the system architecture has to be defined first.

The proposed and discussed system consists of several different components. Below is an overview of the components and their corresponding relations.

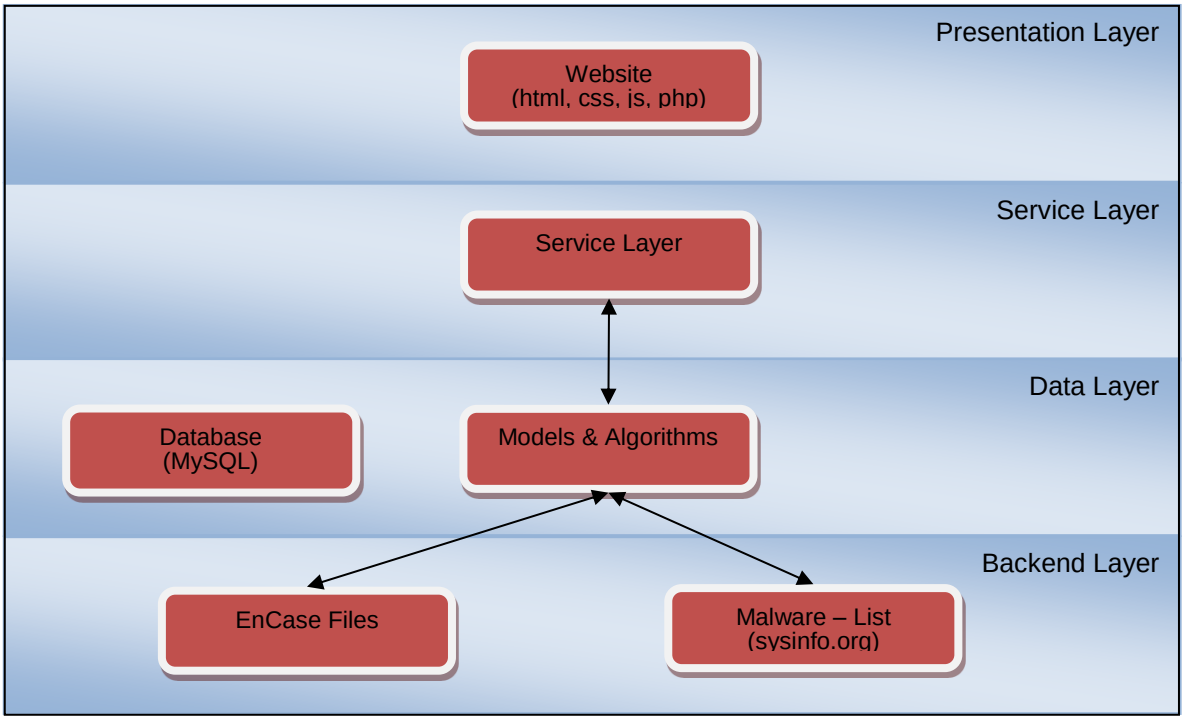


Figure 17, System Architecture Overview

The “Backend Layer” includes two main components. The first handles the EnCase result files and stores all viable information in the database. The second component is the automated malware-list collector. This information is mandatory for the functionality of this implementation.

The “Data Layer” utilises two main components: On one hand there is the database which stores and provides all collected information. It supports the identification process with all available information. On the other one there are all developed models and algorithms which are initiated during an investigation.

This component provides a way to define different models for the forensic investigation. It can be used to extend the technical functionality by introducing additional search algorithms.

The next component described will be the “Service Layer”. The “Service Layer” handles all the database operations and the communication between the website and the stored system data.

The last involved component is the website itself which is located within the presentation layer. The website presents all interfaces and results in a graphical way. The website consists of three pages which all need authorisations:

- Administration Page: This page contains all administrative functionalities like updating the malware list or adding additional users
- Investigation Page: This page initiates the forensic investigation. It requires importing the generated EnCase results. Afterwards it evaluates all collected data and generates a result file.
- Result Page: This page presents all generated and collected results in a graphical way. The results are visualised with the help of additional web utilities.

5.4. Technical Realisation

After identifying the legal aspects of computer forensic investigations according to the Austrian law, a technological prototype was defined and implemented to achieve all assigned goals.

The technical requirements for the prototype can be simply identified within the following definitions: Availability, Usability, Modularity and Security.

One key aspect of this prototype was to develop a system which can be accessed from all different client systems at any time regardless of the current location.

Another important aspect of this prototype development is usability. The goal is to create a system that can be easily accessed by system users without any additional knowledge or specialisation. In addition there should be no limitation to only one main operating system or special application. The prototype has to be accessible by most known computer systems and provide at least half of the designated functionalities.

Modularity plays a crucial role within every software development process. There must be the possibility to extend the functionality of a software tool by introducing additional modules. Those expansions need pre-defined interfaces which guarantee the flawless communication between different functionalities.

The last key feature of this prototype is the security aspect. Considering that the main functionality of this prototype lies within investigating forensic computer crimes it has to provide the highest level of security. It has to apply also to all known standards to provide additional help within law enforcement operations.

The following paragraphs will explain in more detail all involved technical components of the developed prototype called CFAA. Afterwards the CFAA functionality will be explained and described.

5.4.1. CFAA - an Automated Forensic Support System

The need for an automated system which is capable of supporting a computer forensic investigation was already identified within the previous chapters. This was the initial motivation to create the technological prototype called “Computer Forensic Analyser and Advisor” (CFAA) which analyses the generated output of EnCase investigations.

At this stage of research it only focuses on the identification of possible malware programs which can affect a running computer system. Due to the modular structure of this prototype, additional improvements and advanced developments can easily be added to adjust to newly developing crime scenarios.

In addition to analysing the generated metadata results extracted from EnCase, CFAA also tries to provide the investigator with additional information about the running investigation. The given advice can even lead to a complete restart of the entire investigation process due to the lack of required information or new plausible conclusions.

The CFAA prototype already includes a possible threat analysis component which tries to determine the knowledge level of a hacker. If for instance the threat scenario proves to be on a very high level (a black hat hacker for instance) the entire investigation and analysis process will have to be done in a much deeper and broader way[84].

5.4.2. System Overview

After evaluating different prototype solutions like several stand-alone applications, the decision was taken to develop a web-application which can be accessed by all different mobile and stationary computer systems. The main advantage of such a development is that it is completely independent from the operating system and that the only need for full access is an average standardised web-browser which is capable of simple JavaScript operations.

The following figure shows the entire CFAA technical architecture in accordance with the defined requirements. It persists of four different technical solutions which will be described in the following sections.

The prototype consists of a PHP Server connected to a MySQL database that stores all valid information. Every CFAA analysis is stored within the MySQL database to provide solid results and to increase the reporting functionalities.

[84] See section “5.6 - Classification of Cybercriminals“ for more information.

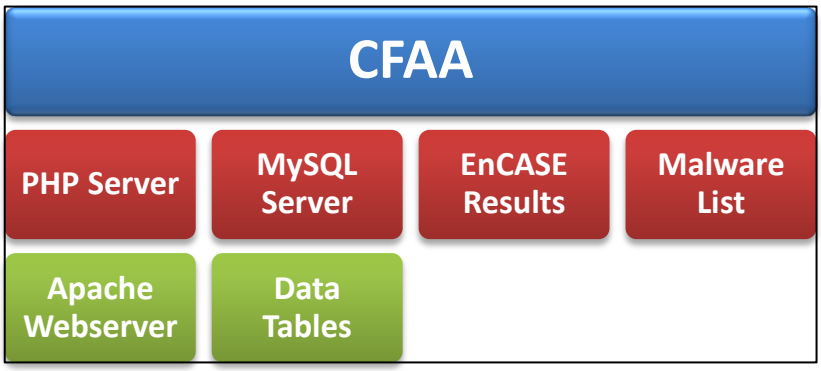


Figure 18, CFAA Functional Architecture

The entire CFAA functionality is written in PHP, a server-side programming language. The use of industry standard software guarantees an efficient solution with constant system updates. In addition, it can be easily installed and maintained, what should help to reduce the operating costs of the developed system.

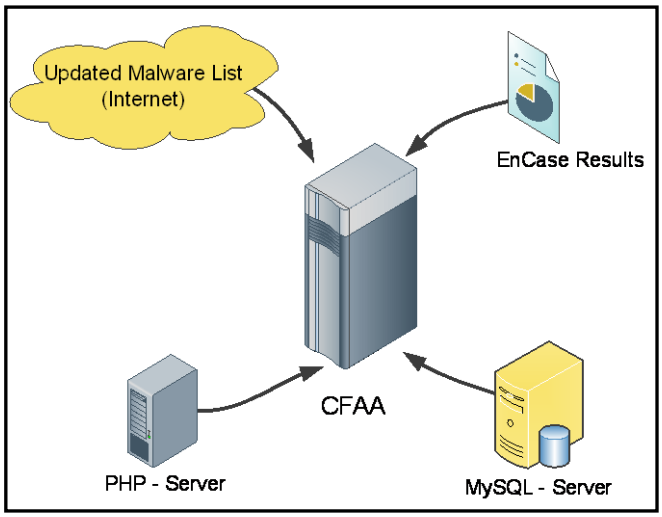


Figure 19, CFAA Prototype Architecture

Besides the analysis functionality, CFAA also includes an automated feature to gather the current list of known malware programs. This list is obtained from a saved as a text file at the CFAA server. In case the list should be outdated, a new list can be automatically acquired over the Internet.

5.4.2.1 PHP – Server System

All conducted tech evaluations showed that the server-side programming language PHP provides all needed functionalities. The main advantage of PHP lies within the server-side calculation of prepared algorithms which reduces the required computation power on the client's side. Besides PHP is developed and supported by the Open Source community and released under the PHP license which permits educational work[85].

The main functionality of PHP can be described as a typical server-side solution. The special PHP code is generated and stored at a standardised web-server with activated PHP functionality (i.e. Apache web-server + PHP module). When a http request is sent to the web-server the PHP server executes the code and presents the output in a standardised html form. This process makes it exceptionally easy to modify the content for various types of clients.

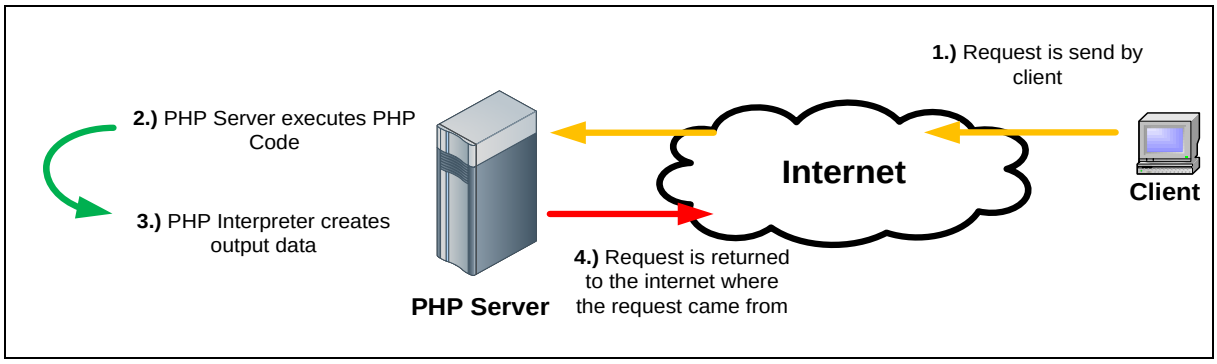


Figure 20, PHP functionality

Nevertheless it has to be mentioned that PHP includes some technical limitations. The most obvious one is the computational power of the server system. If many PHP scripts are executed at the same time, the responsiveness of the server can be limited and running calculations delayed. Apart from the above there are additionally voices within the PHP community that raise

[85] Follow this link for additional information about the PHP license - http://www.php.net/license/

concern about the security implementations of PHP with regard to the PHP parser. As a consequence of these concerns the PHPIDS application was developed to avoid any illegal actions and criminal intruders[86].

5.4.2.2 MySQL – Database Server

MySQL is a relational database management system which was published under the GNU General Public License[87]. This agreement guarantees the free of charge use of this software tool.

MySQL was mainly written in C and C++ and provides one of the most popular database systems. It uses the standardised SQL language for database actions and works on many different system platforms like Windows, Unix, Solaris and many more.

In addition it includes multiple storage engines like commercial solutions (i.e. IBM DB2) or native solutions (i.e. MyISAM) where the user can decide which functionality he needs or prefers.

"MySQL is used in some of the most frequently visited web sites on the Internet, including Flickr, Nokia, YouTube, Wikipedia, Google and Facebook."[88]

The main strengths of MySQL are located within the robustness of its database system and the continual development and support through the open-source community. In addition the MySQL development team has become a subsidiary of Oracle and focuses now mainly on business developments which ensures the further maintenance of MySQL.

Within the developed prototype the MySQL server system hosts three different data tables. The most obvious one is the user list which is needed to control

[86] See (Heidenreich, et al.) for additional information about PHPIDS.
[87] See (Free software Foundation) for more information.
[88] Cited from http://en.wikipedia.org/wiki/MySQL, those companies represent the business leader of their own industry sectors

user access to the application. It stores all required user information such as username, password and authorisation level.

The second table includes the current malware list which is obtained from the sysinfo.org homepage[89]. The malware list is constantly updated and loaded into the database which guarantees the persistent completeness.

The last table includes all valid information extracted from the generated Encase file[90] like filenames, timestamps, file sizes and access parameters.

The following Figure 21 gives a graphical representation of the MySQL tables' structure used for the CFAA prototype.

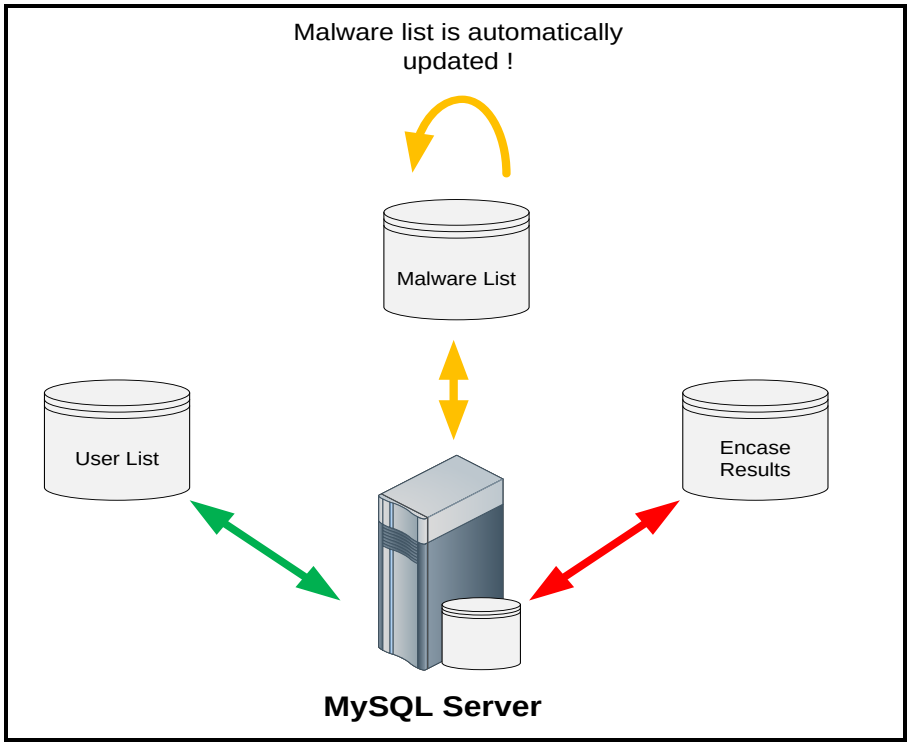


Figure 21, MySQL table structure for CFAA prototype

[89] See (Sysinfo.org) for more information
[90] See section 5.4.2.3 for more detail information.

5.4.2.3 EnCase – Result Files

Before a fundamental CFAA investigation can be initiated, an extensive EnCase investigation has to be conducted first. Based on the outcome of the analysis a result file has to be generated and subsequently imported into the CFAA prototype. This step finally starts the analysing functionality of CFAA and it automatically tries to identify and determine any suspicious files or processes.

As already described within section 4.1.6.1 EnCase represents the current state-of-the-art forensic software toolkit which is used by many law enforcement agencies in the world. In addition it provides a comprehensive documentation and automated interfaces which support extensive data export.

For the CFAA prototype a typical EnCase forensic investigation is initiated. A suspicious computer system is sealed and examined. During an average forensic investigation several different parameters are identified depending on the forensic starting point.

EnCase includes very advanced search algorithms which are capable of analysing disk partitions that are masqueraded and hidden from the user's view. It can also automatically analyse and investigate specified cache locations or even hex variables.

All these variables and parameters can be easily exported into a typical txt file as specified in Figure 22.

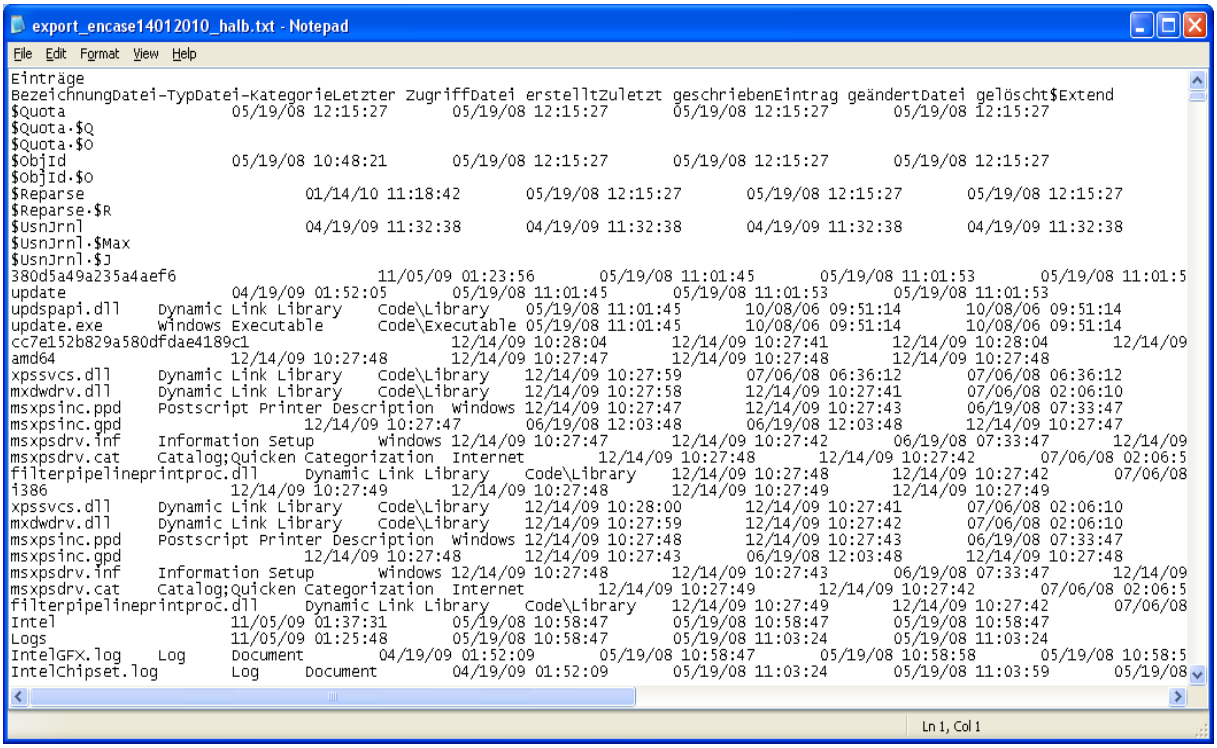


Figure 22, example of EnCase result file

Following parameters are mandatory for the CFAA functionality and must be included within the export file.

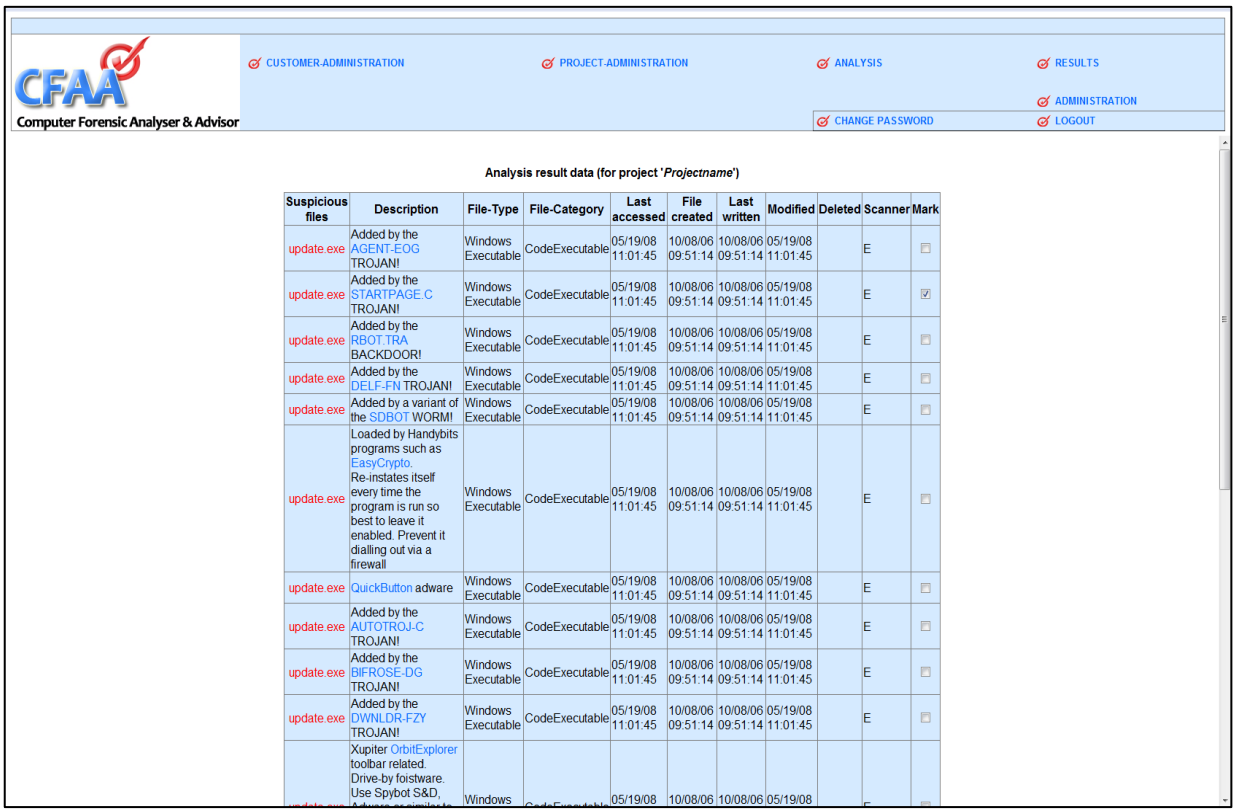
Name	*Description*
• File description	This field includes a distinct name of the data
• Data type	This field defines the data type like “Windows Executable” or “Text”
• Data category	This field defines the data category like “Document”, “Shortcut” or “Temporary File”
• Last accessed	This field specifies when the data was last accessed.
• Data creation	This field defines when the data was created
• Last written	This field defines when the data was last written
• Data changed	This field defines when the data was last changed
• Data deleted	This field defines when the data was deleted

Figure 23, mandatory parameters for CFAA functionality

The main difficulty within a forensic investigation is to determine the exact file list with all related access logs. The most obvious approach to collect such evidence is to examine the automated log system which is included in every modern operating system. What happens if information is compromised by an intruder and manipulated? It is the responsibility of the investigator to find an adequate log list as otherwise he will not be able to reconstruct the committed computer crime.

5.5. CFAA – Functionality

The CFAA prototype first requires the user to have access to exported results of an EnCase investigation. These results files are afterwards imported into the CFAA framework. This step initialises the automated analysis functionality of CFAA. The current functionality of CFAA attempts to identify the existence of any suspicious files or processes.



Suspicious files	Description	File-Type	File-Category	Last accessed	File created	Last written	Modified	Deleted	Scanner	Mark
update.exe	Added by the AGENT-EOG TROJAN!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	
update.exe	Added by the STARTPAGE.C TROJAN!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☑
update.exe	Added by the RBOT.TRA BACKDOOR!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	
update.exe	Added by the DELF-FN TROJAN!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	
update.exe	Added by a variant of the SDBOT WORM!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	
update.exe	Loaded by Handybits programs such as EasyCrypto. Re-instates itself every time the program is run so best to leave it enabled. Prevent it dialling out via a firewall	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	
update.exe	QuickButton adware	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	
update.exe	Added by the AUTOTROJ-C TROJAN!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	
update.exe	Added by the BIFROSE-DG TROJAN!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	
update.exe	Added by the DWNLDR-FZY TROJAN!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	
	Xupiter OrbitExplorer toolbar related. Drive-by foistware. Use Spybot S&D.	Windows		05/19/08	10/08/06	10/08/06	05/19/08			

Figure 24, CFAA Analysis Results

In addition to the EnCase file an antivirus result file (generated through an antivirus system scan) can be uploaded into system as well in order to verify that all suspicious files are checked properly. In the first stage of development it only focuses on malicious programs (e.g. malware). A sufficient list of known malware programs is obtained and updated from the Internet (e.g. www.sysinfo.org), which helps to guarantee that the information is relevant and complete. Based on all the given inputs the CFAA prototype tries to automatically identify any suspicious software and provides the investigator with

additional information as can be seen in Figure 24. If a malware program is identified, a detailed description of the program and the given functionality are presented to the investigator. Currently at this stage of development the visualisation of malicious software is limited to an extensive table view which contains all necessary information. As well as this feature, CFAA can also create advice to increase and focus the investigation on certain and suspicious parts of the affected system (e.g. network logs or access logs).

The main reason for CFAA requiring and functioning on the outputs of EnCase, is to allow the tool to be easily integrated into existing forensic analysis processes and also to allow a division of work. For instance, a trained investigator can perform a preliminary investigation of a suspect's computer within EnCase. The outputs of these preliminary investigations can subsequently be imported into the CFAA system, which will run through an automated analysis and present these results to less skilled (or at least those not trained in the use of EnCase) investigator.

This division of tasks allows trained analysts to perform faster 'overview' investigations and present these results to non-technically trained investigators for discussions. This approach of separated workload enables the highly skilled investigators to focus on more complicated cases, whilst the less experienced investigators can browse the 'overview' results in order to identify the events on a system that lead to the criminal activity.

5.5.1. CFAA – Use-Case diagram

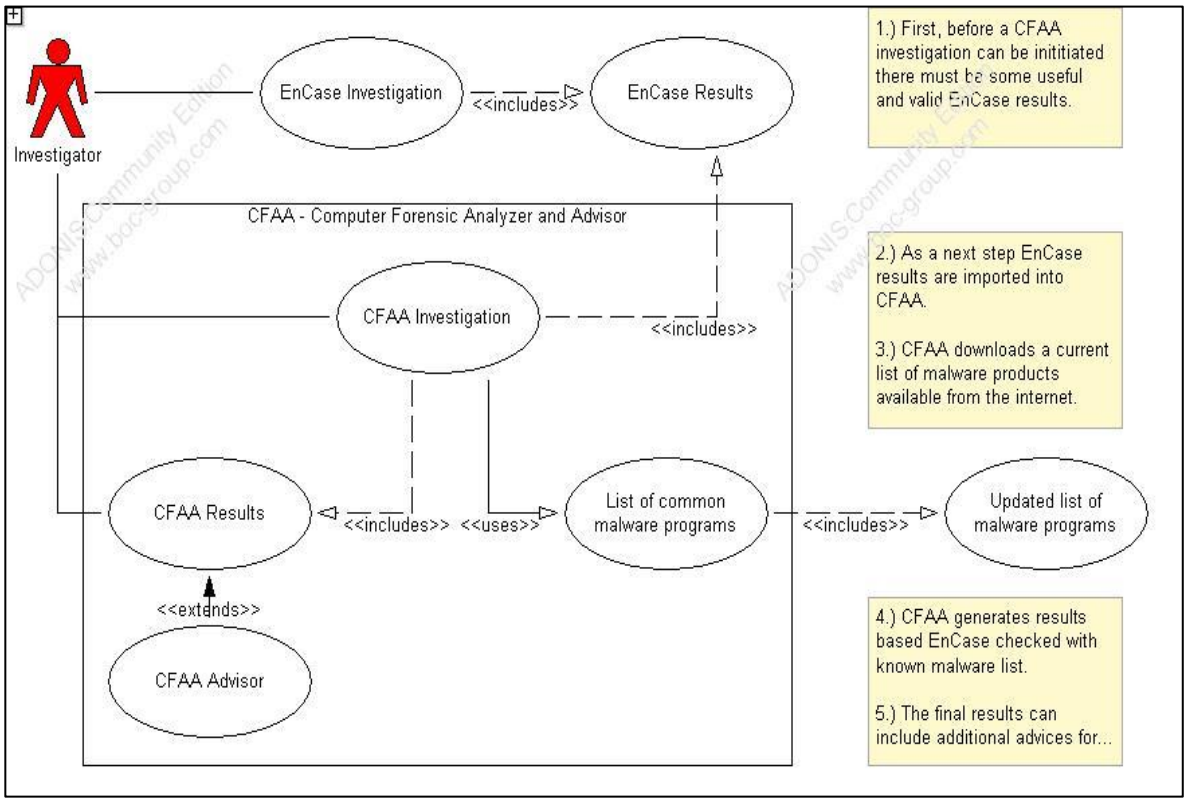


Figure 25, CFAA functionality displayed within a use-case diagram

The above Figure 25 illustrates the CFAA functionality with a detailed use-case diagram.

At the beginning of every CFAA investigation a standardised EnCase analysis has to be performed first. EnCase is capable of identifying all computer files on a system through an advanced search algorithm. It can investigate all running computer processes on an active machine and even initiate mail searches with the specified mail context.

All gathered results can be exported into a traditional txt-file. The detailed structure of the export file was already explained in section 5.4.2.3.

After generating an EnCase log file the CFAA prototype can be activated and

the malware investigation initiated. It is mandatory for a new investigation to designate the investigator, explain the computer crime incident and specify the date of intrusion. This information will be used for the printed report generated by the CFAA prototype.

As a next step the EnCase file has to be imported into the prototype file system. This is handled through a standardised html upload which triggers a predefined PHP subpage. The PHP script loads the entire txt-file onto the webserver and analyses the content. Because of the predefined structure of the export file the information can be separated into several different columns which enables the possibility of useful database storage. The main advantage of databases is that they can store thousands of different values which can be used for automated process in a very time-efficient manner. All gathered results are automatically inserted in adequate corresponding columns of the MySQL database and safely stored.

One technological problem which aroused during the test stage of the prototype was the limited amount of insert actions within a specific time period. After adjusting the PHP configuration file (php.ini) this handicap could be resolved. In the end of the upload process the txt file is deleted from the server to ensure no garbage collection on the running web system.

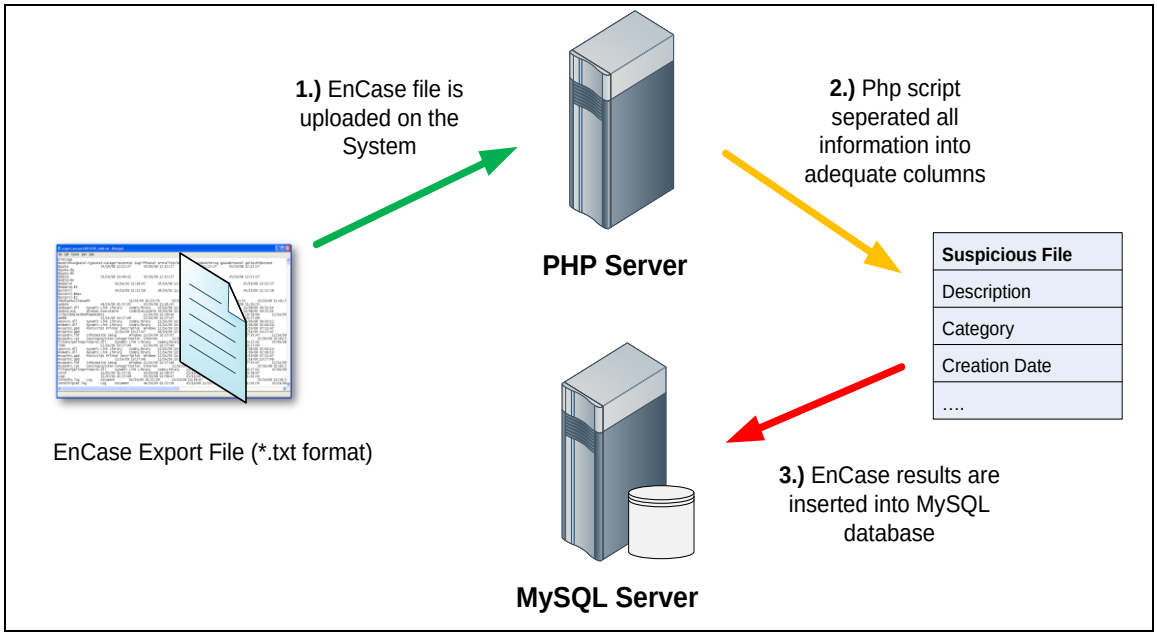


Figure 26, Process of uploading EnCase file into CFAA

After uploading the EnCase file and inserting all relevant data into the correspond database columns, a fresh malware list has to be obtained to generate accurate search results. This malware list will be automatically downloaded from the sysinfo.org webpage which maintains such a software list. The technological process behind this approach is similar to the file upload procedure.

Sysinfo.org provides an exhaustive csv file which includes all known malware programs identified by modern virus scanner. It would extend the scope of this research project to explain the entire malware identification process but it has to be acknowledged that it is a very time-consuming action. Due to the supportive community the sysinfo.org provides the most comprehensive malware list available on the internet. The structure of this csv file is illustrated within the following
Figure 27. It contains five different columns which include all valuable information.

Name	*Description*
• Name or start up item	This field includes a distinct name of the data
• Status	The status field indicates the functionality of the malware program Different status keys: • "Y" - Normally leave to run at start-up • "N" - Not required or not recommended - typically infrequently used tasks that can be started manually if necessary • "U" - User's choice - depends whether a user finds it necessary • "X" - Definitely not required - typically viruses, spyware, adware and "resource hogs" • "?" – Unknown
• Command or Data	This field includes a distinct name of the process
• Description	This field gives a short description of the malware functionality and provides a link for additional information
• Tested	This field defines if the malware program was manually tested

Figure 27, CSV file structure of malware list

5.5.2. CFAA – Analysis

The CFAA – Analysis process represents the core element of the CFAA prototype. It evaluates all available evidence and cross checks with the corresponding malware list obtained from sysinfo.org. If any suspicious file can be detected or identified the CFAA prototype immediately produces an alert message for the forensic investigator.

One of the biggest technical problems was to develop an automated algorithm that is capable of comparing such a big number of files with the corresponding malware list.

The first attempt to solve this technical issue was conducted by trying to verify every file explicitly. This attempt ended up in a complete failure because the needed computational power was beyond available capacities. Due to this limitation a more general approach was selected. Instead of dealing with every computer file and full code in detail, only the file names were analysed and investigated. This solution provided the possibility to efficiently cross-check all computer files in a very fast way. Due to the MySQL technology and the corresponding SQL syntax all files can be checked in a very time-efficient process.

The results and outcome of this investigation process is stored in another secure MySQL database table where every user interaction is logged and documented to secure the authenticity of the collected evidence.

Another very important part of the CFAA analysis is to confirm the reproducibility of the gathered evidence. Within all technical test-runs the CFAA analysis tool always generated the same and exact results due to the involved search algorithm.

In the end the CFAA analysis process has only one big drawback because of already discussed limitations. It only investigates and searches with the use of filenames. If a malware program for instance tries to masquerade or change its filename in a random way the CFAA analysis tool will fail. However because of the constant update of the Sysinfo malware list this limitation can be neglected as the list includes even permutations of known malware names that expand the possible scope.

There is also another issue which has to be mentioned at this stage. The Sysinfo malware list includes even malware programs that masquerade as average computer processes with their common names like explorer.exe or

plugin-container.exe. The CFAA analysis process will always detect these suspicious files and include them within the CFAA output file although in most cases these files will not be really affected. This is related to the designated limitation that only the filenames will be analysed and not the full source codes or any hash value. Such false-positive values will always appear because of the involved search algorithm combined with file-names.

During several test-runs the following performance values were evaluated which can be seen in Figure 28. This figure illustrates the efficient performance of the CFAA analysis process.

Number of files (22000 list of malware programs)	*Time*
~500	< 1sec
~1000	< 1sec
~10000	1min 24 sec
~50000	6min 51 sec

Figure 28, CFAA analysis performance

5.6. Classification of Cybercriminals

As already discussed the CFAA prototype is a valuable solution to increase the efficiency of forensic investigations. However it still has some drawbacks and limitations which can be handled by introducing additional information about an attacker. Under certain circumstances it is possible to evaluate if an attacker has the knowledge level of “Script-kiddies” or an IT-professional. In many cases it is just more than enough to look at the affected system and all the security measures which had to be bypassed or outwitted to get access thereto. In such situations it can be very helpful to have a valid classification of possible cybercriminals to determine the possible threat level. If a criminal shows the capability of more advanced strategies or techniques a deeper and more fundamental investigation is required.

The following classification that this research project will introduce, is based on D. Shinder approaches [91] . She discusses in her book that not every cybercriminal has the same motivation to commit a crime. There are several different levels of criminals and all have special backgrounds which can have influence on a computer forensic investigation.

5.6.1. Common Motives for Committing Cybercrimes

There are mainly six different motives which can encourage a person to commit a computer crime. The following aspects are based on (Shinder, et al., 2007):

1) Just for fun

   This is a group where most of the mentioned “Script-kiddies” fall into. These cybercriminals do not know or underestimate the effect of their actions. They do not try to realise any monetary or practical gain from their hacking activities.

2) Monetary profit

   This group of cybercriminals is similar to “offline” criminals. They are only motivated by the desire for financial gain and success. Many professionals join this group in the hope to improve their financial situation. This group forms an extremely dangerous fraction because modern criminal organizations try to make use of professionals who seek fast money.

3) Anger, revenge and other emotional needs

   Another very strong motive in contrast to the already mentioned is the emotional motivation. Anger or pain can drive people to do things they would normally never think of. They are often unpredictable and unconventional which makes them very hard to analyse and foresee. Revenge differs a bit from anger. In cases where cybercriminals committed a crime out of revenge, they were usually better planned and

[91] See (Shinder, et al., 2007) for more information

prepared. This makes them more dangerous and effective because those criminals have more time to think through their plans.

4) Political motives

Political motivation can often be found within members of extremist and radical groups. They often do not agree with current political parties and situations and try to influence them by committing cybercrimes. The range of possible cybercriminals starts at single hackers who just want to make a political statement and ends up at organised terrorist groups who try to destabilise entire regions.

5) Sexual impulses

Psychologists and psychiatrists already proved decades ago that sex is one of the strongest instincts in any human being. Therefore it seems obvious that there must be an own designated motivation group for these cybercriminals. One of the biggest problems with prosecuting sexual cybercriminals is the different jurisdiction systems all around the world. Pictures, comics and stories that are fully legal in one country can be prohibited in another one. As long as there is no common jurisdiction this problem will remain unsolved.

6) Psychiatric illness

The last group of motives is focused on mental illness. D. Shinder describes this group as followed: "…some criminals are motivated to engage in illegal and antisocial behaviour by underlying psychiatric conditions, especially those conditions that manifest themselves in symptoms such as lock of impulse control …or… hallucinations…"[92].

[92] Cited from (Shinder, et al., 2007)

5.6.2. Categorising Cybercriminals

This paragraph tries to describe and categorise three different types of cybercriminals. To accomplish a detailed categorisation of cybercriminals there must be vague distinction of two broad areas. One area covers “criminals who use the Net as a tool of the crime” and the other deals with “criminals who use the Net incidentally to the crime.”[93]. It is important to distinguish between these groups because this can lead to a better understanding of the full criminal act.

The area of criminals who use the net as a tool to commit a crime can be divided into three separate groups:

1) White-Collar Criminals

   White-collar criminals, derived from the image of a typical office worker, as individuals who have no personal ethics that would prohibit from stealing or cheating[94]. They often commit crimes only in response to serious financial troubles. Typical criminal acts are changing computer records at companies, manipulating financial transactions, selling company information or creating false information within companies to disrupt their activities.

2) Computer con artists

   According to D. Shinder “Computer con artists” use the internet as a tool to reach their possible victims. They make use of chat rooms, email addresses and web sites to propagate their fraudulent actions. These criminals focus mainly on typical internet fraud like auctions where buyers pay for their products but never receive their goods or on internet service scams. Other typical criminal acts are credit card frauds or all other sorts of internet scamming.

[93] Cited from (Bielecki, et al., 2009)

[94] Term was introduced by Edwin Sutherland in his address to the American Sociological Society in 1939 (Edwin, 1939).

3) Hackers, crackers and network attackers

Hackers are often, in comparison to the other already mentioned groups, professionals who need the internet as an essential tool. They are gaining their experience through studying network protocols, operating systems and focusing on possible vulnerabilities. They are often well trained by companies, universities or even by military institutions. The hacker community itself can be divided into two different groups:

- White-Hat Hacker

  Professionals of this group search consequently for possible vulnerabilities within a computer system and inform involved companies about their security holes and weaknesses. Besides they often develop open source software that tries to help companies to avoid any security leaks or threats. They mainly use their knowledge for noble and legal purposes.

- Black Hat Hacker

  These hackers break into computer systems illegally or for personal gain. They are often driven by rival hacker groups to show off with their capabilities. In the end the black hat group unites all aggressive hackers and crackers who try to compromise a computer system and all of the involved security systems. This group also includes all types of Script-Kiddies and copycat individuals.

5.6.3. Envisaged Approach for Categorising Criminals

The envisaged approach focuses on the combination of the CFAA prototype together with the categorisation of cybercriminals. The idea behind this approach is to increase the accuracy and the efficiency of the automatic investigation tool. Based on D. Shinder's classification the investigator has to determine independently what kind of cybercriminal the attacker represents. This requires special knowledge and skills from the investigator to make proper

assumptions. The cost of such additional trainings can be easily regained through the increase of efficiency and accuracy of on-going investigations.

According to the already discussed classification, following attacker profile model was developed which will help to implement the classification structure into the CFAA.

Type of Cybercriminal	*Technical Skills*	*Threat Level*
White-Collar Criminals	Low	Low
Computer Con Artists	Mediocre	Low
Hackers (in general)	High	High
→White Hat Hackers	High	Low
→Black Hat Hackers	High	High
Script-Kiddies	Low	Mediocre

Figure 29, Attacker Profile Model

Based on this attacker profile the CFAA settings can be adjusted to be much more sensitive if a black hat hacker attacks.

How shall the investigator know who is attacking?

A good strategy for investigators to determine an attacker profile is first to look at the designated and attacked computer system. What kind of system does it represent and what files or applications are stored? Does it have any vital effect on the company if the system has to go offline? All these questions define the possible decision tree which results in a final attacker profile[95].

The author Eoghan Casey calls this approach forensic crimes victimology which involves understanding why an offender has chosen a specific victim and which risks he was willing to acquire.[96]

[95] See Figure 30 for more information
[96] Based on (Casey, 2000) page 163, last paragraph

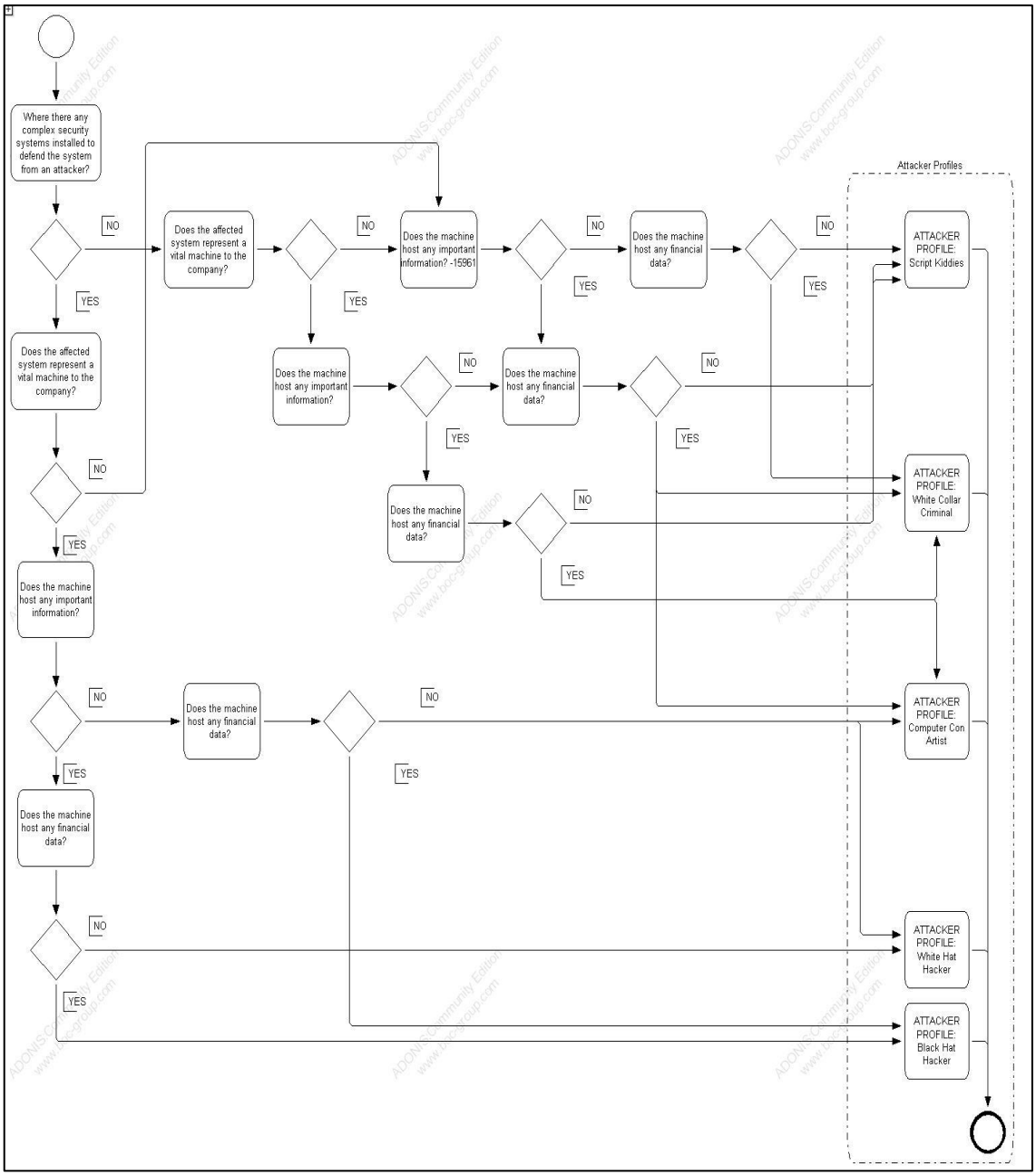


Figure 30, Decision tree to identify attacker level

The categorisation is primarily done by verifying the difficulty to bypass all security installations and the value of the designated target. More valuable systems represent more prestigious attacks which can be probably only conducted by skilled professionals. With the increasing threat level the entire forensic investigation has to be more thorough and extensive. It is predictable that professional hacker will make use of novel attacks and vulnerabilities which have to be taken into consideration as well.

Additionally CFAA has the capability to identify anomalies or to report unexpected values. During an investigation with a probable black hat hacker the level of reporting and the search for anomalies is increased. Following areas are investigated in a more detailed way:

- Log files (including verifying network logs, access logs and system logs)
- System relevant files have to be verified by valid hash values
- System time and the equivalent file dates have to be controlled to catch possible anomalies
- File permissions have to be controlled and verified.

The outcome of such an extended investigation will hopefully lead to more accurate and clearer results by providing additional information and supporting the investigator.

5.7. CFAA – Output

The CFAA – Output process represents the final step of the CFAA prototype. It analyses and evaluates all gathered data and results and generates a standardised output file. It combines even the attacker level categorisation with the collected evidence and prepares an argumentation strategy for the upcoming court case. The following Figure 31 shows the current output of the CFAA prototype.

Analysis result data (for project '*Projectname*')

Suspicious files	Description	File-Type	File-Category	Last accessed	File created	Last written	Modified	Deleted	Scanner	Mark
update.exe	Added by the RBOT.BDA WORM! Note - this is not part of the popular WinZip file compression utility	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Added by the MYOTB-EH WORM!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☑
update.exe	Added by the WINLOGON TROJAN!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Added by the RBOT-EMO WORM!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Could it be related to this or something similar?	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Added by a variant of the SPYBOT WORM! See here	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Added by the QQPASS-AM TROJAN!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Stop-the-Pop-Up popup blocker	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Wireless management utility for the T-Com Sinus 1054 Data WLAN adapter	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Added by a variant of the RBOT WORM!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Added by a variant of the SPYBOT WORM!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Added by the ZEZER WORM!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Added by the RBOT-APU WORM!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Added by the SDBOT-AGP WORM!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Added by a variant of the SDBOT WORM!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Added by a variant of the AGOBOT/GAOBOT WORM!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
update.exe	Added by the RBOT-JM WORM!	Windows Executable	CodeExecutable	05/19/08 11:01:45	10/08/06 09:51:14	10/08/06 09:51:14	05/19/08 11:01:45		E	☐
	Windows Essentials Codec Pack 1.0 is a									

Figure 31, CFAA Analysis

The output of the analysis process can be exported in a standardised doc file which can be used by modern office applications. The doc file format was chosen on purpose instead of a PDF file to maintain the ability of adding additional information manually into the generated document. It includes all suspicious files, their access times and the adequate descriptions. In addition the output file includes the argumentation strategy related to the corresponding attack level. Figure 32 shows the doc output file in more detail.

CFAA

Computer Forensic Analyser & Advisor

25/10/2010

Generated results gathered through CFAA:

Investigator:	Maximilian Bielecki
Client name:	Univie
Project name:	Forensic Investigation
Project description:	Test Investigation for suspicious malware programs
Date of infection:	Unknown
Assigned threat level:	Black Hat Hacker

Suspicious files:

Suspicious file	File description	File type	Category	Last accessed	File created	Last written	Modified	Deleted	Scanner
update.exe	Added by the MYOTB-E Worm	Windows Executable	CodeExecutable	05/09/08 11:00:01	05/09/08 11:00:01	05/09/08 11:00:01	05/09/08 11:00:01		E

Suspicious processes:

Suspicious process	Level	Date	Root	Event ID	User
update.exe	Medium	05/09/08	Root		Root

Figure 32, Word output (example.docx)

5.8. Extension – Visualisation

The current prototype is only focused on and limited to the search for malicious programs and software. Due to the expandable structure of this concept, it can however be upgraded with advanced search routines and algorithms. Such advancements to the system could eventually include the ability to analyse the events that have occurred on a system within a specific time frame, or the ability to focus on a particular type of file, author, source or system event.

An obvious area of concern is the performance factor of such further advancements to the system. Due to the growing size of digital evidence sources, there exists a delicate balance between showing the investigator information that is required and performing a thorough check of every single scenario. For instance, in the current iteration of CFAA to create accurate and valid results, a growing amount of time is needed to check the constantly growing list of possible malware programs that is extracted from the web.

The ability to extract the events occurred on a system, detect patterns of behaviour and file activity within a time frame are just some of possible subsequent steps for the extension of the CFAA prototype. These new analysis techniques however, need to produce results that are understandable to all users; both expert or non-expert investigators and to a jury in a way that is presentable in a court. For this reason the next logical step is to develop manners to filter, focus and present information in meaningful, understandable and efficient ways. Therefore the prototype focuses mainly on the investigation, to overcome both performance and scaling factors (related to focusing on timeframes or certain file events) and information overload.

The idea of such a visualisation extension of the CFAA prototype came up during the Ares 2010 conference in Cracow. Visualisation of gathered results was one of the most discussed topics at the forensic workshop which lead to the implementation. Three different visualisation frameworks were considered and tested to identify the most efficient approach. In the end a well-documented visualisation API, provided by Google called Google Visualisation[97], was implemented into the prototype. Figure 33 and Figure 34 show in detail two visualisation types that were integrated into the prototype.

[97] "*The Google Visualization API allows to create charts and reporting applications over structured data and helps integrate these directly into a website"* (Quoted from http://code.google.com/intl/de-DE/apis/chart/interactive/faq.html#whatis)

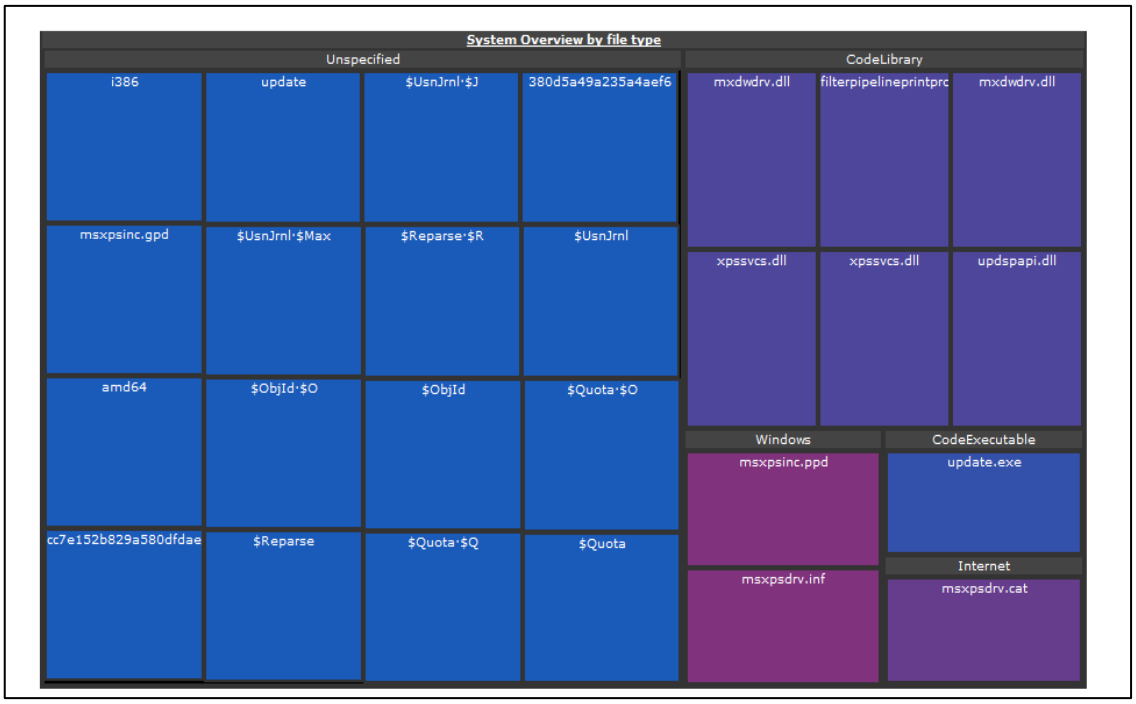


Figure 33, Treemap Visualisation generated with the Google Visualisation API

The first figure shows a tree map where all files are listed. In addition it provides interactive information about the files and their related access times. This graph is especially useful to investigate the different files and their corresponding categories.

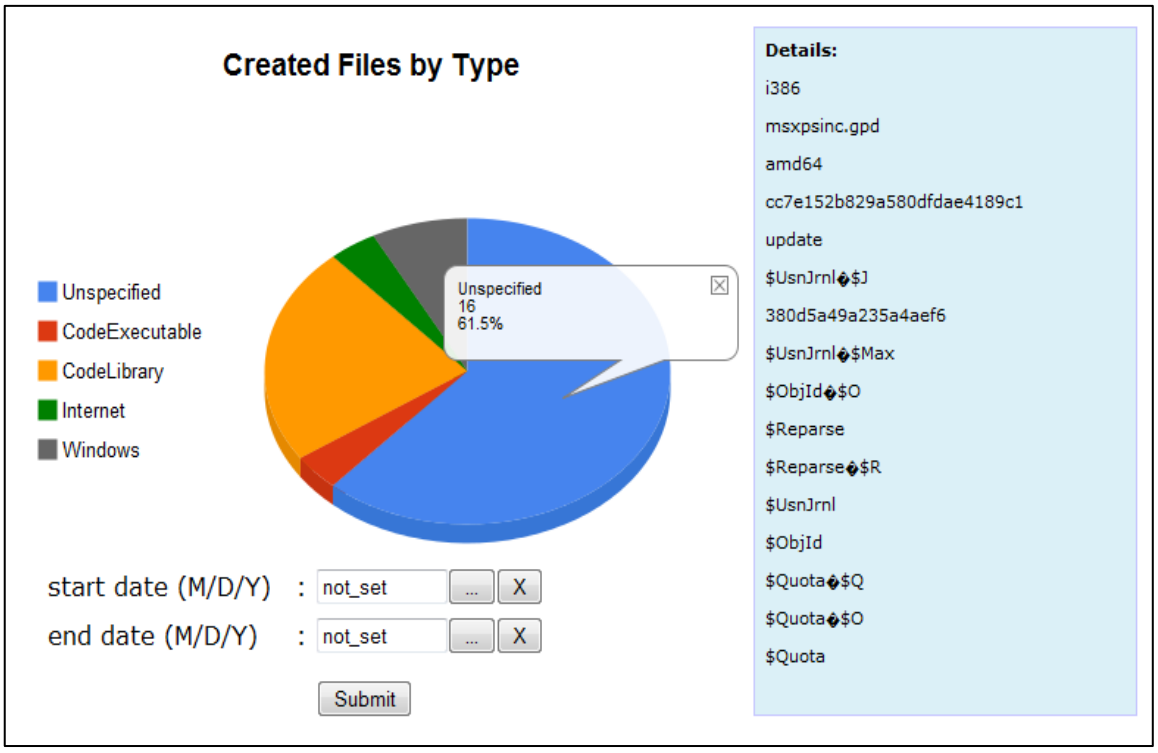


Figure 34, Pie chart generated with the Google Visualisation API

The second figure demonstrates a pie chart which has advanced filtering options. These options can be used for narrowing down the computer crime and to investigate which processes were changed step by step.

Additionally there was an idea to implement a third visualisation chart as a timeline. This implementation was dropped because during the early test phase the usefulness of this visualisation was very limited. In the end it provides only useful information for less than ten files. Different system files generate a more confusing diagram which does not include any additional information for investigators.

One general observation that was made immediately after implementing the visualisation extension was that, although visualisation tools provide a very helpful approach, there is still a need for a human investigator who is capable of interpreting all results properly. Visualisation itself is not a perfect solution, it only supports the investigation process.

5.8.1. Visualisation – Technical Realisation

The technical implementation of the visualisation module was simple due to the extensive documentation provided by Google[98].

The visualisation API requires firstly the set of corresponding data. This data table is generated through a SQL query directly from the connected MySQL database. It is achieved via a standard “SELECT” query to get the appropriate results. As a next step this data is forwarded to the visualisation API which initiates a JavaScript function that finally generates the desired diagrams[99].

The JavaScript Code (library) is centrally stored at Google and loaded each time a new diagram is generated[100]. Instead of loading the full code and storing it locally, this centralised approach enables Google to update and increase the functionality of its libraries and forward it to all users at the same time.

In addition the implemented API allows some optional user-graph interaction to generate further diagrams and information (like Mouse over-effects,..). This functionality is as well achieved via a JavaScript and AJAX function calls[101].

The main problem with JavaScript and AJAX is that the loading browser has to support these programming languages correctly, otherwise it will not work properly. Modern computer browsers provide built-in JavaScript functionalities but this situation is different within the smartphone sector. Because of the limited system resources and capabilities most mobile web-browser lack these functionalities. Depending on the OS of the mobile phone, there are sometimes mobile add-ins which can extend the functionality of the browser.

---

[98] Additional information can be found under the following link: http://code.google.com/intl/en/apis/chart/

[99] JavaScript is a client-side scripting language with a multi-paradigm approach, supporting object-oriented, imperative, and functional programming styles. It was developed in 1995 by Brendan Eich for the Netscape Communications Corporation.

[100] This is a legal issue for the public usage of the visualisation API.

[101] AJAX stands for Asynchronous JavaScript and XML and is a group of interrelated web development methods used on the client-side to create asynchronous web applications.

This visualisation API proves to be a very efficient solution which is capable of generating huge diagrams for more than 100,000 entries. Because of the structure of JavaScript, the main limitation is located on the client's side, where all needed calculations are performed. Weaker or older computer systems will struggle when the number of presented entries exceeds 100,000 items.

5.9. CFAA Summary

The CFAA prototype provides the technical verification of this research project and its involved ideas. It demonstrates the efficiency and functionality of the novel concept and the corresponding model.

Due to the web application functionality it can be used by all modern web browser and even smartphones. The involved technologies do not require any special server installation except a PHP capable webserver, combined with a common MySQL database which proves to be a common server installation.

The usage of standardised software and thrifty computer performance leads to a very capable application that can be easily adopted and expanded for further developments.

The CFAA prototype showed that is possible to support forensic investigations by the use of modern technologies. In addition it provides optional help for investigators by determining possible attackers and their tech-skills involved. It decreases the needed time for advanced malware identification by fully automated processes.

The complete source code for this prototype and all relevant forms and pages will be added to this research thesis on a CD to verify the research results of this research project.

6. Case Study

The following chapter illustrates the functionality of the conceptual model by using the novel CFAA prototype.

6.1. The Realistic Scenario

A computer user receives a suspicious email. Although he is surprised that the message is written in a foreign language, he still decides to open the email attachment. Often these kinds of messages pretend to be from a friend who sends funny attachments or pictures. There are also documented cases where the provided information contains some business of pornographic materials.

The user is misbelieving that his installed and running anti-virus security program will successfully defend his computer software against any malicious program. The current McAfee report states clearly that anti-virus and other security systems still require several hours to fully adapt their programs to novel threat scenarios (depending on the complexity of the innovative malware)[102].

Returning to this case scenario, an average computer user opens the received attachment which includes an exe-file. Exe-files are computer files that include executable runtime code used by Windows programs.

This type of file limits automatically the threat scenario to Windows machines because other operating systems use different file types and will not accept exe-files (e.g. Linux or iOS).

In this case the user still uses the Windows XP operating system (still one of the most common systems) on his machine. The attachment opens and it actually includes some funny pictures or movies. Nevertheless this is only the limited view from the user perspective.

[102] See (McAfee, 2012) for more information

While the user is distracted with some flashy pictures, the exe-file starts to deploy its malicious content. In this case it is a malware program that opens a backdoor to the operating system. Due to the fact that this is a new derivative of common malware programs, the running security system does not detect this infection (=installation of the malware program) nor recognise the threat.

The computer user is still amused by the funny attachment and closes finally the exe-file. So far the case scenario contains only a crime of gaining illegal computer access which is still unrecognised by the user. This will change within the following weeks.

After two weeks the user is suddenly surprised by suspicious transactions on his bank account which he regularly checks via his browser through his online banking access. He calls immediately his bank and requests an explanation. The bank responses that the transactions are valid and were correctly authorised by the customer TAN number. The user recalls that he initiated some bank transactions with his mobile TAN code received by SMS on his separate mobile but for completely different transactions. What was going on? The user is still convinced that there must be a mistake at the bank and starts an additional inquiry. After unsuccessful attempts the user contacts the police that starts an investigation. This is now the starting point for the computer forensic investigation.

6.2. Computer Forensic Analysis

After contacting bank authorities and receiving confirmation from the bank that the transactions were legally authorised and initiated, the law-enforcement unit starts to investigate the affected computer of the user. A detailed computer forensic analysis is conducted.

Firstly any digital evidence is collected and sealed. The main principle which has to be obeyed is that no action taken should change data held on the computer system. In addition a detailed audit trail of all applied processes has

to be created to fully specify and document who exactly has access to the confiscated data and what actions are to be taken.

Data files stored on a computer system are no different from traditional documents or information. For this reason digital evidence is subject to the same rules and regulations that apply to traditional evidence.

In the presented case the sealed data is approximately 80GB which is the average hard disc volume of a typical office machine.

As a next step the digital forensic investigation is conducted. EnCase as a wide-spread and state-of-the-art solution is used for forensic analysis. As already described in chapter 4.1.6.1, EnCase provides an extensive toolkit for all kinds of investigations. The main problem is that scope of functionality of EnCase is too broad which makes it difficult to use correctly.

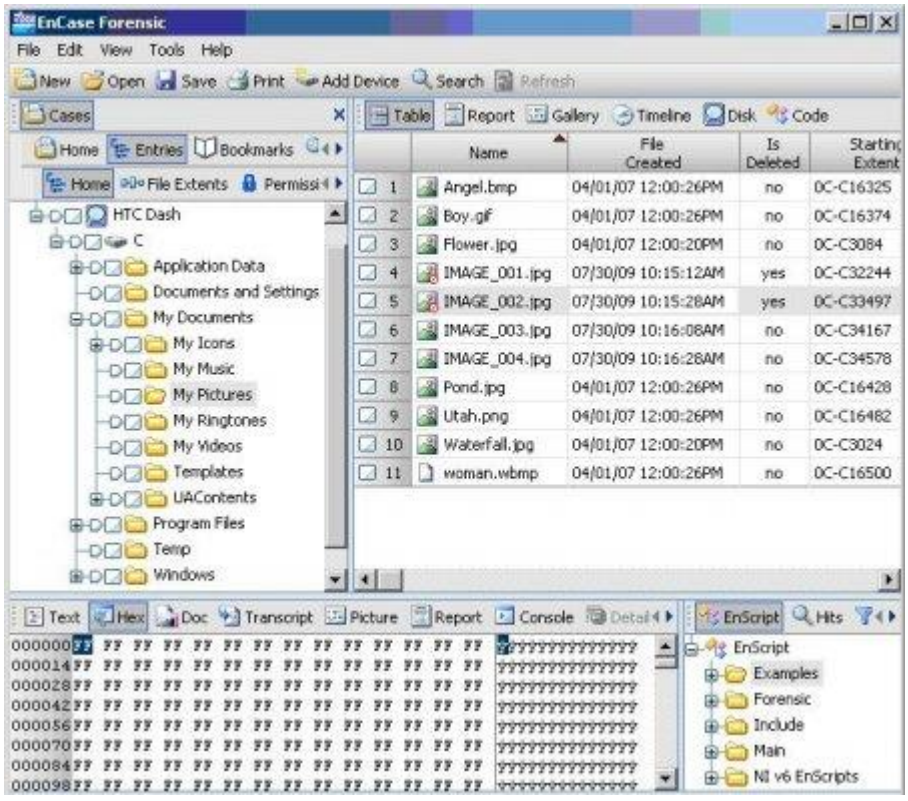


Figure 35, EnCase Investigation Screenshot[103]

[103] Screenshot taken from **http://computer-forensics.sans.org/blog/category/computer-forensics/evidence-acquisition/**

Figure 35 illustrates the EnCase graphic user-interface. In this case the user's computer system is analysed and the special EnScript file activated.

This batch process generates a result file list which will be afterwards imported into the CFAA prototype. The total amount of inspected files lies around 155000 items. The import into the CFAA prototype takes around 19 minutes. Within the next step the forensic investigator enters the threat level according to chapter 5.6.3. In this scenario the threat level is high and the included tech skills appear to be high as well which leads to a Black Hat Hacker that tried to achieve as much benefit or damage as possible.

The outcome of the CFAA generates a list of four suspicious malware files:

- C:\Windows\msagent\msdqwn.com (size 41KB)
- C:\Windows\System32\mspgcs.com (size 43KB)
- C:\Windows\dxdgns.dll
- C:\Windows\System32\dxdgns.dll

These four infected files lead to the "BEAST" malware backdoor-program which belongs to the type of Remote Administration Tools. These tools allow the attacker to achieve full control over the affected system and record every entered key.

The correct technical term for this malware program is Backdoor:Win32/Beastdoor.DL[104].

The default ports used for the direct and reverse connections are respectively 6666 and 9999, though the attacker had the option of changing them. The malware has a built-in firewall bypasser with the ability of terminating some Anti-Virus or firewall processes. It also contains a file binder that can join two or more files together and then change their corresponding icon[105].

[104] See http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Backdoor%3aWin32%2fBeastdoor.DL#tab=2 for more information about this Beast malware program

[105] Cited from Wikipedia http://en.wikipedia.org/wiki/Beast_Trojan_%28trojan_horse%29

Within this scenario the attacker misused the victim's computer and recorded every entered keystroke. That is how the attacker gained the required online banking PIN and TAN codes to manipulate the online transactions.

The CFAA prototype successfully identifies the malware program and provides additional information about the malware program. This step supports the investigator and provides additional help for the on-going investigation.

As a final result CFAA generates a final report that documents the infection and tries to specify a possible infection timestamp based on the local file system and last time of manipulation.

As a next step the CFAA tries to investigate how this malware program landed on the victims machine. It is now a lot easier for the investigator because he knows now exactly what he is looking for. At this point the advanced forensic skills of the computer expert are decisive to end up the ongoing analysis positively.

Because of the CFAA output an appropriate timestamp can be determined and the Windows log files investigated. Due to the comprehensive log capabilities of the Windows operating system, investigators can identify and recognise the suspicious attachment within that time period[106].

Because the entire victim's system is sealed and an identical copy generated the suspicious attachment can be easily restored. In addition the mail log files can be extracted that provide valuable information about the source of the malware program.

This investigation leads to a remote internet address 203.113.17.129 located in Vietnam which appears to be a dead end because of the lack of legal possibilities. Additionally this IP address is used by several local ISP at the

[106] These capabilities are even more extensive in the novel Windows operating system versions http://windows.microsoft.com/en-us/windows/what-information-event-logs-event-viewer#1TC=windows-7

same time which makes it technically impossible to bind it to a specific computer system.

Computer hackers try to masquerade their moves as good as possible. In this situation the recognised IP address was used for a relayed mail server which was deactivated shortly after.

Due to the technical structure of the collected evidence, no additional investigation can be conducted.

6.3. Conclusion of this Case Study

The CFAA prototype works fully as expected and defined. This proves that the defined conceptual model generates valid results that can be used as preparation for court cases.

Although the outcome of this case study was not satisfying because no criminal could be fully identified, the CFAA prototype provided full support for the ongoing computer forensic investigation.

This case study can be considered as a typical computer forensic investigation which leads to dead ends because of legal and technical limitations.

In addition with all the technological supportive tools, it still requires a highly-skilled investigator to interpret the gathered results correctly. One crucial criteria for professional investigators is the experience. Forensic investigators need to have the ability to think like a criminal and evaluate the initiated steps correctly.

Technological tools provide additional help and can increase the efficiency of investigations but they still require professionals who can use them correctly and effectively.

7. Discussion and Evaluation

This chapter discusses the gathered results by adopting a novel concept for computer forensic investigations. Within the following paragraphs the discovered limitations will be analysed and explained. As a next step the research project in general will be evaluated. At the end of this chapter all discovered findings will be discussed in more detail.

7.1. Introduction

The approach of this research project was to analyse the current situation of computer forensic investigations and identify possible limitations. After this analysis, a novel model which has the main aim to increase the efficiency of these investigations was developed. Additionally this new concept was tested against three main fields surrounding computer forensics: the legal area, the organisational area and the technical area.

This chapter presents a detailed discussion of the research findings that underline the efficiency of the newly developed model.

From the three areas described in previous chapters it has been identified that each area itself is facing its own significant problems and difficulties. Research and development projects in each area are working on solutions for these challenges. However, this research project has clearly highlighted that there is a need for a more general approach which combines all areas. All work conducted within this field of science has to look beyond the obvious borders of a predefined area.

From a computer forensic perspective, this raises concerns about collecting digital evidence and about the relations between technical, legal and organisational solutions which are currently developed. More specifically, the

concern is that these solutions are adversely impacting each other with completely coherent effects.

It is useful for the following discussion to revisit the primary research question once again:

> Research Question: How can the efficiency of Computer Forensic investigations be improved by a better integration of standardised tools in the forensic analysis process, especially regarding the preparation of evidence for presentation in court?

Analyses in chapters 2 and 3 have generated insights that contribute directly to answering these questions. Chapter 4 introduced a practical development of the newly created concept model by developing a technological prototype.

The first part of this chapter will discuss the defined limitations of this research project which were necessary to achieve the research goal. The second paragraph will discuss the findings and evaluate this research project.

7.2. General Limitations

This research project was conducted in the modern field of science called computer forensic. Computer forensic is an adaptation of classical forensic approaches combined with computational challenges. The problem with modern computer systems is that there is constant development within industry. New operating systems are developed almost every two or three years and released to the market which makes it extremely difficult for computer forensic experts to always keep ahead[107]. The knowledge about the OS system is crucial for computer forensic investigations because the OS can store hidden information that can provide important evidence for committed computer crimes[108].

[107] See Windows Release Cycle for instance: http://www.directionsonmicrosoft.com/sample/DOMIS/update/2005/06jun/0605rtlc_illo1.htm

[108] See http://home.comcast.net/~supportcd/DiagnoseXP.html for Windows XP secrets

Apart from the log files, every OS system has its own memory and data management and often uses incompatible file storage mechanisms which make it even harder for investigators. There are Linux distributions that use ext4 or ltf, whereas Windows uses NTFS or Fat32[109]. It is illusionary to expect that every computer forensic investigator is an expert within every operating system.

In addition to the operating system, computer forensic experts need to have the understanding of novel computer technologies and the related network techniques. Modern network technologies like BT or WiFI network connections must be fully understood. Besides this traditional techniques novel technologies are constantly introduced like virtualisation[110] or cloud storage[111]. Without this fundamental knowledge no computer forensic investigation can be conducted successfully.

It has to be reminded as well that a computer forensic expert still has to observe to the current legislations although he has enough technological knowledge to collect evidence in an illegal way like breaking an encryption mechanism for WiFi connections[112] for instance. It is a very similar situation as with law enforcement institutions which always walk a tight path to achieve their goals.

Different legislations provide additional difficulties to forensic investigations. Although the European Union is a highly regulated community of European countries with similar economic legislations, almost every European country has a different approach towards computer security and data privacy. As clearly highlighted within chapter 4.1.4 the EU already started an initiative against cybercrime within their member states but faces huge difficulties with different national regulations. It would be too difficult to introduce the same laws and regulations in every country because the current legislations and legal systems

[109] Comparison of different file systems http://en.wikipedia.org/wiki/Comparison_of_file_systems

[110] Virtualisation describes the technique to run a virtual instance of an OS or application on top of a running system. The advantage of virtualisation lies within the strict separation between the virtual and host instance.

[111] Cloud storage is a model of networked online storage where data is stored in virtualised pools of storage which are generally hosted by third parties.

[112] WEP was an old-fashioned wireless-network encryption standard which is outdated now. It was replaced by WPA and WPA2.

vary. Nevertheless every European inhabitant should be protected by the fundamental principles of the above mentioned initiative.

After identifying the technical and legal limitations, the last limitations are within the organisational area. The main difficulty with identifying possible limitations within this area is that they are closely related to legal regulations.

One essential problem for forensic investigation is that there is no official and standardised organisational hierarchy which has to be obeyed by every company. A company or enterprise is comparable to the growth of a flower. At the beginning it is just a small seed planted within fertile earth. Over time this flower grows and extends its roots into ground.

It is the same with companies. They often start with only one employee and grow bigger through the years. The IT department is often later introduced within the structure and has to deal with the current business processes which were established years ago. This makes it extremely difficult to introduce new security standards without influencing running business processes. Companies often reject and reconsider such changes because of the fear of losing volatile business. This unacceptable approach and the lack of understanding of possible threats lead to the increased number of computer crimes.

Companies and organisations often spend big amounts of money on their computer systems but fail to secure them in a proper way. Additionally they fail to clearly define IT guidelines and conduct possible risk analyses to be better prepared for worst-case scenarios. Computer forensic investigators are often confronted with the situation that organisations do not have clear strategies how to handle situations after cybercrime incidents.

There is the lack of proper RISK assessment and RISK management. Risk assessment is needed to determine crucial areas within a company which need special treatment and support. This can include organisational areas as well as technological solutions and systems. Risk assessment and management are often taken as a basis for additional disasters recovery processes. These

processes define the proper and adequate procedures within a critical situation and support the recovery process.

Especially small and medium sized companies often fail to define such strategies and procedures properly[113]. It often proves to be difficult to allocate the proper amount of money for disaster recovery and realistic testing.

A predefined disaster recovery procedure is only as good as the realistic execution. Personnel has to be trained adequately to handle crisis situations efficiently. Best practise for these strategies is to test them at least once a year, depending on the company size and risk assessment[114].

7.3. Evaluation of the Research Project

After identifying known limitations of forensic investigations a more efficient approach had to be determined. This resulted in the creation of a novel conceptual model which could provide additional assistance to forensic investigators. One of the main difficulties was the close relation of the three main areas: legal area, organisational area and technical area. Every area on its own provided some possible solutions to support forensic processes. Nevertheless solutions which can help in one area can have a completely opposite effect on another one. The novel model had to deal and consider any possible relations on the one hand. On the other hand it should provide an easy to implement solution which should provide sustainable assistance to forensic investigators.

This research project has identified and explained the interrelated areas connected with forensic investigations. In response to the principal research question how the forensic investigation can be supported a novel conceptual model was established. To verify the effectiveness of this model approach a technical prototype was developed. The CFAA prototype provides an easy to

[113] See Business Review for short analysis http://www.businessnewsdaily.com/1868-small-business-data-recovery.html

[114] Find more information under http://searchdisasterrecovery.techtarget.com/answer/How-often-should-I-conduct-a-disaster-recovery-DR-test

use technical solution that can support investigators by automatically analysing affected computer systems. The prototype proved that all designated objectives were achieved. Investigators are supported by providing additional information about a possible malware infection. Currently there is no similar software solution available that can provide the same amount of additional information like the CFAA prototype.

In addition to the automated investigation the forensic investigator is supported by an argumentation strategy. The generated strategy is based on the outcome of the malware scan. During the analysis process the investigator has the possibility to classify the possible hacker what directly relates to the generated argumentation strategy.

For a fundamental analysis of the developed model the prototype was tested within realistic scenarios. The effectiveness and efficiency of this model proved that the approach is focused on the right direction. Although some possible limitations were identified and provided additional difficulties, in general the model proved to be valid and useful.

One big limitation for this research project was the focus on one specific forensic investigation type. Although the typical computer forensic investigation has to analyse hundreds of different crime scenarios, malware infection analysis was selected. Malware is the abbreviation for malicious code that gains access to the system through a backdoor or a careless system user. The results of such contamination can be tremendous. The scope can be from harmless desktop pictures, redirected web browser or changed search engines to destroyed data, malfunctioned hard drives or misusing entire systems for possible botnets (like DDoS attacks).

Malware code and programs showed to be an old online plague which proved almost impossible to eliminate. Based on the McAfee threat report 2012[115] the

[115], [84] See Mcafee Threats Report (McAfee, 2012) for more information

number of malware programs constantly grows. Figure 36 illustrates the amount of new malware which was taken from McAfee threat report[116].

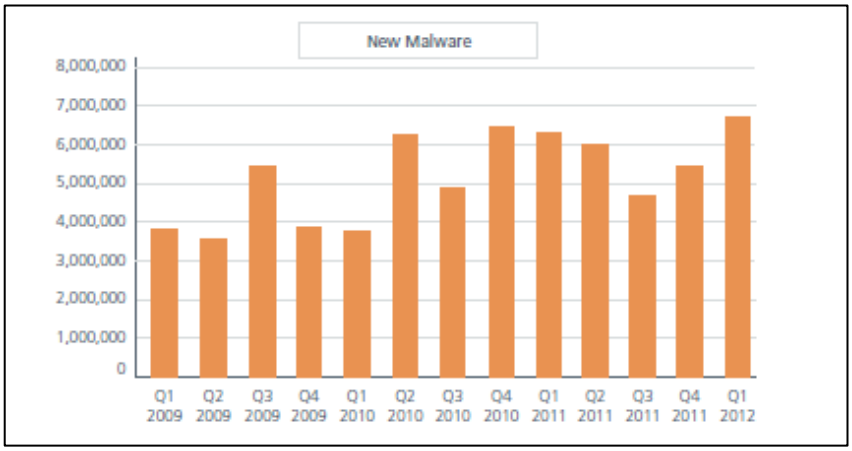


Figure 36, Diagram illustrating amount of malware programs

Besides traditional malware program a new trend has risen: signed Malware. "Attackers sign malware in an attempt to trick users and admins into trusting the file, but also in an effort to evade detection by security software and circumvent system policies. Much of this malware is signed with stolen certificates, while other binaries are self-signed or 'test signed.' Test signing is sometimes used as a part of a social engineering attack."[117]

Figure 34 illustrates the growing amount of signed malware binaries. In addition another new area of malware was introduced: the Mac OS environment. Although the Mac OS environment was always neglected by malware programs, the numbers constantly grow as well. McAfee estimates that there are around 2500 malware binaries written especially for Apple Mac OS systems.

[117] Cited from Craig Schmugar blog http://blogs.mcafee.com/mcafee-labs/signed-malware-you-can-runbut-you-cant-hide

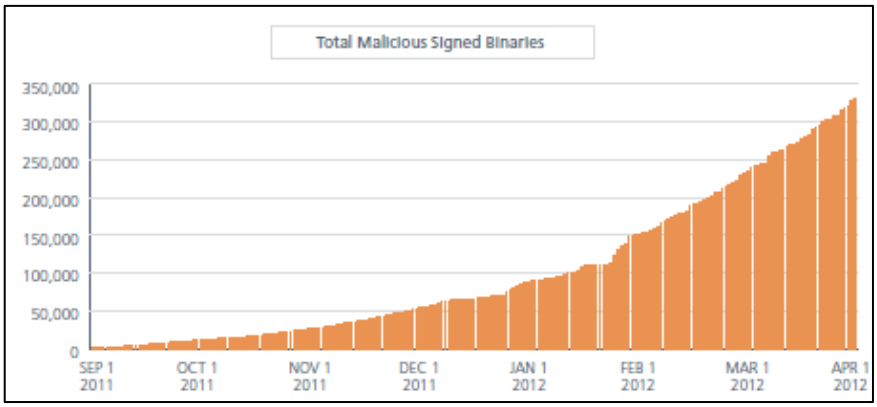


Figure 37, Illustration of amount of signed malware code

Due to the fast growing numbers of mobile smartphones, malware programmers started to focus on these modern mobile devices. Especially the mobile OS system Android showed to provide the biggest field of interest. In comparison to the Windows malware section however, these numbers are still very low. McAfee estimates that there are around 8000 mobile malware programs available for the Android platform. Google, founder and maintainer of Android OS, already showed some signs of concern about this development and announced a new security layer for Android applications[118].

Another hardware producer, Apple, is facing similar difficulties with their own developed operating system called iOS[119]. Although the situation is slightly different because of the different structure of the Apple eco system called iTunes. Every application to be joined to the iTunes community has to pass a very exhaustive system test conducted by Apple engineers. During this test phase the entire code basis is analysed and if no violations are determined the application will be granted. Apple defined a very strict set of regulations which have to be obeyed by every app developer (e.g. no malicious software, no nudity,…). The drawback of such strict and tight security procedure is the extremely long approval process which can take sometimes more than 3 weeks.

[118] See Google response for more information about the new security layer for android smartphones and tablets http://googlemobile.blogspot.com/2012/02/android-and-security.html

[119] iOS should not be confused with the Cisco router software. The former name of the operating system was called iPhone OS. After rapid growth within the mobile sector, Apple decided to rebrand their OS and changed the name to iOS in June 2010. In addition an license agreement was signed between Cisco and Apple which defined the usage of the iOS trademark for Apple See http://www.apple.com/pr/library/2007/02/21Cisco-and-Apple-Reach-Agreement-on-iPhone-Trademark.html for more information.

On the other hand this approach guarantees that iTunes user only get access to valid and working apps within the eco systems. This restriction limits the possible distribution of malware programs within iOS but hackers and their creativity to bypass such security installations should never be underestimated[120].

7.4. Technical Evaluation

During the concept phase of this research project the technological prototype was adapted several times (according to the “Design Research” methodology). At the beginning the main idea was to support forensic processes but after identifying possible boundaries and limitations the field was narrowed down to the automated identification of malware programs. Malware programs are sometimes harm-less programs that only manipulate computer systems in an annoying way. Nevertheless there are some advanced malicious programs spreading around that can harm the security of crucial computer systems very badly.

The developed and presented CFAA prototype focuses and investigates on detection of these malware programs. It uses the common available sysinfo.org malware list which is thoroughly maintained by malware experts. In conjunction with an EnCase results file, the affected computer system is cross-checked with the malware list and analysed[121].

How to evaluate the technical prototype?

The evaluation was conducted via several test scenarios and empirical experiments. To conduct an extensive assessment, three different EnCase investigations were carried out on three different personal computers to evaluate the efficiency of the system. Due the high level of installed security measures, all three test objects proved to be malware free. Within the following

[120] See http://news.cnet.com/8301-1009_3-57506159-83/apples-ios-and-android-are-new-favorite-malware-victims/ for more information.
[121] Detailed process was described in chapter 5 ”Prototype Development“

step additional malware programs were manually and on purpose installed on the three test objects.

Afterwards the typical EnCase investigation was performed and the results cross-checked with the CFAA prototype. The outcome in all three scenarios was always the same. The malicious software was always unambiguously identified and CFAA provided additional information for the investigator.

These results lead to the conclusion that the technological prototype works successfully and generates valid results. The evaluation process can be in general described as a success.

At this stage it has to be reminded that CFAA does not have the functionality to automatically identify novel or modified malware programs. The prototype uses the provided list of malicious software as a template to spot any suspicious malware [122]. This additional functionality of autonomous recognition would extend the scope of this research project beyond the defined borders.

[122] List taken from (Sysinfo.org)

8. Conclusion and Future Work

8.1. Chapter Introduction

This final chapter provides reflections of the conducted research and identifies areas of potential future studies and possible extensions. The primary objective in evaluating the developed prototype was to discover if and how it resolves the practitioner‘s problem and facilitates the development of future research opportunities.

A conceptual model was defined and designed to support possible forensic investigations. The subject was to increase efficiency and to provide substantial assistance for investigators during their analysis. The typical investigational scenario was discussed and possible limitations identified. As an outcome of these analyses the main scope of the automated functionality was identified and a corresponding argumentation strategy defined.

The following paragraphs will first start with the synthesis of the findings which will include the three previously defined areas. In addition there will be the discussion of some current legal issues and initiatives in more detail which have become very controversial. After the synthesis the previously identified limitations of this study are analysed and discussed. The following paragraph describes the reflections of this research project which have a very broad spectrum. The purpose of this section is to discuss all possible ideas and considerations which have grown according to this research project.

8.2. Synthesis of Findings

To completely analyse and discuss all findings of this novel approach every involved area has to be discussed separately. First the technical area will be discussed especially with the focus on the technical prototype. The following

paragraph investigates the legal area and possible related difficulties. The last part focuses on the organisational area and the influence of this model on current organisations and investigators.

8.2.1. Technical Area

The technical area is one of the most obvious ones in case of computer crimes. Computer crimes per se require the involvement of technical systems and networks. It is logical that forensic investigators use similar tools and technical solutions for their analyses. The proposed model within this thesis can be transformed into an automated technical solution. Its functionality is simple but efficient. Through the help of EnCase a list of all system files is generated and investigated. This list is compared with a constantly updated malware list. In case a positive match is identified the investigator is automatically informed and warned. In addition the investigator has the possibility to identify the skill level of an attacker through the hacker classification which is also implemented. These tools provide help for the investigator and can be used additionally to current forensic investigations. They do not interfere with other processes and can be considered as a supplementary investigation system.

One very important issue for computer forensic investigations is the sealing of digital evidence. Forensic investigators have to provide digital evidence which cannot be tempered or manipulated. The outcome of their forensic investigations always has to conclude reproducible results. Another forensic investigation should lead to the same outcome and findings.

8.2.2. Legal Area

The legal area represents a broad field of different legislations, laws and regulations. Even the approach to narrow down possible legal aspects only to the European continent will soon be faced with hundreds of different provisions of law. In the end every country has its own approach and strategy to deal with computer crimes. Although the European Union initiated a legal convention on

cybercrime most of the member states still have not fully adopted the proposed regulations.

Due to the huge scope of different legislations the focus was shifted towards the Austrian legislation which proved to have specific laws concerning computer crimes. Although the Austrian and German laws are similar in some legal areas, this time the Austrian regulations showed to be much more advanced and applicable.

This thesis presented the current Austrian regulations related to computer crime (see chapter 4.1.3 for more information).

Legal systems have to continuously adapt to novel situations to remain fully functional. The level of technical understanding has to be supported as new computer crimes use advanced techniques which can only be fully understand by experts. There is no point of a jury or court to judge a computer crime if they do not understand the nature and manner of a committed crime and the involved techniques.

In addition to the current European initiatives there is also a novel multinational treaty which tries to establish international standards for intellectual property rights enforcement, called Anti-Counterfeiting Trade Agreement (ACTA)[123]. Although the ACTA agreement focuses mainly on copyright infringements and tries to eliminate the process of illegal content download, it includes some additional treaties that can influence and support computer forensic experts worldwide.

8.2.2.1 Anti-Counterfeiting Trade Agreement

The ACTA agreement “aims to establish an international legal framework for targeting counterfeit goods, generic medicines and copyright infringement on the Internet and would create a new governing body outside existing forums,

[123] Read agreement for detailed information (Treaty, 2012)

such as the World Trade Organization, the World Intellectual Property Organization or the United Nations"[124].

Currently it is a multinational treaty which was signed in October 2011 by Australia, Canada, Japan, Morocco, New Zealand, Singapore, South Korea and the United States. In January 2012 the European Union and 22 member states signed this agreement and it is subject to the ratification process now.

The main idea behind this agreement was to establish an efficient legal system to stop the trade of counterfeit goods and pirated copyright of protected works in general. Major American industries, such as the American MPAA or the American Pharmaceutical Industry were deeply involved in the treaty's development which explains the purpose why the treaty mainly secures the intellectual property holder.

Considering the secret multinational negotiations which excluded civil society groups, NGOs and even general public, the ACTA agreement was highly criticised which led to public demonstrations especially in Eastern European countries in January 2012[125].

On the first view there is no direct connection visible to any computer crime related topics. With a closer look however at the proposed laws included in this agreement, the changes could lead to fundamental legal changes.

The American government proposed two novel additional laws which should constitute the basis for the ACTA agreement, called the PIPA and SOPA act. Both laws will be now discussed in more detail.

[124] Cited from (Wikipedia, 2012)
[125] Protesters in Poland angry about proposed ACTA – see for more information http://www.euronews.com/2012/01/25/protesters-in-poland-angry-about-acta/

8.2.2.1.1. PROTECT IP Act

The PROTECT IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, or PIPA)[126] is a proposed US law, which provides the US government with adequate tools to restrict access to rogue websites dedicated to infringing or counterfeit goods, in particular sites located outside the US territory. The US government would have the absolute power to decide which international websites should be shut down because of providing access to illegal materials.

This act was introduced in May 2011 and can be considered as a rewrite of the COICA act (Combating Online Infringement and Counterfeits Act)[127], which was previously blocked by the US Senate.

The act defines infringement as a distribution of illegal copies, counterfeit goods or anti-digital rights management technology. Infringement exists if "facts or circumstances suggest [the site] is used, primarily as a mean for engaging in, enabling or facilitating the activities described."[128]

8.2.2.1.2. Stop Online Piracy Act

The Stop Online Piracy Act (SOPA) is a novel US bill to expand the ability of U.S. law enforcement to fight online trafficking in copyrighted intellectual property and counterfeit goods[129].

This discussed legislation aims not at the illegal websites but at the service provider who tries to earn money with those pages. This bill would target advertising companies, payment facilities, as well search engine companies which try to conduct business with infringing websites in the same way. In addition service providers could face legal actions against them if they do not

[126] Read the proposed bill (Senate, 2012)
[127] Read the proposed bill (Senate, 2012)
[128] Cited from the proposed bill (Senate, 2012)
[129] Cited from http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act

control every provided webpage. The technical challenges for bigger service providers would be enormous to fulfil. [130]

Basically this bill is based on the PIPA Act (described in chapter 8.2.2.1.1) but supplements additional criminal laws especially against illegal content streaming. The main goals are to protect intellectual property of content creators and to protect against counterfeit drugs. Although it seems like a lose connection between the protection of intellectual property and medical drugs, but it makes sense when analysing the process of defining this bill. In December 2011 the House Judiciary Committee Chair Representative Lamar S. Smith accused Google of obstructing this bill because Google actively provided and distributed ads from Canadian pharmacies, leading to illegal imports of prescription drugs into the US. This was the cause for adding the protection against counterfeit drugs into this mainly technical bill for protecting intellectual property[131].

If this legislation passes the US senate it will influence everyday web-business in the US. Every service and content provider will have to verify and determine all provided content. Even content that is mainly created by users will have to be analysed and in worst case adapted or censored. This scenario can lead to some kind of legal extensive censorship. Even classic libraries with old-fashioned literature will face enormous exertions to obey this novel regulation.

In addition there are several American NGOs supported by officially decorated legal scientists who publicly warn that this bill will even have impact on online freedom of speech[132].

Even open-source software developers express their concerns about the SOPA act and comment that it can have influence on current software projects.

[130] Check the following document for more detailed information about the SOPA Act
http://judiciary.house.gov/hearings/pdf/112%20HR%203261.pdf
[131] Follow this link for detailed information about Google and illegal drug ads
http://www.theregister.co.uk/2011/08/24/google_five_hundred_million_doj_settlement_over_illegal_pharmecies/
[132] See paper written by Laurence Tribe, professor at Harvard university for detailed information
http://www.scribd.com/doc/75153093/Tribe-Legis-Memo-on-SOPA-12-6-11-1

A classic example will be the Firefox web browser developed and maintained by the Mozilla foundation. The browser itself does not violate this possible bill because it cannot verify the information it displays. However the included add-on applications that extend the functionality of the browser could be against the proposed law[133].

The technical issues combined with this law will involve a broad variety of developed technologies. It will have to include deep-packet inspection implemented at service providers. This will mainly produce possible bottle-necks which can influence the provided services. Additionally the DNS system itself will have to be adapted to easily eliminate illegal websites and services. This will require additional organizational changes within the ICANN organization. It will lead also to the broad implementation of the Domain Name System Security Extensions (DNSSEC) developed by the Internet Engineering Task Force (IETF)[134]. This specification was established to secure certain kinds of information provided by the classical DNS service used on the internet protocol (IP).

On the 16th of November 2011 most of the biggest American internet companies participated in the organised “American Censorship Day” to underline their negative attitude towards the proposed SOPA bill. They displayed black banners over their site logos with the words "STOP CENSORSHIP" [135] .In addition in January 2012 the English Wikipedia encyclopaedia decided to join the protests and turned off their services for 24 hours with a redirect to the “STOP CENSORSHIP” banner. There are estimates that more than 160 million people saw this banner during that day[136].

[133] See following article for more information about Firefox and connected add-on http://www.wired.com/threatlevel/2011/05/firefox-add-on-redirect

[134] See following article for more information about the technical topics related to the SOPA bill http://www.skatingonstilts.com/skating-on-stilts/2011/12/the-sopa-rope-a-dope.html

[135] See following article about the American Censorship Day for more information http://www.bloomberg.com/news/2011-11-16/-american-censorship-day-makes-an-online-statement-the-ticker.html

[136] See following article to find more information about Wikipedia joining the SOPA protests http://www.washingtonpost.com/business/google-says-7-million-signed-petition-against-anti-piracy-bills/2012/01/19/gIQAJ2MiBQ_story.html?tid=pm_business_pop

The bill is currently subject to the discussion state at the US senate, but it is obvious that the legal representatives are clearly divided. This bill will not come up for a vote until a consensus within the Senate will be reached.

8.2.3. Organisational Area

The organisational area proved to be the most difficult field of research to investigate. As already mentioned at the beginning of this thesis, organisations that suffered from computer crimes neglect to discuss about these incidents.

There are several explanations why those companies prefer to pretend that nothing happened. One obvious cause is the fear of loss of reputation. If a big company admits that their computer systems and networks were compromised, they will have to face a huge loss of reputation because of the breach of customer/client trust.

Another problem is that modern regulations demand public explanations and the presentation of initiated countermeasures to circumvent such situations in the future. Due to the lack of appropriate IT departments (that can protect the company in the first place!) those companies have no strategies and concepts to resolve such issues on their own.

During this research project there was an idea to contact big Austrian companies to discuss this matter of committed computer crimes and installed security systems. However none of the contacted companies responded to interview requests, often with the same comment, that they will not discuss security installations in public.

This is another organisational issue which has to be discussed. Is it better to hide any available information and pretend that the installed security system is a huge black-box? Or is it better to communicate to the public that a modern security systems was installed and show all processes in a very transparent way?

These questions have a very philosophical core but both approaches seem to be legitimate. If an attacker does not know what he is dealing with, it will be more difficult for him to achieve his goals. This is the most common approach in IT departments worldwide. This strategy is true to a certain point but what happens if an attacker gains fundamental knowledge of the system architecture and the involved security systems. The most common attack to determine such information is called “Social Engineering Attack”[137] and the most interesting part thereof is that there is no need for special sophisticated tech-skills to conduct it.

On the other hand the open-minded approach which plays with open cards is risky as well. If the installed security system has an officially unidentified security flaw and the company communicates that it is secured because of this system, sooner or later it can become the next target.

There is a similar discussion with open-source and closed-source code of computer software. Which approach is better, is a philosophical question and the answer would require an entire research project on its own.

The best strategy seems to be to combine both aspects and take the best out of both worlds. On one hand keep the security details and specific information (number of firewalls, OS, etc.) secret but let the outside world know that there are some advanced security systems installed.

To summarise this field of science the organisational area proves to be the most crucial part because there is no simple evaluation possible. The legal and technological area can be revived and presented. However the organisational area shows to be different at every analysed organisation or company because of different approaches and strategies.

[137] *“Social Engineer Attack” is the act of manipulating a person to accomplish goals that may or may not be in the “target’s” best interest. This may include obtaining information, gaining access, or getting the target to take certain action”* (Quoted from http://www.social-engineer.org/).

Companies should always take into consideration that without a working and safe IT system, their entire business concept can fail or suffer from terrible drawbacks.

8.3. Limitations of this Study

As already presented in chapter 4.4 this research project identified several limitations, which had to be considered to achieve the designated research goal.

Due to the fact of this broad field of science, following assumptions were defined. To successfully accelerate the outcome of forensic investigations the focus was shifted on malicious program code, called malware. The attempt to identify every different kind of viruses, worms and other malicious software code leads to this limitation. The scope of such an approach is definitely too broad to be of any practical use. Although this shows to be a suitable extension for this research project in the near future.

Another identified technical limitation was the operating system which was investigated in more detail. When this research project started in 2006 Windows XP was a widely common used operating system and so the focus was shifted on these machines. Nevertheless the results of this project can easily be adjusted and adapted to be suitable for novel operating systems especially from the Windows world.

Besides the technical limitations, the overall theoretical approach was to increase the efficiency of computer forensic investigations. This proved to be a very wide approach and consequently had to be defined more precisely. Based on the three general computer forensic steps, SAP – secure, analyse and present – the focus was shifted to the analysis part which showed to be the most complicated and time-consuming section. Within this fragment all forensic steps were examined separately and discussed which could be supported by developing an additional technical extension and which field would be most

promising. This limitation was mandatory for the positive outcome of this research project.

8.4. Reflections on the Research Methodology

As discussed in chapter 3, the design research method was selected to comply with requirements for the design and implementation of a novel conceptual model based on the information technology solution. Various authors discussed how models and methodologies are developed by the adoption of the design research method. This research method is especially useful for projects that require the flexibility to repeatedly return to former research results and readjust predefined assumptions. In conducting this research the design research method facilitated iterative processes in creative problem solving while defining the expected research progress by never losing the research focus.

The Venable „Design Research“ methodology presented in Figure 6, Design Research Process, in the research methods chapter closely reflects the process undertaken in this project.

The „Design Research“ framework encourages researchers to pursue reassessment of their concepts by engaging in progressive and iterative model and problem solution development. An action research aspect of the „Design Research“ is readily applicable when engaging with perspective groups where suggesting solutions and modifying design elements lead to enhancements of final products.

Over an extended period of time several iterations of the research approach led directly to desirable outcomes while dissolving undesirable characteristics of the developed product.

This study mainly focused on a limited technological development beyond a theoretical model leading to practical implementation to support forensic investigations.

During this research project several different forensic ideas and concepts were discussed and analysed. It is important to remember that the science field of computer forensics is still very young. There are constantly novel developments which lead to new approaches.

The author of this study tried to identify and support the computer forensic community by developing the CFAA prototype for automated malware inspection. The prototype functionality was tested and because of the design research approach refined several times which led to a very suitable and efficient solution. Due to the limited feedback it is difficult to evaluate the success rate at a higher scale. Within ideal circumstances the CFAA proved to be a very helpful tool which can accelerate the time consuming forensic investigations.

One other important problem for the evaluation process was to collect and analyse realistic research data from victims of crime which proved to be another limiting aspect of this research project. It would have been especially helpful for further research projects if a set of real crime cases could be prepared for automated investigations.

8.5. Future Work

This research project has several limitations that had to be introduced to support the positive outcome. These restrictions can be seen as borders that can be extended in future extensions. By adopting the limitations the scope of this project can be stretched to a broader field.

One of the first steps in this process should be the extension of the conceptual model by adding further program types to the automated investigation utility. The functionality of the CFAA prototype could be easily extended to investigate different types of known malicious software by extending the known list of malware like viruses and worms. The problem with such an extension is the need for additional resources (in a technical way) and novel concepts to handle such threats.

Another strategy could be to verify the generated results with a more accurate evaluation process to determine the efficiency of the technical prototype. This will require a set of data of realistic computer crimes that can be automatically investigated by the technical prototype.

This research work is theoretically based on the C.J. Armstrong[138] research thesis which is mainly used as the argumentation strategy. The author investigated and defined an extensive meta model which defines the forensic science. The current research project focuses on the established model and tries to develop a conceptual approach to support forensic investigators in an automated way.

Future research is necessary to verify that the established technical model remains valid and solid when adapted and combined with other novel forensic frameworks. Due to the modular structure technical extensions can be easily implemented and the functionality extended.

This research project can be considered as the technical realisation of a presented meta-model. The used research methodology can be used for other advanced meta-model testing procedures to generate realistic results.

In addition to the above areas, computer forensic still relates very closely to national legal regulations. This research thesis investigated the Austrian legal system and identified the affected legal relations. It would be very interesting to conduct similar research work on other legal systems for instance the German or French system to identify potential deficits.

Another very interesting and promising field of future work related to computer forensic would be the usage of anti-forensic techniques and approaches. What are the new strategies to counteract possible forensic investigations? How can investigators be prepared and supported to identify such actions and oppose such tactics? The outcome of this research project is a tested conceptual model

[138] See (Armstrong, 2010) for more information

with the technical implementation. This implementation can be used to implement additional strategies to overcome such anti forensic techniques.

Computer forensics is still a very young field of science. Nowadays there are very interesting and promising research projects which analyse and investigate different forensic strategies. A big problem is that computer experts try to use their well-established models and concepts to deal with computer crime incidents and related forensic analysis. Some of these approaches seem adequate, whereas most of them simply do not fit into the corresponding situation. Computer forensic investigators have to make use of the well-established and traditional forensic work enforced by modern police departments. These specialists developed strategies and concepts which can be very helpful even for current computer forensic investigations. Although the old-fashioned forensic procedures where developed and established even before modern computer systems were conceptually devised, they still seem to be relevant for modern crimes.

The areas of future work based on this research project can point into several different directions. The possible scope is very broad but the main aspects which are needed, are time, intellectual manpower and proper resource allocation for further interesting research projects.

8.5.1. Expanding the Forensic Approach

This research project focused mainly on computer forensic approaches and techniques. Another very fast growing field of science is called “Network Forensic”. Network Forensic is closely related to the field of network security although it has different goals and aims. Network forensic attempts to track down any actions and results of a successful network intrusion and in particular the criminal source of the intrusion; whereas network security deals with preventing network breaches and taking precautions.

To fully understand the term Network Forensics and the involved techniques there is a need for extended knowledge of computer networks and the structure

of the internet protocol. Network forensics systematically tries to track any incoming and outgoing traffic on the designated network. Intruders always leave some trail behind which can be investigated and analysed, similar to Computer Forensics.

Network Forensics is a long and tedious investigative process. Answers can be hidden everywhere, on Routers, NAS devices or even simple network switches. Key strategy is to determine the appropriate network logs which will lead directly to the intruder and the security flaw which was breached.

In addition to network analysis Network forensic investigations also include computer forensics techniques. Those two fields of science are closely related so the involved techniques are in some cases similar.

8.6. Concluding Research Reflections

In general, there is a growing awareness that cybercrime can have serious implications in the physical (real) world. The Austrian Federal Office of Criminal Investigation (Bundeskriminalamt) prepared a report for the year 2011 which analyses the actual situation in Austria[139]. Although the provided data does not include current figures and numbers, it shows an interesting overview of the current development of computer crimes. The discussed numbers of investigations prove that the internet is a novel world for any kind of criminal activities. New types and forms of cybercrimes evolved which automatically adapted to the changed circumstances.

[139] Based on (Bundeskriminalamt, 2012)

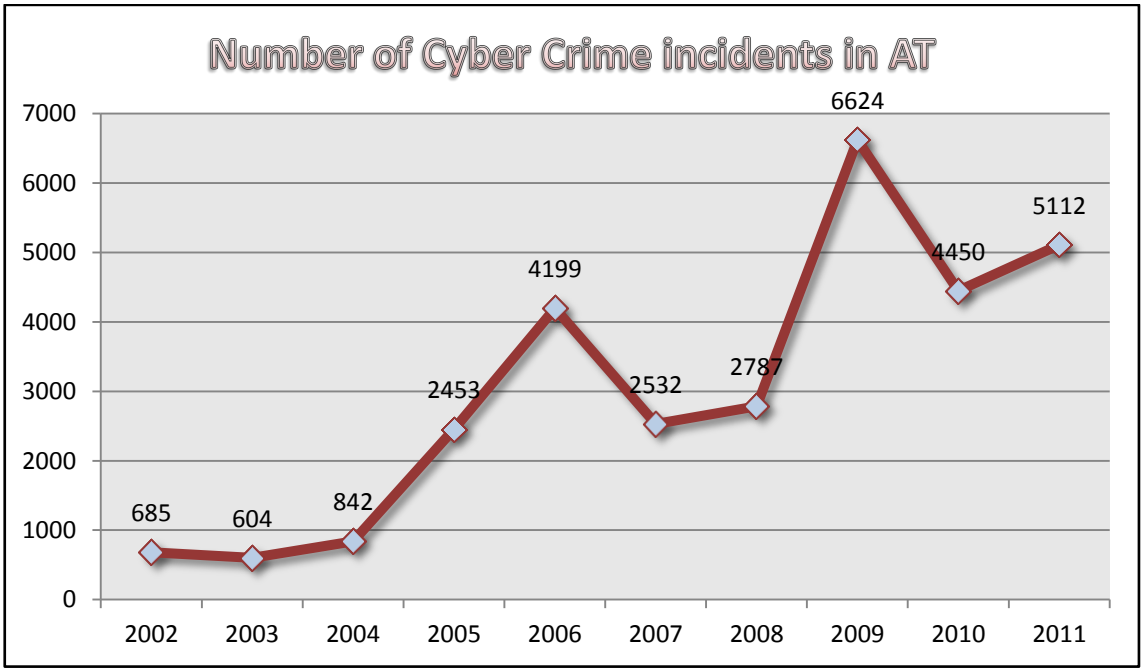


Figure 38, Number of Cyber Crime incidents in Austria 2011

Figure 38 illustrates the dramatic growth of cybercrimes only investigated in Austria. The year 2009 was exceptional as two big cybercrimes occurred with the use of automated algorithms which autonomously attacked other vulnerable computer systems. Another interesting point from the presented report is the average age of cybercriminals. Almost 50% of all cybercrimes in Austria were conducted by criminals between the age of 24 and 39. This shows that the average age is shifting towards the younger generation.

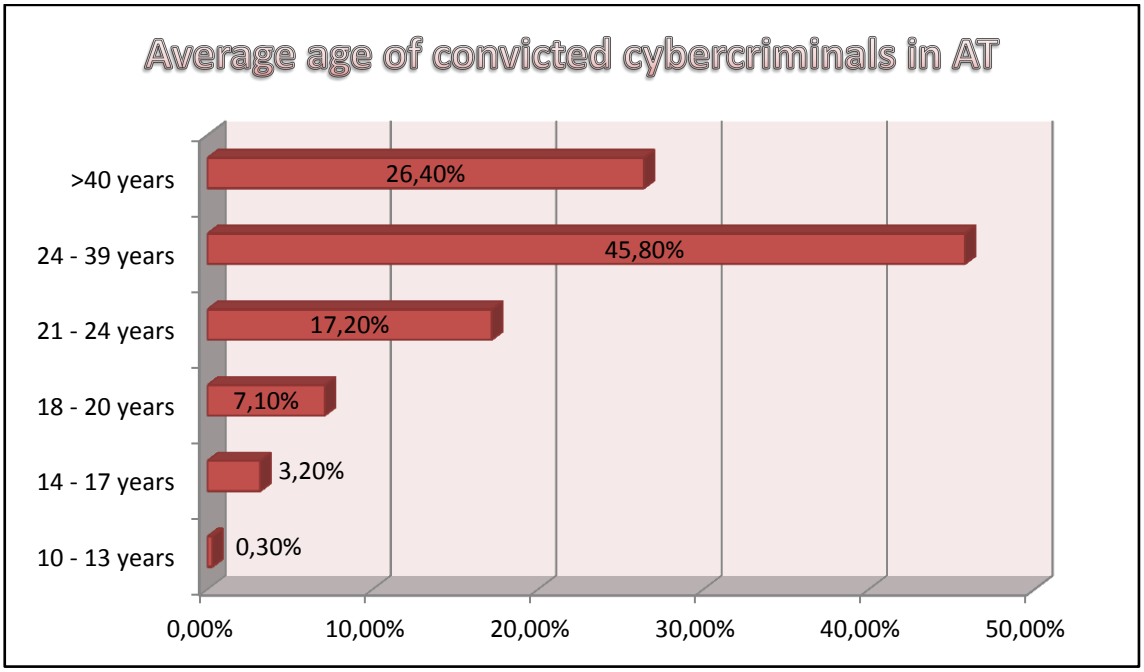


Figure 39, Average age of convicted cybercriminal in Austria[140]

The strategies to fight such computer crimes are analogue to old-fashion crimes. Nations found organisations which specialise in the investigation of specific crimes. The European Union established on the 1st of January 2013 the European Cybercrime Centre (EC3) at the Europol headquarter in Hague.

Figure 40, Official Logo of the European Cybercrime Centre

The Centre will be the focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of online crimes. It will support Member States and the European Union's institutions in building operational

[140] Figures taken from (Bundeskriminalamt, 2012)

and analytical capacity for investigations and cooperation with international partners.[141]

The aim of the EC^3 is to become the European central point to fight computer crimes, through building operational and analytical capacities for investigations. The EC^3 will have 5 main functions: Data fusion, skilled operations, designated strategy, R&D training and close contact with the private sector to respond comprehensively to cybercriminal activities.

It has to be mentioned at this point that the simultaneous growth of the internet economy, called e-commerce, contributes to the constant economic growth in Europe. If the initiated countermeasures to protect the economy fail, Europe will jeopardise the economic stability.

On the other hand those involved criminal organisations try to adapt to changed circumstances. The structure of cybercrime groups marks the cleanest break to date from the traditional concept of Organised Crime groups as hierarchical. Very often there is no obvious leadership, work is divided according to individuals' technical specialists and most members know each other only online. Online forums are therefore essential introduction and recruitment services for the digital underground economy. These both facilitate collaboration and exhibit a degree of organisation at the administrative level, enabling criminal elements to swarm together to work on specific projects. These groups are often only loosely connected to easily replace a lost node.

Moreover, it has been argued that cybercrime's organisation lies in its automation, which by using the force of technology dispenses with the operational requirement for physical groupings and force of numbers. In this context, botnets – networks of infected "zombie" computers – are crucial to cybercrime's profitability. With a botnet, cybercriminals can make use of thousands of compromised computers at a time to automate attacks on private individuals and corporate systems, send spam, host phishing websites,

[141] Cited from https://www.europol.europa.eu/ec3

distribute crime ware, mount denial of service attacks and scan for vulnerabilities: without one, they must target victims and machines manually and individually.

The monetisation of data is likewise essential to cybercriminal enterprise. “Mules” are recruited via employment search websites and social networking sites to “cash in” stolen personal and financial information, very often in different jurisdictions to those from which the funds have been removed. As the individuals tasked with turning data in hard cash, mules are the visible face of cybercrime.

The high-tech nature of cybercriminal activity results in a demographic profile not traditionally associated with transnational Organised Crime – namely, young, highly skilled individuals who are often recruited from universities. These features find analogies in hacker culture more generally, where absence of hierarchy, celebration of technical proficiency and comparative youth are prevailing characteristics. This younger offending demographic is to some extent maintained by the ready availability of exploits and attack tools on the Internet. Phishing and spamming require fewer technical skills than some other types of cybercrime, while complete crime ware kits like Zeus arguably make attacks more accessible.

The developments of web services of the 2nd generation lead to a new wave of cybercrimes 2.0. Criminals start to make use of social networks and try to distribute their malware programs with the help of security holes within the new Web 2.0 services. In many social networking sites environments exist in which users feel a sense of security. They enable cybercriminals to bypass the more work intensive aspects of social engineering so characteristic of offline and email-based attempts to elicit personal and financial information. Moreover, the unprecedented size of social networking’s user base - there are, for example, as many Facebook and Twitter accounts as there are EU citizens – provides the

digital underground economy with a ready-made means of distribution for malicious software.[142]

Web 2.0 has supported the development of services which collect personal financial information from savings and checking accounts, credit cards, investments and loans. Since these platforms enable access to a range of services with a single set of log in credentials, it is reasonable to expect that they will be of interest to criminals involved in the retail and exploitation of personal financial data.

Another current field of fast changes is the novel science called cloud computing. Individuals and organisations are increasingly opting to outsource their data storage to third parties, as a cost-saving option and to enable remote access to data from any location. This poses both a threat to users and a challenge to law enforcement.

Data stored in “The Cloud” is not only accessible to any authorised users but also vulnerable to external attacks. And whilst corporate owned servers are evidently subject to hacking, the lack of direct control entailed by cloud computing raises concerns whether security measures will be properly enforced by the storage provider or understood by the data owner and/or customer. In the cloud computing scenario, for example, the personal and financial data of retail customers can be stored on the Internet by a third party without that customer’s knowledge and without the direct control of the organisation who has processed that data. The key to cloud computing’s success and long-term uptake will be whether the convenience of remote access will be matched by confidence in its security provisions[143].

[142], Based on the INTERNET FACILITATED ORGANISED CRIME report, found here: https://www.europol.europa.eu/sites/default/files/publications/iocta_0.pdf

Due to the extensive growth and development of the technology and threats and risks coming therewith the improvement of the tools the law enforcement institution dispose of is necessary.

APPENDIX

List of References

A Design Research Approach. **Duffy, Alex H und O'Donnell, F. 1998.** Lisbon, Portugal : Workshop on Research Methods, 1998.

Aquilina, James M., Casey, Eoghan und Malin, Cameron H. 2008. *Malware Forensics - Investigating and Analyzing Malicious Code.* Burlington : Syngress Publishing, 2008.

Ardi, Shanai und Shahmehri, Nahid. 2009. A Post-Mortem Incident Modeling Method. *2009 International Conference on Availability, Reliability and Security.* 2009.

Armstrong, Colin. 2010. *A tactical management model of forensic evidence processes.* University of Western Australia : University of Western Australia, 2010.

Australian Computer Emergency Response Team. 2006. Australian Computer Emergency Response Team. [Online] 05 2006. [Zitat vom: 20. 05 2009.] http://www.auscert.org.au/images/ACCSS2006.pdf.

Bace, Smith. 2003. *A Guide to Forensic Testimony. The Art and Practice of Presenting Testimony as an Expert Technical Witness.* Boston, USA : Addison-Wesley, 2003.

Bielecki, Maximilian and Quirchmayr, Gerald. 2009. *Towards Requirements for a Case Preparation Support System Based on Digital Evidence.* Athen : s.n., 2009.

Bielecki, Maximilian. 2007. *DDoS – Distributed Denial of Service.* London : RHUL, 2007.

Boucek, Vlastimil. 2009. *Forensic Computing: Exploring Paradoxes.* Tasmania : University of Tasmania, 2009.

Bundeskriminalamt. 2012. Bundesministerium für Inneres - Bundeskriminalamt. *Cypercrime - Jahresbericht 2011.* [Online] 10. 10 2012. [Zitat vom: 01. 04 2013.] http://www.bmi.gv.at/cms/BK/publikationen/files/CybercrimeReport2011web.pdf.

Carter, David, L. 1995. Computer Crime Categories - How Techno-Criminals Operate. *FBI - Law Enforcemeant Bulletin.* 1995.

Casey, Eoghan. 2000. *Digital Evidence and Computer Crime.* Cambridge : Academic Press, 2000.

—. 2002. *Handbook of Computer Crime Investigation.* London : Academic Press, 2002.

Collins, Allan, Joseph, Diana und Bielaczyc, Katerine. 2004. Design Research: Theoretical and Methodology Issues. *The Journal of the Learning Sciences.* 2004.

Collins, Paul und Klein, Tony. Sysinfo.org. [Online] Safer-Networking Ltd.[Zitat vom: 01. 12 2010.] http://www.sysinfo.org.

Council of Europe. 2004. Convention on Cybercrime. *Council of Europe.* [Online] 01. 06 2004. [Zitat vom: 10. 02 2011.] http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm.

Department for Business, Innovation and Skills. 2013. Gov.uk. [Online] 29. July 2013. [Zitat vom: 22. February 2014.] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf.

Edwin, Sutherland. 1939. *Principles of Criminology.* Chicago : J.B. Lippincott, 1939.

European Parliament, Council . 2002. EUR-Lex. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).* [Online] 31. 07 2002. [Zitat vom: 02. 04 2013.] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT.

Free software Foundation. GNU - GENERAL PUBLIC LICENSE. [Online] [Zitat vom: 01. 03 2011.] http://www.gnu.org/licenses/gpl-3.0.txt.

Ghernaouti-Hélie, Solange. 2009. An inclusive information society needs a global approach of information security. *2009 International Conference on Availability, Reliability and Security.* 2009.

Guidance Software. EnCase by Guidance Software. [Online] [Zitat vom: 01. 11 2010.] http://www.guidancesoftware.com/forensic.htm.

—. EnCase Forensic. [Online] [Zitat vom: 20. 05 2009.] http://www.guidancesoftware.com/products/ef_index.asp.

Harris, Shon, et al. 2008. *Gray Hat Hacking - The Ethical Hacker's Handbook.* s.l. : The McGraw Hill Companies, 2008.

Heidenreich, Mario, Matthies, Christian und Strojny, Lars H. www.phpids.org. *Web Application Security 2.0.* [Online] [Zitat vom: 01. 03 2011.] http://phpids.org/.

Jayaratna, N. 1994. *Understanding and Evaluating Methodologies.* Maidenhead, England : McGraw Hill, 1994.

Kellermann, Tom. 2012. Trendmicro. [Online] 20. 09 2012. [Zitat vom: 24. 09 2012.] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/op_kellermann_peter-the-great-vs-sun-tzu.pdf.

Korosides, Konstantin. 2009. Netzwelt - Skandalgerichts-Entscheidung in Frankfurt. [Online] 17. 03 2009. [Zitat vom: 01. 11 2010.] http://www.netzwelt.de/news/79623-kommentar-skandalgerichts-entscheidung-frankfurt.html.

Lee, Jooyoung, Un, Sungkyung und Hong, Dowon. 2009. Improving Performance in Digital Forensics by using pattern matching board. *2009 International Conference on Availability, Reliability and Security.* 2009.

McAfee. 2012. www.mcafeee.com. [Online] 01. 02 2012. [Zitat vom: 31. 05 2012.] www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf.

Nelson, Bill, et al. 2006. *Guide to Computer Forensics and Investigations.* Boston : Thomson - Course Technology, 2006.

Osborne, Grant und Turnbull, Benjamin. 2009. Enhancing Computer Forensics Investigation through Visualisation and Data Exploitation. *2009 International Conference on Availability, Reliability and Security.* 2009.

Pontell, Henry N. und Geis, Gilbert. 2007. *International handbook of white-collar and corporate crime.* Irvine : Springer, 2007.

Privacy and security concerns as major barriers for e-commerce: a survey study. **Godwin, Udo J. 2001.** s.l. : MCB UP Ltd, 2001.

Richardson, R. 2008. CSI Computer Crime and Security Survey 2008. [Online] 2008. [Zitat vom: 20. 05 2009.] http://www.gocsi.com/forms/csi_survey.jhtml.

Seger, Alexander. 2007. Council of Europe - Cybercrime. [Online] 30. 05 2007. [Zitat vom: 01. 02 2011.] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/567-LEG-country%20profile%20Austria%20_30%20May%2007_En.pdf.

Senate, US. 2012. Combating Online Infringement and Counterfeits Act. [Online] 01. 03 2012. http://www.govtrack.us/congress/bills/111/s3804/text.

—. 2012. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011. [Online] 01. 03 2012. http://www.govtrack.us/congress/bills/112/s968/text.

Shinder, Debra L. und Tittel, Ed. 2007. *Scene of the Cybercrime - Computer Forensics Handbook.* Rockland : Syngress Publishing, 2007.

Simon, Matthew und Slay, Jill. 2009. Enhancement of Forensic Computing Investigations through Memory Forensic Techniques. *2009 International Conference on Availability, Reliability and Security.* 2009.

Skoudis, Ed. 2004. *Malware - Fighting malicious code.* New Jersey : Pearson Education, 2004.

Socialweb. 2013. socialweb.com. *Why Reactive IT Security Practices Don't Work Anymore.* [Online] 09. 04 2013. [Zitat vom: 11. 04 2013.] http://www.sociablweb.com/why-reactive-it-security-dont-work-anymore.

Society, The Design Research. The Design Research Society. [Online] [Zitat vom: 03. September 2011.] http://www.designresearchsociety.org.

Steinberger, Richard. 2012. crime-research.org. *Proactive vs. Reactive Security.* [Online] 2012. http://www.crime-research.org/library/Richard.html.

Strafprozeßordnung, Republic of Austria -. 2009. RIS. *RIS.* [Online] 01. 06 2009. [Zitat vom: 27. 10 2010.] http://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR30007163/NOR30007163.pdf.

Symantec. Symantec. *Malware.* [Online] [Zitat vom: 01. 11 2010.] http://uk.norton.com/security_response/malware.jsp.

Sysinfo.org. Sysinfo.org. [Online] [Zitat vom: 01. 03 2011.] www.Sysinfo.org.

Szor, Peter. 2005. *The Art of Computer Virus Research and Defense.* USA : Symantec Press, 2005.

Team, Computer Emergency Response. 2002. Organized Crime and Cyber-Crime: Implications for Business. [Online] 2002. http://www.cert.org/archive/pdf/cybercrime-business.pdf.

The Network Group. 2002. RFC3227 - Guidelines for Evidence Collection and Archiving. [Online] 2002. [Zitat vom: 20. 05 2009.] http://www.faqs.org/rfcs/rfc3227.html.

The Opensource Inititative. The Opensource Inititative. *Common Public License Version 1.0 (CPL).* [Online] [Zitat vom: 25. 11 2010.] http://www.opensource.org/licenses/cpl1.0.php.

The Sleuth Kit. The Sleuth Kit. [Online] [Zitat vom: 24. 11 2010.] http://www.sleuthkit.org/sleuthkit/desc.php.

Treaty, Multinational. 2012. Anti-Counterfeiting Trade Agreement. [Online] 01. 03 2012. http://www.international.gc.ca/trade-agreements-accords-commerciaux/assets/pdfs/acta-crc_apr15-2011_eng.pdf.

Trend Micro. 2012. Trendmicro.com. *Inside an APT - Campaign with Multiple Targets in India and Japan.* [Online] 03 2012. [Zitat vom: 24. 09 2012.] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf.

—. 2012. Trendmicro.com. *The Tinba/Tinybanker Malware.* [Online] 12. 09 2012. [Zitat vom: 24. 09 2012.] http://blog.trendmicro.com/trendlabs-security-intelligence/the-tinbatinybanker-malware/.

US. Department of Justice. 2008. Electronic Crime Scene Investigation: A Guide for First Responders. *National Institute of Justice.* [Online] 01. 04 2008. [Zitat vom: 24. 11 2010.] http://www.ncjrs.gov/pdffiles1/nij/219941.pdf.

Vacca, John R. 2005. *Computer Forensics - Computer Crime Scene Investigation.* Massachusetts : Charles River Media , 2005.

Venable, JR. 2006. *A Framework for Design Science Research Activities.* Washington, DC : Ideal Group Publishing, 2006.

Whitman, Michael E und Mattord, Herbert J. 2012. *Principles of Information Security.* Boston : Cengage Learning, 2012.

Wikipedia. 2012. Wikipedia. [Online] 20. 02 2012. http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement.

—. Wikipedia - EnCase. [Online] [Zitat vom: 01. 11 2010.] http://en.wikipedia.org/wiki/EnCase.