

DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

**DEVELOPMENT OF A FRAMEWORK FOR
CYBER CRIME INVESTIGATION**

by
Ayşe OKUTAN

October, 2019
İZMİR

DEVELOPMENT OF A FRAMEWORK FOR CYBER CRIME INVESTIGATION

**A Thesis Submitted to the
Graduate School of Natural and Applied Sciences of Dokuz Eylül University
In Partial Fulfillment of the Requirements for the Degree of Master
in Computer Engineering**

**by
Ayşe OKUTAN**

**October, 2019
İZMİR**

M.Sc THESIS EXAMINATION RESULT FORM

We have read the thesis entitled “**DEVELOPMENT OF A FRAMEWORK FOR CYBER CRIME INVESTIGATION**” completed by **AYŞE OKUTAN** under supervision of **PROF. DR. YALÇIN ÇEBİ** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.


.....
Prof. Dr. Yalçın ÇEBİ

Supervisor


.....
Assoc. Prof. Dr. Gökhan DALKILIÇ

(Jury Member)


.....
Asst. Prof. Dr. Enis Karaarslan

(Jury Member)



Prof. Dr. Kadriye ERTEKİN

Director
Graduate School of Natural and Applied Sciences

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisor, Prof. Dr. Yalçın ÇEBİ for his immense knowledge, continuous support, supervision and useful suggestions throughout this study. From the very first day, he has always encouraged me. His guidance helped me in all the time of my research and writing of this thesis.

Also, I would like to offer my special thanks to my mother, my father and my brother for supporting me spiritually throughout writing this thesis in general. It would not have been able to complete this thesis without their support and help.

Ayşe OKUTAN

DEVELOPMENT OF A FRAMEWORK FOR CYBER CRIME INVESTIGATION

ABSTRACT

In recent years, as a result of the widespread use of the internet and the development of technology, the number of users meeting the needs of technological tools has increased considerably. With information systems that make a rapid entry into people's lives, users are either consciously or unconsciously committing a crime or being exposed to a crime. As these crimes take up a lot of space in daily life, there is a need to redefine information crimes. Thus, private law rules and methods of finding evidence emerged. Even though all these needs have been started to be fulfilled, the integrity of the existing order has not been achieved. In particular, there are not enough resources on the methods required to detect the offender.

In this thesis, legal legislation and crime types have been examined and forensic informatics steps have been included for the determination of evidence. By gathering these data, the necessary steps to identify the perpetrator have been transformed into a chain of events and a new framework has been established for information crimes. This framework makes it easy to identify the perpetrator and makes it easier to identify gaps in cybercrime. In order to, overcome these shortcomings, which are determined in the field of legislation and in the technical field, a solution proposal is also included in this thesis.

Keywords: Informatics crimes, forensic informatics, evidence detection, detection of the offender, legislation

BİLİŞİM SUÇLARININ İNCELENMESİ İÇİN BİR ÇERÇEVE GELİŞTİRİLMESİ

ÖZ

Son yıllarda internetin yaygınlaşması ve teknolojinin gelişmesinin sonucu olarak, teknolojik aletler ile ihtiyaçlarını karşılayan ki sayısında oldukça artış olmuştur. İnsanların hayatına hızlı bir giriş yapan bilişim sistemleri ile kullanıcılar bilinçli veya bilinçsiz şekilde suç işlemekte veya bir suça maruz kalmaktadır. Bu suçlar, günlük hayatta oldukça fazla yer kaplamaya başladığı için bilişim suçları adı altında yeniden bir tanımlama yapılması ihtiyacı doğmuştur. Böylelikle kendine özel hukuk kuralları ve delil tespit etme yöntemleri ortaya çıkmıştır. Tüm bu ihtiyaçlar giderilmeye başlanmış olsa dahi mevcut düzende bir bütünlük sağlanamamıştır. Özellikle suçluyu tespit etmek için gerekli yöntemler hakkında yeterli kaynağa rastlanmamıştır.

Bu tezde, yasal mevzuat ve suç türleri incelenmiş, ayrıca delil tespiti için adli bilişim adımlarına yer verilmiştir. Bu veriler bir araya toplanarak suçluyu tespit etmek için gerekli adımlar bir olay zinciri haline dönüştürülmüş ve böylelikle bilişim suçları için yeni bir çerçeve oluşturulmuştur. Bu çerçeve, suçlunun tespit edilmesi için kolaylık sağlar ve siber suç alanında eksiklerin daha kolay fark edilmesine olanak sağlar. Mevzuat alanında ve teknik alanda tespit edilmiş bu eksikliklerin giderilebilmesi için çözüm önerisine de bu tezde yer verilmiştir.

Anahtar kelimeler: Bilişim suçları, adli bilişim, delil tespiti, suçlu tespiti, mevzuat

CONTENTS

Page

M.Sc THESIS EXAMINATION RESULT FORM.....	ii
ACKNOWLEDGEMENTS	iii
ABSTRACT	iv
ÖZ	v
LIST OF FIGURES	ix
LIST OF TABLES	xi
 CHAPTER ONE - INTRODUCTION	 1
1.1 Computer Forensic and Cybercrime.....	1
1.2 Purpose	2
1.3 Organization of the Thesis	2
 CHAPTER TWO - RELATED WORKS	 4
2.1 Cyber Crime Perspective.....	4
2.2 Forensic Informatics Perspective	6
2.3 Technical Perspective.....	12
2.4 Law Perspective	18
2.5 Security Perspective	24
 CHAPTER THREE - LEGISLATION AND FORENSIC PROCESSES IN TURKEY.....	 26
3.1 Legislation in the Turkey	26
3.1.1 Article of the Constitution (Art. 20.)	26
3.1.2 Turkish Penal Code (TPC)	27
3.1.3 Electronic Signature Law (5070).....	35
3.1.4 Intellectual and Artistic Works Law	35
3.1.5 Anti-Smuggling Law	36
3.1.6 Publishment on Internet (5651)	36
3.1.7 Criminal Procedure Code Computer Investigation	36

3.1.8 Judgment No. 2012/3842 About Cyber Security.....	37
3.2 Forensic Informatics Processes in Turkey.....	37
3.2.1 Evidence Detection.....	38
3.2.2 Evidence Collection and Preservation.....	40
3.2.3 Evidence Extraction.....	42
3.2.4 Evidence Analysis	45
3.2.5 Evidence Organization	47
CHAPTER FOUR - INFORMATICS CRIME.....	49
4.1 Cyber Attacker Profile.....	50
4.2 Informatics Crime Categories	51
4.3 Common Cybercrimes and Their Properties	53
CHAPTER FIVE - TOOLS OF INFORMATICS CRIME INVESTIGATION	67
5.1 Digital Evidence	67
5.2 Types of Digital Evidence	68
5.3 Forensics Software, Hardware and Other Tools	72
5.3.1 Image Retrieval Tools	73
5.3.2 Analysis Tools	76
5.3.3 Make Inferences Tools	77
5.3.4 Control Tools.....	78
5.3.5 Platform Tools	79
5.3.6 Additional Tools	79
5.3.7 Accessories	80
CHAPTER SIX - A FRAMEWORK FOR CYBER CRIME INVESTIGATION	82
6.1 Confronting Crime	82
6.2 Steps to Find Cyber Criminals	85
6.2.1 Detecting a person who commit a crime with e-mail.....	85

6.2.2 Detecting a person who commit a crime with web	95
6.2.3 Detecting A Person Who Insults on Social Media	98
6.2.4 Detecting Man in the Middle Attacker	100
6.2.5 Detecting Ransomware Attacker	105
6.2.6 Detecting DDoS Attacker	111
6.3 Training Recommendations for Those Who Fight Cybercrime	118
6.4 Legal Requirements in the Fight Against Cybercrime	123
CHAPTER SEVEN - CONCLUSION AND FUTURE WORK	127
7.1 Conclusion.....	127
7.2 Future Work	128
REFERENCES.....	129
APPENDICES	143
Appendix 1: Definitions	143
Appendix 2: List of Abbreviations.....	145

LIST OF FIGURES

	Page
Figure 6.1 Confronting crime.....	83
Figure 6.2 What to do when faced with cybercrime	84
Figure 6.3 What to do when faced with cyber attacks	85
Figure 6.4 IP by "Received from"	86
Figure 6.5 Framework for identifying an offender by e-mail	87
Figure 6.6 Whois Process” in e-mail framework	88
Figure 6.7 Query with IP address.....	88
Figure 6.8 Domain and IP information with RIPE	89
Figure 6.9 “Whois” query with domain name	90
Figure 6.10 “Email Firm Process” in e-mail framework	91
Figure 6.11 “ISP Process” in e-mail framework.....	92
Figure 6.12 “Firm Process” in e-mail framework.....	94
Figure 6.13 Framework for identifying an offender by web.....	95
Figure 6.14 Example of questioning in which city IP is located	96
Figure 6.15 “DNS Firm Process” in web framework	97
Figure 6.16 “FingerPrint Method” in web framework.....	98
Figure 6.17 Social media framework.....	100
Figure 6.18 Detecting the attacker's IP address with Wireshark.....	101
Figure 6.19 Detecting the attacker's computer name with Cain & Abel.....	102
Figure 6.20 MITM framework.....	103
Figure 6.21 Monitoring the MAC address of a system in communication.....	104
Figure 6.22 Finding a manufacturer with MAC address.....	104
Figure 6.23 Ransomware framework.....	107
Figure 6.24 An example of an attacker's message on the computer with virus	108
Figure 6.25 Example that files on the victim computer are encrypted	109
Figure 6.26 Example of running malicious software “amdqkacroic.exe”	110
Figure 6.27 Screenshot of a virus-detected site in VirusTotal	110
Figure 6.28 Framework for identifying an offender by DDoS	111
Figure 6.29 “Find Log” part in DDoS framework	112
Figure 6.30 “Check Protocol Types” part in DDoS framework	113

Figure 6.31 “UDP” part for analyze attacks in DDoS framework.....	114
Figure 6.32 “TCP” part for analyze attacks in DDoS framework.....	115
Figure 6.33 “SMTP, HHTP, ICMP” part for analyze attacks in DDoS framework	117
Figure 6.34 “Find Country” part in DDoS framework	118



LIST OF TABLES

Page

Table 3.1 Crimes are described as information technology crime only.....	27
Table 3.2 Crimes are not described as information technology crime only.....	31
Table 4.1 According to their forms of operation	52
Table 4.2 According to regulation of the legislation	52
Table 4.3 According to violance	53
Table 6.1 Device information description.....	106
Table 6.2 Operating system information product name.....	108
Table 6.3 Technical information of the offender file obtained by FTK.....	109

CHAPTER ONE

INTRODUCTION

1.1 Computer Forensic and Cybercrime

In today's world, technology has entered all areas of daily life, business and public safety. As technology develops and enters more lives, critical data and millions of pounds circulate openly for attacks in the cyber space of the world. Because of the personal information of individuals in cyberspace, the technologies used should be stable, reliable and flexible. Because today, cyber criminals use computers, computer networks, mobile devices and smart devices for bad purposes.

The place of informatics in our lives reveals the important point where informatics security comes. With the continuous development of technology and the rapid spread of information and communication technology tools, it has become very easy to reach information in our age. The information is wanted at home, in the park, at school, anywhere in the journey is easily accessible. Today, information systems are becoming widespread due to many reasons such as increasing productivity, accelerating workflows, faster communication with employees and other institutions, and facilitating our daily lives. As a result of the developments in information technologies, central structures have been replaced by distributed architectures, electronic applications that can be accessed via the Internet and networks. As a result of the increase in the use of electronic information infrastructures such as web applications, remote accesses, online systems, computer networks and the internet, e-concepts have become a part of our daily lives.

The concept of crime has been reshaped with all these developments. It has caused many types of crime to emerge or change the environment. New crime definitions have been made and are still being made. Law rules have also been revised. Security measures have also shifted to different dimensions. There are many studies under the title of IT crimes. At the same time academics have introduced many research about the added decisions and laws in the field of law. The concept of forensic informatics

has also been added to these studies and many theses related to the methods of obtaining evidence have been revealed.

There are many factors and areas involved in cybercrime. Forensic tools, policies, legal data, security concepts, risk management, trainings, applications, institutions and organizations, computing equipment, personnel, infrastructures, telecommunication systems and all information transmitted and stored in cyberspace. Although it covers such a large area, all the works that have been done so far have been handled from a single framework. The relevant studies have been examined only within the area of interest of individuals. Examining different areas such as law, technology, security, risk and telecommunication that are chained together in the cyber world cause interruptions. When the concepts examined by experts in the field come together, there are gaps in between. However, there have been almost no studies on the methods to be followed in order to identify criminals.

1.2 Purpose

The aim of this study is to gather the subjects examined in different fields in the cyber world in one place and to provide a single-handed analysis of the distributed system. The aim of this thesis is to examine how the detection of bad software crimes such as viruses, trojans or keyboard readers, or theft of bank accounts belonging to individuals in the cyber world, and to analyze what the legal provisions are. In this context, the content of this thesis has been studied until now. Turkey's legislation is interpreted, it is described steps that follow the law enforcement agencies. Types of informatics crime are defined. Most importantly, the steps taken to identify the perpetrator are discussed and what needs to be corrected in the system is mentioned.

1.3 Organization of the Thesis

This thesis is organized in seven chapters and the remainder of the thesis is structured as follows:

In Chapter 2, cybercrime, forensic informatics studies, legal and technical studies on informatics crimes, researches, theses and articles about cyber security are given.

In Chapter 3, the legal legislation is examined on cyber crimes and the stage is examined after the crime of informatics. It provides information on how to obtain evidence to identify the perpetrator.

In Chapter 4, firstly the profile of informatics offenders is examined. Afterwards, IT crimes were categorized and information was given about the details of IT crimes.

In Chapter 5, what is digital evidence is mentioned and the types of evidence are explained. Then, the software and hardware tools used to obtain evidence are mentioned.

In chapter 6, in the first part, the framework for six cyber crimes is established. These frameworks contain the steps to be followed to identify the information offender. In the second part, it is mentioned in which fields the persons who identify the information criminals should specialize. Suggestions were made for the trainings to be taken. In the last part, suggestions are given for the changes that should be made in order to better implement the legislation.

Finally, in Chapter 7, some concluding remarks and future directions were presented.

With the advancement of computer technology, crime rate increases in computer and internet environment. Evidence-bearing elements should be reported by trained and experienced experts.

CHAPTER TWO

RELATED WORKS

In this chapter, lots of research in relation to the cyber world presented and explained in detail to provide an overview of how can be applied deal with different problems. The present studies clearly show that it has created a perception that researchers are specialized only in their fields. This review also shows that a new framework should be created and a study covering all areas should be developed.

The studies examined were grouped under five headings. Cyber Crime, Forensic Informatics, Technical, Law, Security Perspective were collected in five different groups

2.1 Cyber Crime Perspective

Two interchangeable terms “cybercrime” and “computer crime” are adopted to its subject matter. Then, their relationships to two terms ‘economic crime’ and “intellectual property infringement”, which on some occasions may overlap with the subject of this research, are examined (The Council of Europe, 2001).

There are studies that are focused on online cybercrime. Because crime areas also differ according to whether there is an internet network or not. A research attempted to identify a potential set of circumstances that create an environment in which people are more likely to engage in cybercrime. Behavior on the internet, crime perceptions and resources on the Internet. As a result, they are combining to create an environment in which people more readily engage in cybercrime. The others the nature of behaviors online and the landscape of the world-wide web combined with current attitudes towards cybercrime create an environment that encourages people to more readily engage in criminal activities online (Kirvan, 2017). Another research is analyzed how online cybercrime groups form, organize, and operate in this thesis. It reflected on the group element of cybercrime targets of online crime. The research forms the basis for thorough understanding of online criminal groups and encourages discussions on how they might be unraveled and potentially even thwarted (Nurse & Bada, 2018). The

other one says a concise review of literature that has investigated how and why the Internet provides special opportunities to commit crime, and what this implies for the governance of cybercrime. It sketches some typologies of cybercrime and lists some risk factors of the Internet provide a structure for crime (Koops, 2010). On the other hand, one research reviews various types of cybercrimes and the Internet's overall effect on the evolution of crime. Because, millions of people across the globe are affected by online crime every day. Cybercrime has become one of the most threatening and difficult problems for law enforcement, the judicial system and the public at large (Norden, 2013).

Due to the intertwining of banking transactions with technology, the majority of cybercrime accounts are account theft and fraud. One of the studies examining these problems says the information technology has become the foundation for communications, banking, transformation. Organizations computers, servers and laptops have, therefore, increasingly become targets of crime and tools for committing crimes. The risk of terrorist organizations turning their attention to technology and cyberspace is very real (Rogers & Siegfried, 2012). Another study is aimed at investigating the fear of Cybercrime which is credit card fraud victimization. Binary Logistic Regression and Cross tabulation were used to predict both fear and risk of cybercrime victimization. The findings of the study indicate that prior experience of victimization and internet use behaviors. They are both positively associated with students' fear and their risk of becoming victims of credit card fraud (Abdulai, 2016).

There are also studies linking facilitation of crimes to different reasons. One of these studies, the broad state-of-the-art research in cybercrime intelligence in order to identify existing research gaps. Aim is designing and developing a multipurpose framework that is able to fill these gaps using a wide range of techniques. This present an outline of a framework designed to aid law enforcement in detecting, analyzing and making sense out of cybercrime data (Nouh, Nurse & Goldsmith, 2016). The other study work to raise awareness regarding legal loopholes and enabling technologies, which facilitate acts of cybercrime and objective of this research encourages policy

makers to reevaluate strategies for combating the ubiquitous and evolving threat posed by cyber criminality (Brown, 2015).

Cybercrime is the problem of every country today. Therefore, there are studies in which researchers deal with problems in their own countries. For instance, Kenya has cybercrime indeed a major problem. Cybercrime is not common, but there is a lack of trust in law enforcement. The conclusion of this study Internet users and institutions are learned on steps to take victims of cybercrime (Kangogo, 2008). Different a work presents a refined and comprehensive taxonomy of cybercrime and demonstrates its utility for widespread use. It analyses how the USA, the UK, Australia and the UAE align with the CoE Convention and finds that more needs to be done to achieve conformance. This paper with an analysis of the approaches used in Australia, in Queensland, and in the UAE, in Abu Dhabi, to fight cybercrime and identify a number of shared problems (Alkaabi, Mohay, McCullagh & Chantler, 2010).

2.2 Forensic Informatics Perspective

The digital judicial investigation processes published in the literature are summarized. In summary, he stated that it would be unwise to depend upon “audit trails and internal logs” in digital forensics investigation. In addition, he noted that a future digital forensics investigation process will only be possible if future tools and techniques make a proactive effort at evidence collection and preservation (Garfinkel, 2010). In many organizations, a thesis explaining that the incident response team is currently carrying out evidence collection activities has been prepared. The need for collecting those evidence and preserving it in a systematic proactive approach still an open issue (Rowlingson, 2004).

In order to conduct anti-forensic research, a study was suggested that organizations should decide early on which information they will collect and protect in a forensic manner (Garfinkel, 2007). In a different study explain digital forensics is a synonym for computer forensics as the use of scientific methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and

presentation of digital evidence derived from digital sources for the purpose of facilitation (Reith, Carr & Gunsch, 2011).

Believe that corporate security investigators are making increasing use of computer forensics in areas such as fraud, the accessing of pornography, and harassment and traditional criminal investigations need to be supported with digital collection and analysis tools and techniques. This need has led to the development of digital forensic science and specifically computer forensic (Krutz et al., 2007).

Digital forensic investigation is defined as the application of scientific, systematic and proven methods towards the preservation, collection, validation, identification, analysis, interpretation. Presentation of digital evidence are derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal. This study says digital forensic investigators were constantly tried to find better and more efficient ways of uncovering evidence from digital sources (Palmer, 2001).

In the traditional tool design, the study says that it is up to the auditor to control each source of digital evidence as a binary large object and analyze the relevant items from evidence. There is a wide range of forensic and analysis tools available to investigate digital evidence available today (Raghavan, 2013).

A multi-perspective cybercrime investigation process modeling that can be considered as a basis for standardization has been conducted. This model is constructed by extending and unifying the existing approaches. This paper, investigation is required to be done in order to extend the defined model by taking into consideration the detection of an attack in order to trigger the investigation process (Achille, 2012).

A research model that combines, generalizes and extends existing models is presented. Unlike, previous models, this model is explicitly represented the information flows in an investigation and captures the full scope of an investigation,

rather than only the processing of evidence. It provides a basis for the development of techniques and especially tools to support the work of investigators (Ciardhuáin, 2004).

There is work supporting intelligent software in digital forensic investigation that helps maintain the integrity of digital evidence. This is digital forensics can be helped as the use of scientifically derived and proven methods and techniques for the identification, preservation, reconstruction, and presentation of digital evidence derived from digital devices found to be an attack or incident (Ademu, 2013).

The article states that live forensic research is blocked due to lack of definitions of live forensic medicine and standard procedures in live research. In addition, the authors suggested the automation and activation of evidence-collection tools in live investigations. This automation should involve minimal user intervention to improve the integrity of the evidence. Thus, a multi-component view of the digital forensic investigation process has been proposed (Grobler, Louwrens & Solms, 2010).

An article proposing a standard for digital evidence to be used in reports generated using computer forensics tools. The authors focused on developing a standard digital evidence items by surveying various digital forensic tools while keeping in mind the legal integrity of digital evidence items. Research results enabled the authors in creating a defined XML schema for digital evidence items. This paper proposed a standard data requirement for digital evidence items, that could be used in reports generated using computer forensic tools (Bariki, Hashmi & Baggili, 2010).

A unified version is planned for physical crime and cybercrime analysis. This approach uses data mining techniques for crime detection and criminal identity for physical crimes and digitized forensic tools for evaluating cybercrimes. This work digitized technique aids the development of the society by helping the investigation businesses to follow a custom-built investigative technique in crime analysis and criminal identification as opposed to manually looking the database to analyze criminal activities. Classification and clustering techniques are uses for analyzes.

Criminals are recognized culprits and propose a coordinated innovation for both cyber and physical crime. This work can state that with a specific end goal to recognize physical crime for criminal distinguishing proof by filtering the number of suspected lawbreakers (Jain, Bhanushali, Gawade & Jawale, 2016).

An article was written about the details of cyber forensics as well as vital information about the different tools that work in the digital forensic process. It includes forensic analysis of encrypted drives, disk analysis, analysis toolkit, volatile memory analysis, captures and analyzes packets on network. the need to devise effective methodologies and develop efficient tools to detect these attacks timely. This research provides a provisional study of the tools regarding cyber forensic analysis (Kaur at al., 2016). A study investigating the deletion of electronic evidence was conducted. The system is start with collecting the related work and analyzes the organizations security policies and strategy, finding out the security level of the computer systems, the work situation for staffs the personnel secures awareness level (Zhou & Jiang, 2012).

The investigative capabilities of law enforcement have been worked previously in needs assessments and analyses conducted on issues involving digital forensics (Peterson & Sommers, 2010). A study was conducted to analyze cyber criminals similar to those used in law enforcement practices. Computer Forensic Analyzer demonstrates an approach of a fully automated system that supports investigators by independently identifying malicious software and programs (Bielecki & Quirchmayr, 2010).

An article explaining the complexity of computer systems and the preparation of computer piracy tools and techniques and computer forensic analysis techniques is very important. Forensic investigation aim is to analyze malicious executable files that hackers might have installed in an intended system. Some techniques are uses for this work and it able to detect any modified malicious programs without executing the program (Park, Kim, Noh & Joshi, 2006).

Information was given about what to do after cyberattacks. He mentioned in detail the images of the authorities to take during the forensic analysis against spy activities and the network traffic to be monitored (Ansar, 2016). Protecting the confidentiality of data is explained and research has been carried out in order to eliminate personal data which is not related to the analysis in computer forensic examination. In the modern world, the massive use of computers develops a huge amount of private data and there is correspondingly an increased expectation to recognize and respect human rights in digital investigation (Frank et al., 2011).

In order to encode semantic knowledge of evidence, a study was introduced that introduced a proof management methodology. A structured vocabulary of terms, ontology, is used to model the results in a logical and predefined manner. The encoded descriptions aim to help the investigation in the task of report writing and evidence communication and can be used in addition to existing evidence management techniques (Kahvedžić & Kechad, 2016). Since various digital forensic procedures involved in cybercrime research are considered to be necessary, a detailed investigation of various cybercrime needs is done. Then details are explained their advantages, disadvantages, challenges, and drawbacks for digital forensics tools. Finally, the paper recommends the need of training programs and judgement of signature base image authentication (Sansanwal et al., 2017).

The use of personal computers used in daily life was preferred and thus the thesis was tried to reveal the relationship between computer memory and forensic information. With this study; memory reviews in forensic informatics, it is possible to access operating system, social media, e-mail passwords, visited web site information, running applications, commands entered from the command line (Bolat, 2015).

Research has been conducted in the United States and the importance of digital evidence for the judicial justice community has been explained. In one case, an example of how digital forensics could be central to closure and prosecution was presented. Demonstrated how digital evidence missteps can have serious implications and highlighted the challenges for modern investigation when digital evidence is

limited or does not exist (Goodison, Davis & Jackson, 2016). The investigation of cybercrime in hacking and phishing in the Netherlands has been examined. This paper looked at the functioning of the Dutch police regarding cybercrime. The Dutch police are insufficiently organized to combat cybercrime. As a result, there is the lack of priority and proper capacity throughout the entire police organization to fight digital crimes (Leukfeldt, Veenstra & Stol, 2013).

Cybercrime challenges have been said to be technical difficulties that prevent the availability of law enforcement agencies to detect and prosecute criminals who work online, legal challenges arising from the law, and the inability to capture technological, structural and social changes (Rogers & Siegfried, 2004). Since the success of law enforcement officers in the investigation of information offenders is uncertain, the study has been carried out on how to improve it. The law enforcement officers conduct these investigations for many years. It found that there were no training, tools or personnel to conduct the investigation. This study has been discussed on cybercrime, reasons for conducting a digital forensic investigation, various branches of digital forensics in details, and What the Future Holds in the Field of Digital Forensics (Mugisha, 2015).

The thesis that the crimes committed in the field of informatics has increased rapidly all over the world and that the problems in the follow-up of these crimes have increased due to various reasons. He argues that these reasons are new for the law enforcement and the judicial authorities, both for the internet environment and for information crimes, and that there is no shortage of knowledgeable and experienced personnel on the subject. It requires law enforcement and judicial authorities to work in cooperation with both domestic units and other country units. However, although other countries are experiencing the same problem, there is still a long way to go in terms of cooperation, especially for our country (Orta, 2015).

The methods used frequently in information crimes and how they can be processed quickly by explaining the offender and victim profiles of criminals are explained. Also, computer, information systems and internet concepts, and the work carried out by the

General Directorate of Security, which is the law enforcement agency in charge of combating these crimes, and our suggestions on these issues are included. As a result, suggestions have been made to increase the social and institutional awareness in the fight against cybercrime and the measures to be taken and the situation of the Police Service in charge of combating these crimes have been tried to be examined (Alaca, 2008).

The concepts of cybercrime, forensic informatics and evidence are briefly defined and the measures taken by the states up to this time are mentioned. The findings obtained by examining Turkey and in the world of computer forensics training and programs to remedy the deficiencies and the results were evaluated (Orakcı, Kök & Çakır, 2016). The policy developed by the General Directorate of Security (EGM) in the fight against cybercrime has been analyzed with the Classical Approach Model in the public policy process. The legislative arrangements issued by EGM in the fight against cybercrime, the technical units it has established, the personnel policy and the factors that push them to develop these policies have been examined. It has been seen that EGM has accelerated its policies in the fight against cybercrime with the introduction of a number of legal regulations and the state's emphasis on the fight against cybercrime after the 2003s (Taşcı & Can, 2015).

2.3 Technical Perspective

Informatics crimes contain the concept of law because of the scope of the crime, but the technical part predominates. While most of the detection phase is applied to technical tools or ways while committing these crimes, technical studies have attracted the attention of the researchers, and many theses have been presented and examined technically. One of these studies is the current state of the Internet environment and the reasons why tracking and tracing cyber-attackers is so difficult. And examines some promising research on technical approaches that may greatly improve the ability to track and trace cyber-attacks to their source. The report concludes with a closer look at technical and policy considerations for next-generation Internet protocols to enhance track and trace capabilities. This report has described the problems and shortfalls in the current Internet environment and has described research approaches for tracking

and tracing (Lipson, 2002). There is a brief survey for tracing cyberattacks about IP traceback in a different article. From the perspective of practicality and feasibility, this paper analyzes and explore the advantages and disadvantages of these schemes for shortcomings (Gao & Ansari, 2005).

The various approaches are classified to network forensics to list the requirements of the traceback the traceback solution will be a major step in the direction of attack attribution and investigation. The most challenging problem for network forensics, IP traceback, was examined in this paper. The proposed technique can trace the attacker till the ingress edge router even with a single packet which meets the basic requirement of network forensics (Pilli, Joshi & Niyogi, 2010). Also, another study, it is mentioned that the IP address is a record and it can be presented as evidence in the context of cybercrimes. IP evidence alone does not necessarily represent the perpetrator. In addition to IP evidence, it is emphasized that forensic informatics analysis, attitudes and behaviors of the accused, other paper evidence or related records, who has benefited from the crime as a result of the crime, should be evaluated and submitted to the file. If the court decides on the merits of the case based solely on IP evidence, it is unfortunately unjustified, unlawful and unfortunate, as mentioned above (Akgün, 2016).

The studies and literature review, studies on the detection of cybercrimes are examined. According to the results obtained by making applications to detect IP based evidence of attacks on computer network systems; assessments were made about the deficiencies and measures that could be taken closely to end users and system administrators. As a result of the applications and researches, it concludes that the security of network devices such as servers, switches, hubs or computers in network systems should be increased (Gündüz, 2013).

To efficiently simulate cyber-attack scenarios, this paper, presents a simulation modeling approach to represent computer networks and intrusion detection systems (IDS). This paper can be useful to model a cyberattack by phases (Kuhl, Kistner & Costantini, 2007).

An article investigating the effect of common network attack on performance biometric readers was prepared. The experiments are conducted using Denial of Service attacks (DDOS) and the ARP cache poisoning attack. And this paper shows that they are not designed to include basic security mechanisms, mainly firewalls to filter the network traffic and IDS/IPS systems to detect and prevent network attacks, and malicious network activities. Thus is, their availability and efficiency may become questionable within any institution, and it will be difficult to rely on such devices to implement security policies and conduct digital forensic investigations in case of an incident. Digital forensic investigators should be aware of the fact that current biometric readers are insecure and vulnerable devices and may exchange biometric data that can be easily attacked and altered (Trabelsi, Hemairy, Baggili & Amin, 2011).

Although it is accepted that cyberattacks will be directed to pattern based structures at the beginning, development of automation systems and introduction of general network protocol (IP) as a communication platform has been done to show how comprehensive cyberattack features can be. Therefore, the concept of cyber defense should be established to cover this wide spectrum. Keeping the global network entries and exits at certain points topologically, providing the latest data to the cyber defense coordination center, keeping the filters ready for foreign origin cyberattacks against critical institutions and organizations, especially DDOS attacks that may come from abroad. an external defense shield. Organizations that play a role in the external defense of cyber-defense activities across the country are ISP. In this respect, ISP have a great importance in the cyber defense of the country. It is of great importance that a general network exchange point in which developed countries' internal ISP traffic is being implemented is established in cities with a population of more than a few million (Şenol, 2016).

A research focused on using technology to gather information about potential victims. Digital attacks or threats to information technology may have a momentous impact on organizations. In conclusion, these threats usually lead to the disclosure of information, modification, denial of service (DoS), illegal use, identity theft or repudiation (Ciampa, 2007). However, an article was written that it is important that

the operating systems of the software used by institutions and organizations are reliable. “DDOS Mitigator” device, which was produced in 2013 with the support of TUBITAK and prevents DDOS attacks, enables the attacks to be seen with evidence, is one of the most important national products in this field. It should be ensured that “DDOS Mitigator” device and similar domestic products are widely used in public institutions and private sector organizations (Tübitak, 2013).

A new approach has been made to determine whether a host communicating with TCP is a data source or only acts as a TCP proxy. The results presented here indicate that determining the use of a proxy host is possible, if the network latency between the originator and proxy is larger than the network latency between the proxy and the receiver. This work show that this technique has potential to be used to detect connections were data is sent through a TCP proxy, such as remote login through TCP proxies, or rejecting spam sent through a bot network. This result indicate that this is possible, if the network latency between the originator and proxy is larger than the network latency between the proxy and the responder. Reject spam messages sent through a proxy bot network or block the access to restricted media contents when request arrives from a proxy host or detection of the Tor usage in an incoming connection (Eian, Willassen & Mjølunes, 2014).

SHA256, Tiger192, Haval160, MD5 algorithms have been prepared to research the hash value determined. The function of the MD5 (Message Digest Algorithm 5) algorithm is explained as an output of 128 characters, 32 characters, regardless of the size of the input of any length or shortness. In other words, the MD5 result of a 10 GB ISO file and the MD5 result of a 4 KB Word file are 128bit long. In this way, the hash value can be determined. When there is a change in the input, it causes the output to change. It was concluded that the original evidence was preserved by these means (Payel, 2015).

An article was prepared which presented statistical information and methodological approach to cyberattacks. This article can also be useful with given statistics and methodology for modeling cyber-attack scenarios (Zeadally & Flowers, 2014). And

another study describes the steps of forensic analysis in storage media, confidential data analysis in the file system, network forensic methods, and cybercrime data mining. This paper proposes a new tool which is the combination of digital forensic investigation and crime data mining. The proposed system is designed for finding motive, pattern of cyberattacks and counts of attacks types happened during a period. This paper explains the hidden evidence acquisition from file system, and there are two types of investigation in network, packet capturing and log file analysis and explains crime data mining. Lastly, proposes a new system with digital forensic tool for decision making in the computer security domain (Sindhu & Meshram, 2012).

In order not to be exposed to cyberattacks, large firms attack themselves to control their deficits. One of them is penetration testing. Since it is a very common subject, researchers have also worked on this subject. In a thesis prepared, penetration tests were conducted in corporate networks. and describing security solutions. The security solutions that should be taken in order to prevent the attacks from happening to the corporate networks are explained. Network scanning tools, vulnerability scanners, system, network and social engineering attack tools used in the tests are introduced. The steps of these tests and security solutions are explained in detail and the measures that corporate companies should take in this thesis are explained (Polat, 2016). In another thesis, the necessary service and server installation for penetration tests were prepared. An application has been prepared for penetration tests. A network prototype has been developed. Real life attacks were implemented. It has been shown how to seize the security that has not been tested for penetration and how to infiltrate the systems. As a result, the importance of penetration tests has been demonstrated by experimental studies on prototype (Akyıldız, 2013).

Cyberspace and cyber operational are defined in thesis which environment has been prepared. It compares the classical wars in order to establish the principles of cyber operations and proposes new principles. It examines the existing cyber security simulators and describes the IWSIM they developed. Reveals the database model of cyber operations scenarios. In this way, in order to reach a more realistic working environment, it investigates an effective cyber operations scenario database modeling

and how it should be (Yıldırım, 2016).

Header and footer signatures a study has been conducted in which all identified engraving methods are appropriate for the files. This paper emphasizes on minimizing the time and search of carving files from digital media like GIF, bmp, pdf that does or does not support a file system (Povar & Bhadran, 2011). Sametime, live and dead forensic analysis can be done by saving necessary scripts and different tools such as Autopsy, FDDumper, Scalpel, Fiml to a USB or DVD. This paper says fore forensic perspective, log on/log off, date and time, kernel level information and recently executed commands including processes and network status are of much importance for a forensic analyst in making appropriate decision about the significance of the forensic evidence (Yang & Yen, 2010). Also, a thesis, which provides a technical suggestion for uncovering encrypted drives, has been prepared. The suggested solution can merely decrypt only those sealed drives which are encrypted through Bit Locker using its USB only mode component. For this purpose, brute force attack can also be used to restore the drive whether on a live forensic analysis or physical memory dump file (Dija, Balan, Anoop & Ramani, 2011).

A study was conducted in which some data were found in waste areas and could be used for forensic purposes. Issues to be considered in Forensic Informatics are unpartitioned areas. Confidential information can be stored here. It is explained that wastes from disk partitions, especially NTFS file system, can host VBR sector. Mathematical calculations were made and the sectors that the data could be identified were shared (Dokurer, 2016). An article about Truecrypt has been written to provide analysis of storage, computer forensic crime activity. The computer forensic for Truecrypt encrypted volumes includes normal and hidden volumes. This investigation suggested a tool which is "Cafegrid". It can be used for deep analysis and recovery of data from memory in Windows and Linux. This tool can benefit forensic investigator in evidentiary analysis process as the data structure information can be coordinately used for offline or live analysis in digital forensics (Zhang, Zhou & Fan, 2014).

Technical studies require specialization from time to time. Because work on different operating systems may be possible with different programs. Therefore, an article has been researched on Linux operating system. This investigation has emphasize that the mining and analyzing the useful data of the Linux operating system has become important means and research directions of computer forensic analysis. It provides plenty of useful interfaces for the computer forensic investigation, which will be an important information-gaining tool for the computer forensics on Linux operating system (Chen & Liu, 2010). In a different article, Apple proposes a new method that can be used in a crime scene environment, automatically discovering the necessary information about the target computer to retrieve the RAM content of Mac computers over FireWire. In all experiments the tool successfully performed RAM imaging over FireWire without crashing the target computer. Generally, AIM messages of the ongoing AIM conversations were successfully recovered (Pavel & Almansoori, 2010). It has also been conducted in research offering a simple and inexpensive framework for forensic analysis for the iPhone. Through experimental results using real device, have shown the effectiveness of this framework in extracting digital evidence from an iPhone. In this paper present a simple forensic framework for iPhone. It follows the ACPO guideline and RFC 3227 for evidence collection and archiving to keep the recovered digital evidence sound in legal venues (Husain, Baggili & Sridharl, 2010).

2.4 Law Perspective

Studies on universal values in cyberspace have been made. There are cyberattack and thresholds for considering cyber exploits as use of force. Some existing conflict in laws and political and so is draw its legal frames (Lewis, 2012). It was stated in another study that it should be updated all over the world. The new regulations to be created in the field of informatics should be regulated and universalized based on the principles of sustainability in a way that protects the rights and freedoms of people and societies. It is concluded that there is a need for legal measures and practices in order to prevent the crime-causing structure of the information systems and the triggering feature of the crime (Altunok & Vural, 2011).

The difficulties encountered due to the lack lines of legal legislation were also included in academic studies. A holistic approach that evaluates cyber security with its legal, technical, administrative, economic, political and social dimensions and establishes the necessary legal legislation is need. In preparing legal legislation on this issue, the powers and responsibilities of all public institutions, their coordination and relations with each other should be clearly stated. If the legal legislation is not established clearly; it cannot be put against cyberattacks, an active cyber defense cannot be carried out, and worse, unconsciously, as a result of unconscious attempts to respond to criminal activities (Çifci, 2012). One of the other study states that states also have increased awareness for protection purposes. Although efforts to use the weapon of assault continue in possible situations, no common legal basis has yet been established, covering cyber warfare or crimes. It has come to the conclusion that this will become a necessity in every state (Türkay, 2013).

Some works is investigated problem through an analysis of current practices and workflows of investigators. It uses interviews with experts from government and private sectors who investigate cybercrimes as main data gathering process. This paper also defines a set of recommendations that can aid in providing a better foundation (Nouh, Nursey, Webb & Goldsmith, 2019). On the other hand, some works, the problems experienced in the implementation of the laws related to the development of computer technologies are examined. These problems were handled as the lack of international agreements, inadequacy of legal regulations, problems stemming from the qualifications of the practitioners and problems stemming from technical problems. It was concluded that violations in the internet environment should be remedied. It is thought that the law should be acted on. It is argued that public order should be ensured by combating the crimes committed on the internet (Çakmakkaya & Akpınar, 2018).

One of the studies give an overview of the evolution of cybercrime, and its influence on current legislation. As a conclusion this paper says police agencies will need to employ computer savvy detectives and forensic examiners that specialize in computer crime offenses. Court personnel will a flood the criminal justice system. This article says even federal agencies need trained personnel that they can remotely access and

search computers, storage devices, and phones in cases where victims have had their computers infected with malware (Pavlik, 2017).

The status of personal data in the current law has also been examined. The current laws for the fight against cybercrimes and protection of personal data from a critical point of view; In this context, legal proposals were developed by questioning the competencies (Gönen, Ulus & Yılmaz, 2016). Methods of combating cybercrime have been investigated. The studies conducted in this European Union have been examined. The existing regulations in our country have been evaluated. Developed solutions to new types of crime that may arise. In order to ensure international cooperation in this field, it has come to the conclusion that the legislation should be brought in line with the Cyber Crime Convention which was prepared by the Council of Europe and signed by our country (Özüdoğru, 2011).

Every country related to IT crimes is preparing its own rules of law. A lot of research has been done by countries. US law is researched. The most important law related to cyber security in the USA is the Computer Fraud and Abuse Act. This law deals with the crimes specific to information systems as well as the crimes in which information systems are used as a means. In some court decisions, it is important to include such a distinction in the essence of the law, although every computer on the network is covered by the concept of protected computers. Another feature of the law is that it separates cybercrimes and punishments according to the motivation of the perpetrator. Likewise, another positive aspect is to include definitions of many basic concepts such as computers, financial institutions, losses and losses in order to avoid differences in interpretation (Hekim, 2013). And a researcher seeks to further this path of inquiry by providing a systematic analysis of 40 cases from The Netherlands, Germany, UK, and USA where criminal networks were involved in financial cybercrimes affecting the banking sector. Discusses the theoretical and policing implications of findings. (Leukfeldt, Lavorgna & Kleemans, 2017). Another researcher is investigated exercise control over the Internet in China. China is implemented laws. Administrative regulations are done revolving activity criminalizing, content filtering and user monitoring so as to maintain security and stability at both community and

state levels (Xingan, 2015). Different article is prepared about how cybercrime affects to the nation and the awareness and preventive measures by which one can overcome the threat. Indian laws are well drafted. It capable of handling all kinds of challenges as posed by cyber criminals. But the enforcement agencies are required to be well versed with the changing technologies and laws (Hati, 2016).

Some of the research, a current assessment of the training levels, needs, and perceptions of abilities of Indiana law enforcement agencies and prosecuting attorneys, and whether they are engaged in investigating crimes involving digital evidence. As a result, support the recommendation that a comprehensive resource guide, focused on Indiana, is needed, as standard operating procedures are lacking, and there is a lack of awareness of available training courses or educational materials (Flory, 2016). A paper discussed ways on how to bridge the gap that exists among legislators, investigators, and prosecutors in Nigeria, and suggested recommendations to address the menace of cybercrime threats. As digital evidence grows in both volume and importance in criminal and civil courts, judges need to fairly and justly evaluate the merits of the offered evidence. To do so, judges need a general understanding of the underlying technologies and applications from which digital evidence is derived (Mohammed at al., 2019).

They have tried to contribute to communities in countries and have made some decisions on information crime law. The decisions taken by these communities and the results were examined by the researchers and they were tried to be guided about how to get better. One of these studies, cybercrime poses significant challenges for law enforcement. It also argues that the key cybercrime concern for law enforcement is legislation rather than technical and technological. The study says the European Parliament is largely excluded from policy development in the field of cybercrime, impeding public scrutiny (Hayes, Jeandesboz & Ragazzi, 2015).

The US National Institute of Justice conducted a study designed to identify the issues that the law enforcement community was experiencing in relation to computer crime. The study says lack adequate training, equipment, staff to meet their present

and future needs to fight digital. And it is also identified the need for reliable digital evidence (Ashcroft, 2011).

James Christy, who contributed to the creation of ethical hacker law, director of the American Air Force IT crime investigation unit, how to deployed a hacker team to test the security of military IT systems. This team is reported to have entered Pentagon's forbidden information system in 15 seconds. This use of criminals who have previously been hackers as a hacker provides a more successful control. In this context, Ethical Hacher has been regulated in the Millenn Digital Millennium Copyright Act kanun in the USA. The Ethical Hacher test, which can be carried out in accordance with the provisions of Article 1201 of the Law, is in some way bound to legal status. In the Turkish Penal Code, the destruction of information systems is one of the crimes that require ex officio monitoring. However, this approach will remain superficial, even though it can be described as no crime in terms of the elements of the crime (Karagülmez, 2009).

The study focus on the concept of cybercrime has been discussed and the legal and actual problems in dealing with this new type of guilt have been explained. Then, some instruments or organs that are accepted internationally in terms of combating cybercrime are briefly mentioned. The study constitutes the provisions of the Council of Europe's legal assistance in the Cyber Crime Convention, adopted in Budapest in 2001. Before the contract, then after giving general information about the qualified legal aid applications in Turkey, located in Part 3 of the Convention, provisions and principles of international cooperation were examined. In the conclusion, the point reached in the fight against cybercrime is evaluated. In conclusion; It is far from controversial that the Budapest Convention constitutes a major breakthrough in the fight against cybercrime (Önok, 2013). In the study, the private law of informatics is not entered. Computer search and access prevention measures were also evaluated within the scope of this study. Measures to be taken by individuals and the state in the fight against cybercrimes and the importance of international cooperation have been mentioned and comparative law and Council of Europe Cybercrime Convention have been used to understand the importance of the issues (Taşkın, 2009). And the o study

focus on examines the international and European Union studies on the fight against cybercrime. Evaluating the adequacy of the existing regulations in our country and proposing solutions to the problems created by cybercrime in the field of law. In order to fight cybercrime, it has been decided that not every country should make the necessary arrangements within its own legal system and leave the perpetrators of these crimes unpunished (Turhan, 2006).

Cybercrimes in Turkey by researchers examined by the frequency of law. It is considered that it is appropriate to update the law and regulation related to our country in order to effectively combat cyber threats, into a form that is more applicable, with a wide range of coverage and including all kinds. In legal regulations, cybercrime and cyber terrorism should be defined separately and an international consensus should be reached. Measures that are not taken internationally are considered to have different national strategies and thus create Weak Zones for computer crimes. It is also thought that these weak regions will cause information exchange and trade restrictions (Çakmak & Altunok, 2009). In another study the amendments made in the Law No. 5651 on the Regulation of the Publications Made on the Internet and the Fight Against Crimes Committed by These Publications were mentioned. Difficulties related to this issue are explained. The amendment to the protection of personal rights and the privacy of private life has concluded that the entire law is open to interpretation. For this reason, the objective interpretation of the provisions of the law should be applied in accordance with the principles of a democratic state of law has been proposed (Gönenç, 2014). The studies are carried out in the developed countries and the European Union on cybercrimes in terms of criminal law, to evaluate the scope and adequacy of the Turkish Penal Code numbered 5237, and to make suggestions for the deficiencies and problems of Turkish Penal Code on cyberterrorism. The legal arrangements and measures taken by the developed countries such as USA, Germany, France, England, Japan, China and Russia in the fight against IT crimes and the provisions of the Council of Europe Cyber Crime Convention, the only international document regulating these crimes, were examined. Finally, in the Turkish Penal Code No. 5237, the regulations on informatics crimes were emphasized, and in the conclusion part, after all these investigations and analyzes, the regulations to be made

in order to combat cyber terrorism and cyber terror threat more effectively, the measures to be taken and the measures to be implemented (Ermeýdan, 2018).

2.5 Security Perspective

In the National Cyber Security Strategy and the 2013-2014 Action Plan, the Ministry of Transport, Maritime Affairs and Communications has been assigned the policy, strategy, action plan and coordination tasks related to the provision of cyber security with the decision of the Council of Ministers (ResGaz, 2012).

The basic solution put forward in this thesis is the completion of the information security legal infrastructure, the development of information security culture, the establishment of the necessary infrastructure in the field of data protection. Cybercrime in order to ensure the mutual cooperation of public and private sectors in the decision-making mechanisms established to ensure national information security are established (Güngör, 2015).

The working paper presents the definition and understanding of cyberwarfare and related issues. The paper gives us a general concept of the warfare in cyberspace and summary of major incidents of cyber conflict which can be used as a sample for related scenarios (Schreier, 2015).

According a research the end user is aware of the security measures taken in the cyber space, which describe the abstract or concrete space in which interconnected hardware, software, systems and people interact. Today, in a lot of work has a range of cyberattack methods, this method of examining cyberattacks, cyber security status analysis was carried out in Turkey (Aslay, 2017).

The field of legal studies regarding European cybersecurity policies. For the purpose of conducting this research, a systematic and qualitative literature review was the method of analysis. Data was derived mainly from databases of the European Union. And the EU is step up its efforts to protect its cyberspace but is still approach by uncertainties (Lechner, 2017). In a different research security measures to be taken

to prevent the situations leading to cybercrimes have been mentioned. Measures taken in OECD, EU, NATO and USA are explained. It was concluded that our country should take similar measures (Ercan, 2015).



CHAPTER THREE

LEGISLATION AND FORENSIC PROCESSES IN TURKEY

The legal regulations, what are the steps of forensic informatics and the studies done in these fields will be explained in this below.

3.1 Legislation in the Turkey

When it is investigated the crimes of informatics in legal legislation, it is found that there are sanctions on this subject in 8 different areas. These sanctions and their contents below. Laws and Decisions on Information Crimes in Turkish Law System:

1. Article of the Constitution (Art 20.)
2. Turkish Penal Code
3. Electronic Signature Law
4. Intellectual and Artistic Works Law
5. Anti-Smuggling Law
6. Punishment on Internet
7. Criminal Procedure Code Computer Investigation
8. Judgment No. 2012/3842

3.1.1 Article of the Constitution (Art. 20.)

“The interception of data” is not required for penalizing entries to the information system, illegal entry into the information system. That is, violating the security of the information system becomes a danger crime. The target of the crime is a computer system or network. The legal benefit protected by this crime is “Security of Information Systems” (Anayasa, 2011).

3.1.2 Turkish Penal Code (TPC)

Information Crimes in Turkish Legislation: Entered into force on 26 September 2004. Law No. 5237 in the new TPC, crimes are described in articles 243-246 and the IT field in the second book, part three in Chapter Ten.

Cybercrimes in TPC “crimes in the field of informatics” and “offenses against private life and the hidden field of life” section is arranged. In addition to the types of crimes that can be described as information crime in the TPC, it can be processed through the information system. However, there are types of offenses that cannot be defined solely as cybercrime (Türk Ceza Kanunu, 2004). The articles are collected related to information crimes in two groups according to the TPC;

- a. **Those who are described as information technology crime only:** Crimes that can be defined as a crime of information technology. It is included in the new TPC numbered 5237, “Crimes in Informatics” show that in Table 3.1;

Table 3.1 Crimes are described as information technology crime only

Article No.	Description
243	Entering the Information System
244	Blocking, corrupting, destroying or modifying data
245	Misuse of debit or credit cards
246	Implementing security measures against legal persons

The Crime of Entering and Staying in the Information System as Unlawful (Art. 243): Art. 243 TPC regulates the unlawful entry into and continuation of a whole or part of an information system as a crime. Unlawful entry into the information system without the need to capture data and thus, the breach of the security of the information system has become a crime.

With the regulation of TPC 243, Council of Europe Convention on Cybercrime Article. 2 entitled “Illegal Access”: “Each party state is unfair to any part of a computer

system and make the necessary legal arrangements and take the necessary measures to cover the deliberate access to crime.” parallel to the regulation. The legal value protected is the security of the information system. In addition, the user of the information system and the personal benefits of those who benefit from this system are also protected.

Information system is the material element of crime. In order to this crime to occur, it is illegal to enter the information system and need to continue to stay there. General caste is sufficient for the occurrence of this crime. Anyone can be the perpetrator of the crime. Everyone can be the victim of crime, natural or legal persons.

Cyber infringement crime, which is regulated in all legal systems that have legal regulations on informatics crimes, is regulated in the first article under the title of Informatics Crimes. Entering into this article for any purpose if any information is defined as the actual crime.

There is no requirement to corrupt or obtain data in the information system for the occurrence of crime. The relevant article in the French Penal Code is an example of the article in the TPC. In many contemporary countries, cybercrime crime is considered to be the same. Furthermore, the type of offense in this article is in parallel with the regulation of against unlawful access provided for in Article. 2 of the European Cyber Crime Convention.

Crime, Disruption, Data Destruction or Modification of Information System Operation (Art. 244): This type of crime has been tried to be in line with the intervention to data provisions of Article. 4 of the European Cyber Crime Convention and the systems predicted provisions of Article. 5.

As mentioned in the justification of the article, damaging the systems has become a crime. Actions such as the destruction of data or programs in information systems, alteration of the functions of the information systems, restriction of access, restriction of access are generally regulated as crimes of property damage against information

systems. The information system that is blocked or corrupted, or the data that is destroyed, destroyed, changed or made inaccessible or sent to another place in the system, constitutes the subject of the crime.

In the informatics system, actions such as disrupting the functioning of the system, destroying the data, changing the data and making it inaccessible are the material elements of the crime. Anyone can be the perpetrator of the crime. The owner of the victim information system may be the owner of the information system, the person who has the authority to save on the information system. The legal issue protected by this article is the security of information systems and the data in these systems.

If a perpetrator, unlawfully, has access to all or part of the information system and stays there for a period of time and performs the actions specified in Art. 244 of the TCK, he must be punished separately from both Art. 243 and Art. 244. Because, in the Art. 244, entering the system against the law and staying there are not counted among the executive movements in the element of the crime.

Art. 244 refers to information system disruptions, destructive cybercrime, and especially Denial of Service (DOS) attacks, which prevent general access to websites. Paragraph 2 of Art. 244 includes viruses, Trojans, Keyloggers and Screenloggers applications. Article 1 includes interference with the operation of the system. In Article 2, there is interference with the data. In the last article, there is benefit through the information system.

Crimes Against Credit Card and The Bank (Art. 245): In Art. 245, acts of abuse of bank and credit cards are regulated as an independent type of crime. Any type of crime carried out by credit card or debit card constitutes an offense of unlawful benefit. The unlawfulness of a bank or credit card explained in the reasoning of the article is to prevent the loss of the exposed banks or credit holders and their removal in this way. The offenses defined in the article may be committed with general intent. No special feature has been sought for the perpetrator. This type of crime does not show any characteristic for the victim. Anyone can be a victim.

On the other hand, in the TPC; prevention of communication, insult, violation of the confidentiality of communication, listening and recording of conversations between people, violation of the privacy of private life, recording of personal data, unlawful giving or seizure of data, use of information systems in theft and fraud and to facilitate the use of substances, to establish an organization for the purpose of committing a crime, obscenity, disclosure of secrets related to duty, slander, cooling the public from military service and incitement to obey the laws were arrangements were made.

The misuse of bank or credit cards coincides with the act of unauthorized use of a bank or credit card which is considered within the scope of 52 providing illegal benefit through the information system 52 in Art. 525 b / 2 of the TPC. These abuses, which constitute one of the material elements of a crime in the TPC, have become an independent type of crime in Art. 245 of the TPC.

In the justification of Art. 245 of the TPC, it was stated that the bank or credit card is used illegally to prevent the loss of the banks or credit card holders, to prevent them from gaining benefits and to punish the perpetrators. With this crime, the right to property is protected and theft, abuse of faith and fraud are punished by using internet and information systems.

In the TPC, information crimes are mainly organized in the section lar crimes in the field of informatics and crimes against private life and the hidden field of life". In addition to the types of crimes that can be described as informatics crime, there are types of crimes that can be committed through the information system but cannot be defined as informatics crimes only.

b. Those who are not described as information technology crime only: The crimes which are not described as only information technology crime are given in Table 3.2.

Table 3.2 Crimes are not described as information technology crime only

Article No.	Description
84	Suicide orientation
103	Sexual abuse of children
124	Prevention of communication
125	Insult
132	Violation of the confidentiality of communication.
133	Listening and recording interpersonal conversations.
135	Recording of personal data.
136	Unlawfully giving out or seizing data.
138	Not destroying data
139	Complaint
142	Qualified Theft
158	Qualified Fraud
190	Facilitating the use of drugs or stimulants
194	Supply of hazardous substances for health
204	The official document forgery
205	Corrupt, destroy or hide the official document
226	Obscenity
227	Prostitution
228	Providing space and opportunity for gambling
251	Negligence of the audit task
257	Misconduct
258	Disclosure of the secret of the task
281	Destroying, hiding or changing evidence of crime
285	Breach of confidentiality
286	Recording audio or video
326	Government security documents
327	Providing information on state security
329	To explain the information about the security and political benefits of the state
330	Disclosure of information that should remain confidential
333	Use of state secrets, disloyalty in government services
334	Obtain prohibited information
336	Disclosing prohibited information
339	Possession of documents related to state security

Crimes Against Freedom Blocking Communication (Art. 124): The Internet has become the most widespread and effective communication network in the modern world. Today, most of the communication is made by electronic mail and chat. In addition, telephone calls and teleconferences over transmission data networks are considered as other types of electronic communications.

Since the article of the TPC, which is the subject of the examination, is called only communication and these means of communication are not counted one by one, the prevention of this will be a crime subject to whichever communication is performed. For this reason, the prevention of communication activities carried out through the information system is also considered within the scope of protection of the type of crime regulated in Art. 124 of the TPC.

Crimes Against Cheers Insult (Art. 125): It is also acknowledged that the offense of insult will also occur if the verbal, written or visual message is committed in the second paragraph of the said article. For this reason, it is also punishable for the offense to be committed by means of information systems or internet.

Violation of the Confidentiality of Communication (Art. 132): Today, thanks to the developing technology, communication systems are provided by using information systems, especially via the Internet, such as electronic mail, electronic chat, telephone calls over the internet or teleconference. These new communication methods through the information system are also protected by the regulation of this article and those who violate such communication are punished.

Violation of the Privacy of Private Life (Art. 134): Any person who violates the privacy of persons shall be sentenced to imprisonment of one to three years. In the event of a breach of confidentiality by recording images or sounds, the penalty shall be increased by a factor of one.

Anyone who unlawfully discloses images or sounds of the private life of persons shall be sentenced to imprisonment of from two to five years. The same penalty shall be imposed in case of the publication of these data through press and publication.

Turkish Panel Code Data Illegally Seize (Art. 136): This regulation is particularly applicable in countries such as the United States and the United Kingdom, where the highest number of cybercrimes committed in the field of identity theft.

Today, there is a lot of personal information on the Internet. Most of this information is given to various sites based on the consent of the people. The provision of such information as unlawful giving to third parties, dissemination of such information or the seizure of such data by third parties is regulated by this article.

Data Destruction (Art. 138): In accordance with this law, the personal data in the system are kept in these systems and thus their accessibility is prevented and sanctions are applied to those who do not remove the data from the system.

However, one of the most important elements in the detection of information offenses is the service provider or information system log records. The legislator is required by law to provide a minimum period of time to store records other than personal information. This regulation has been realized within the framework of the “Law No. 5651 on the Regulation of Publications made via the internet and the Prevention of Crimes Committed by these publications”.

Right to Complain (Art. 139): As can be seen, among the qualified cases, the processing of information systems, especially via computer, is not considered as a qualification that increases the penalty. Again, the pursuit of these crimes should not be subject to complaints. The fact that the private life of individuals is not violated is related to public order and necessary follow-up is necessary. Offenses in this category, which do not depend on the complaint, lead to a much greater loss of interest behind the sight. Although the detection of these crimes will be difficult to follow due to the fact that they are committed in an abstract environment, this can be facilitated

by means that can be developed in this respect. Today, even a simple search engine can detect and filter specific words and provide a warning message to the user. Law and technology should be brought and the deficiencies should be eliminated by using the judicial organs, legislators and the technical opportunities of the country in an advanced manner.

Today, social media has become our personal signature. The necessity of protecting our identity in a virtual, unrestricted environment is an undeniable issue.

The other issue is that the quality of forensic experts should be important as it will be difficult to determine the accuracy of time, place and crime tool in committing these crimes. Likewise, the competence of public prosecutors conducting investigations should be increased and special courts should be established where these offenses are required.

Blocking is one of the most important sanctions imposed on web pages today. Art. 8 of the Law no. 5651 listed the reasons for blocking but kept these reasons narrow, except for these limited number of crimes, this sanction cannot be imposed.

Theft (Art. 141): In this article, the use of the term mal movable property in the definition of the theft is subject to controversy in the doctrine of law. Although the possibility of the purchase of a movable property through information systems is discussed, it is considered that it does not meet the elements of the crime under cyber theft. Although all kinds of energy carrying economic value are accepted as movable goods, it has expanded the classical meaning and scope of the crime. It is not considered appropriate to define the data in information systems as energy. Despite these discussions, it is possible to consider unauthorized money transfers made in bank accounts using information systems within the scope of the de facto taking the money from the place where it is located.

Crimes Against Assets (Art. 142, Art. 157, Art. 158): The TPC defines cyber fraud as a crime within the scope of qualified fraud instead of regulating it in a separate law article.

Crimes Against General Ethics (Art. 226): The subject of obscenity is a subject of constant debate in legal circles. The fact that the concept of obscenity varies according to time and different cultural groups within the same society is interpreted as a deficiency of the law article and it is emphasized that the word pornography should be selected instead of obscenity. In addition, the fact that child pornography is not regulated as a separate crime type by taking the relevant articles of the European Convention on Cyber Crime is one of the criticisms against the law.

3.1.3 Electronic Signature Law (5070)

In Electronic Signature Law has two important articles. These are unauthorized use of signature creation data and fraud in electronic certificates. These will be briefly explained below (Elektronik İmza Kanunu, 2014).

Unauthorized use of signature creation data (Art. 16): Apart from the consent of the person concerned for the purpose of creating an electronic signature; those who obtain, give, copy, and recreate the signature creation data or the signature creation tool and those who create unauthorized electronic signatures by using the signature creation tools obtained without permission are punished.

Fraud in electronic certificates (Art. 17): Fully or partially fake electronic certificate issuers or those who emulate or falsify the currently issued electronic certificates and those who knowingly use these electronic certificates are punished.

3.1.4 Intellectual and Artistic Works Law

Infringement of moral, financial or related rights and infringement of financial right are common crimes. So, laws were created on them (Fikri ve Sanat Eserleri, 2001).

Infringement of moral, financial or related rights (Art. 71): Violating the moral, financial or related rights related to the intellectual and artistic rights protected by this

Law. The right to make the software public, the right to indicate the name of the Software owner, the right not to change.

Infringement of Financial Rights (Art. 72): Preparatory actions to neutralize protective programs. Modifying, copying, duplicating, spreading, trading, mediating, crime. A person who produces, sells, sells, or holds for sale other than personal use of programs or technical equipment designed to neutralize additional programs created to prevent unlawful reproduction of a computer program shall be sentenced to imprisonment of from six months to two years.

3.1.5 Anti-Smuggling Law

The penalties specified in the provisions of the TPC regarding the fraud and informatics crimes of the Turkish Criminal Code shall be multiplied for those issuing any documents or declarations or committing these crimes through informatics for Fake declarations and documents in customs administrations (Art. 12) (Kaçakçılıkla Mücadele, 2003).

3.1.6 Publishment on Internet (5651)

The offenses that are subject to the reasons for obstruction as envisaged by Law No. 5651 are regulated in Law No. 5651 as a special law. These include referring to suicide (Art. 84), sexual abuse of children (Art. 103), facilitating the use of drugs or stimulants (Art. 190), provision of dangerous substances for health (Art. 194), obscenity (Art. 226), prostitution (Art. 227), provides space and opportunity for gambling (Art. 228) (İnternet Suçları, 2007).

3.1.7 Criminal Procedure Code Computer Investigation

The type of action that is frequently encountered with the developing information technology and also constitutes an attack on personal rights is the placement of personal data in the information systems without the consent of the individuals. In Art.

135, for detection, listening and recording of communication was created legislation. It is known that especially hospitals, their patients, financial institutions and insurance companies collect and use such data for the credit facility and solvency of their customers and commercial companies collect and use such data for advertising and marketing purposes. The transfer of such information to the virtual environment as data and the absence of the consent of the relevant person while making this has been turned into a crime type with the subject matter. Thus, organized by the Council of Europe and Turkey is a signatory to the "Agreement Relating to Automatic Processing of Personal Data Protection Against Persons" of the relevant regulations came into force (Ceza Muhakemesi, 2004).

3.1.8 Judgment No. 2012/3842 About Cyber Security

The purpose and scope of this decision shall be taken by the real and legal persons involved in the operation of critical infrastructures related to information and communication technologies, taking measures to ensure the security and protection of the confidentiality of all the services, transactions and data provided by the public institutions and organizations over the information technologies and the systems included in their provision. to regulate the procedures and principles to be followed. In this decision, the Cyber Security Council, the duties and powers of the ministry, working groups and temporary committees, the powers of the Cyber Security Council, the Authority of Information Technologies and Communication are explained (Ulusal Siber Güvenlik, 2012).

3.2 Forensic Informatics Processes in Turkey

Forensic IT process includes laboratory investigations within the preliminary investigation. As in all forensic sciences, Forensic Informatics is a study carried out in a laboratory to prove a forensic event with material evidence. However, the process of collecting evidence from the crime scene before this study and expressing such evidence in court in a descriptive manner is also a subject of Forensic Informatics as it requires special knowledge. Those interested in these issues are called the Forensic IT Specialist.

1. **Evidence Detection:** Action plan, supply of necessary materials, determination of possible digital data sources.
2. **Evidence Collection and Preservation:** Collection of digital evidence from the crime scene, storage of data in a way to maintain integrity.
3. **Evidence Extraction:** Searching for data that may constitute a crime element, preparing the results for analysis.
4. **Evidence Examination/Analysis:** Recovery of deleted, encrypted or damaged data, detailed examination and understanding of the event.
5. **Evidence Organization:** Reporting the findings to be accepted by law.

3.2.1 Evidence Detection

It is the step that determines the required competencies before going to the scene. Forensic IT specialist to have sufficient competence, computer or electronic engineering forensic IT Specialist training and law protection training must be taken. They must have laptops with different operating systems (Microsoft, Mac, Linux). Disc, DVD, CD, SD Card, MMC Card, multiplexers, cable and fasteners of almost all types, cameras, GPS devices, hash programs, software tools for forensic analysis, packaging, digital evidence preservation materials, anti-static bags, foam, sponge-carrying materials, and electronic tools should be available.

Crime scene investigation as a result of sudden development is often encountered by police forces. Their work is to ensure that the relevant units, teams and experts seize and examine the incident by keeping the scene properly. It should be ensured that the relevant unit has information about the type of crime it is related to. Crime scene investigation teams need to be very careful and sensitive. They must maintain the scene. It is necessary to wait for experts to intervene at the crime scene computers and devices. Because the interventions of unqualified people can create problems.

Computers are expensive device. Special attention should be paid to their examination and restraint. If non-experts in the team are interested in the computer during the search, the information that can be accessed in later stages may cease to be

evidence. The open computer may need to be examined in that way. It is best to keep it open for him. Computer work is very much dependent on the password, suspects do not want to give it to the computer next to the password, secret compartments can be written on paper, must be investigated.

The computers and computer devices that constitute the subject of the crime should be transferred to the expert personnel at the scene. It should be ensured that all the investigations are carried out in the laboratories in order to examine these devices or records at the crime scene more widely according to the size of the investigation. This work should be done by experts in the field without damaging the devices and information. For him, it will be important to choose a team of experts, because these devices are very sensitive magnetic media, misuse, and so on. reasons will adversely affect. Assistance should be sought from the IT departments and other specialist units.

What is sought for the technical staff as an investigator should be clearly communicated. It should be asked to investigate the issues. The expert may contact the other persons with the information obtained and collect information that may be evidence. It should be noted that there can be computers of any size in any environment and their connections can be provided from many different locations. Planned research will lead to success. Computer system and information in it; these must be learned by the person who produces, sells, and user experts.

Planned searches should be taken care of the search decision. The presence of judges and prosecutors at the scene is useful for the prosecution of the investigation. In case of sudden events, the first responding team and the subsequent expert teams should consult with their superiors and these units to ensure that the relevant units seize the incident and direct the investigation of the incident and the scene. During the calls, the suspect should not be allowed to touch the computer system or assist the technical team. Because a small transaction that will be done will ruin information that may be evidence. Therefore, it is necessary to isolate individuals from the environment. An internal intervention can do more damage than the remote.

At the time of the event, the lines may need to be open to discussion, what should be detected on the screen, and information about the connection to the other computer can be found. It should be known that computers may be connected to other computers through the network. Therefore, data that may be evidence on the computer may be uploaded to computers elsewhere through these connections. This second computer can be at home and abroad. In this case, the authorities of the relevant place of contact should be contacted.

3.2.2 Evidence Collection and Preservation

It covers the process of ensuring environmental safety at the scene of the incident, from delivering evidence to the laboratory. The first response group to the scene must first be sure of its own security. Before start collecting evidence, need to get everyone away from the computer system. Take a photo of the scene and draw the connection diagram of the computer system at the scene. Attention is paid to activities that may cause harm.

Collecting evidence from the scene is the most basic stage. Because more healthy the evidence is collected, the more successful the subsequent stages will be. Even the collection of evidence requires special expertise. Crime scene teams should have sufficient knowledge of information systems and be careful with digital booby traps that can destroy evidence.

Physical and electronic perishable evidence should be protected. Devices that connect to the computer by telephone, such as modems, call boxes, must be detected. In addition, if there is a LAN / Ethernet, wireless, infrared, firewire connection, they should be detected and labeled in the same way. Fingerprints or other physical evidence must be maintained on the keyboard, mouse, floppy disks, CDs and DVDs, and other computer components. Persons present at the scene should be separated and identified and their current locations identified. Owners and users of electronic evidence, passwords, usernames and internet service providers should be identified.

Details that may be the password at the scene are examined. If the scene is reached with the computer turned on, a screenshot is taken. If there is a screen saver, the passwords found are used to cancel. Anything that looks unusual is noted. If it is present in the environment, the laser can be used to print any kind of matrix printer; without pulling it off, but directly from the current. The same process is performed for network active devices (hubs, switches, routers, DHCP servers). If there is a personal management system, it is kept as it is without turning it off. If the personal management systems have a disc, the summary defined for the discs is extracted.

The computer is disconnected from power. It should be noted UPS systems. The network cable is disconnected. The jammer is used when necessary. Cables and ports are named. The beginning and end of the cables are marked. Specified if the cable is not connected. The serial numbers of the devices are stored. All external equipment and cables are disconnected. Internal discs and cards are removed.

Collecting evidence from independent desktops and laptops, collecting evidence from computers in complex systems, preparing original media for images, image retrieval (hardware, software) should never be done on original evidence (Image retrieval: One-to-one copy of the media. Bit-Copy, Bit.Plus-Copy).

Images are taken from computers to make the review (one-to-one is copied). If possible, no direct examination of the evidence media should be carried out and a copy of the image should be obtained after writing protection. If it is not possible to make a one-to-one copy of the media, inspection of hardware devices with a write protection measure should also be carried out. The bit-to-bit image of the magnetic or optical media is taken using write-blockers, no changes are made to the original media, and the integrity of the received images is calculated by calculating the hash values.

Due to their structure, electronic evidence must be packaged and transported by a special collection, packaging and transport system. The data must be carefully protected in case of damage or deterioration from the magnetic field generated by static electricity, magnetic, radio transmitters and other devices. All collected evidence

should be documented before packaging. Make sure it is labeled and registered. Scraping, bending and folding computer media such as floppy disks, CD-ROMs, and magnetic tapes should be avoided. If possible, each hardware is packaged separately. For these used in antistatic balloon sachets, antistatic foam, original carry boxes, paper bags. Heat, static electricity, high electro-magnetic environment is created to prevent the environment.

Moving the devices intact can cause loss of evidence. For this reason, robust transport boxes are preferred. Transport with special vehicles protecting from shaking, heat and cold. It is fastened firmly with a special belt in the vehicle. It is transmitted from a secure route as soon as possible to forward to the specialist to examine. A note is made on the evidence that there is evidence for careful transport. Special storage rooms and shelves are created. It is kept in safe places where the entrance and exit are controlled.

3.2.3 Evidence Extraction

Images from devices are examined. The possibility of any data loss should be taken into consideration and a summary of the image should be taken before starting the examination. Hardware parts are brought to the inspection stations. Write protection systems are created with all kinds of transducers. Storage unit, evidence review and evidence deletion software is available. Daily inspections are performed backwards. Password cracking and deleted data recovery operations are performed at this stage. Evidence Extract: Existing file search, deleted file search, file search from unallocated area, word search, internet operations, link files, PrintSpool files, registry review, file signature analysis, hash analysis, recycle bin recovery, swap file, unused disk area, programs that run automatically at windows startup, hidden partitions. The data obtained at this stage will be included in the report that will be prepared to be forwarded to the forensic authorities, and it is checked by evaluating whether the data is safe, undamaged and unchanged.

Evaluation of found crime elements. Identification of criminal elements that will be the definitive evidence. It is determined that which of the findings found in the evaluation phase will be brought before the judicial authorities as definitive evidence. It is important to note that the information that will guide the investigation is fully identified for the presentation phase. For example, normal computer documents or files that do not constitute evidence should not be eliminated and considered as evidence. It will of course take a lot of time to prepare all the data on the media that may contain digital evidence as evidence and prepare for the presentation stage and it will not be possible to evaluate all the data in the evidence category and will confuse the judicial authorities by breaking the labor force. The aim here is to provide the most accurate and criminal information as evidence and to make it ready for reporting. Briefly, accurate and concise data should be presented as evidence in a way that will illuminate the crime in an uncompromising and comprehensible manner.

The golden rule in the Computer Criminalistics community, never use the suspicious computer and “trust the suspicious computer” rule should always be kept in mind and act accordingly. It should be kept in mind that in some IT crimes, suspicious software may be used by suspects, and the evidence on the system may be damaged as a result of triggering that may result from the use of the system. Here, of course, mind. So, the question of how to get the evidence that is likely to be on the operating system without using computer systems may come. The data in RAMs, which are the temporary memories of computer systems, active applications on the running system, active network connections or ports on the system, active users, etc., of course, can be considered as evidence. There are various hardware and software solutions that can be used to obtain such data without disturbing the integrity of the evidence. In the face of such situations that require advanced technical knowledge and skills, if there is no available solutions and capability, it is an accepted idea in computer criminals to lose a little bit of evidence is a thousand times better than the loss of evidence integrity. Deterioration of evidence integrity will void the validity of all evidence that can be obtained. Before applying this principle; the fact that the evidence considered to be lost in the present case will be important in clarifying the crime.

The question that might come to mind during the collection of possible evidence objects is the question of how to collect them after they cannot use or shut down their computer systems. The collection of possible evidence objects is meant to contain objects under law to be taken to a full-fledged computer criminal laboratory for evidence review. There is no certainty in the method of shutdown according to the services provided by the computer system, the software running on it and the disk structures. Again, the job depends on the advanced knowledge of the examiner in terms of hardware features of the existing computer systems, software features, and the structure of the operating system in order to ensure minimum data loss never to lose and the integrity of the evidence.

Investigations on computer systems that may contain evidence should be performed on one-to-one copies of the data storage units of the system. One-to-one copy for review is called Forensic Image in computer criminality. This one-to-one copy, image retrieval, must be carried out by low-level copying of the data on the target system under examination.

Taking the sector-by-sector data of the system on low level means that only a valid image is obtained. In the copies made with various copying software, there is no valid image acquisition since only the files on the system are copied. Because low level bit-based copying is taken as a sector-based reflection of the data storage unit on the system, the empty data areas on the data storage unit, the deleted data areas and the disk structure are cloned as is. Image retrieval solutions such as Partition Imager and Norton Ghost. Since it clones the data storage units on the system only on the basis of boot record, partition table, file system table and existing files, it does not copy the areas on the system, but the files are not available. This will inevitably lead to the loss of free disk space, which may include deleted data loss of evidence during the review phase.

When the data storage unit of the computer system with the evidence object is attached to another system, there is the possibility of data damaging evidence if there is no hardware or software protection that applies write protection to the data storage

unit installed on that system. For example, accessing any file on a data storage medium attached to another system in this manner may change the access date of that file, which may be evidence in the future.

3.2.4 Evidence Analysis

Inspection on image media with file listing, word search, file identification, file view, forensic image, hash value, analysis of evidence, data integrity and hash control, elimination of known and copy files, recovering deleted data and file scraping, optical character recognition, system files and timeline analysis, classification, encrypted, corrupted, analysis of files can be made. Keyword search;

- Stem search; (o - ku - tan)
- Search operator; (and - or - * - ? -)
- Fields search; [subject]
- Date search; [created]#2015-12-15...2015-12-30#
- Template search; TCK, IBAN, Credit Card
- Fuzzy search; Ayse Okudan
- Proximity search; (Ayşe w/4 Okutan)
- X word before from Y; (Ayşe pre/2 Okutan)
- Group search; apple pre/3; (orange or pear ((apple and pear) or grape) pre/2 (orange or grape)

Determining what kind of data will be searched for the crime faced. The data to be investigated generally tends to change according to the media subject to the same crime as the crime encountered. Each analysis is unique according to its subject and search. A single file can be searched from within multiple files. Rarely encountered file types are also available. It can be analyzed in encrypted and encrypted files. Analyzed devices can be computer, laptop. Mobile phone reviews, memory cards and USB sticks are also common. Network reviews are also included in the analysis process. Hardware or software data recovery is performed.

Cryptoanalysis is used to decrypt the encrypted devices. Wireless sources are examined. At the eviction stage, deleted files, folders and partitions are recovered and data that may be evidence is extracted from the swap area, slack areas, unallocated sections and temporary files on the media. In addition, using hash functions eliminates known files and reduces the number of files to be examined. At the stage of extracting evidence, files that may be evidence from the media are removed. These operations are made with evidence extraction operations, existing file search, deleted file search, unallocated area file search, word search, internet operations, link files, print spool files, registry review, file signature analysis, hash analysis, recycle bin recovery, swap file, unused disk area, windows startup automatic programs, hidden partitions.

All files extracted during the evidence review phase are examined. Forensic IT specialists may not have time to review each file on the computer one by one. Today, disk sizes are constantly growing and there are tens of thousands or even hundreds of thousands of files in the discs. Different methods can be used for examination; known file types review, word review, image reviews, file viewers, etc. The stage of organizing the evidence is the presentation of the evidence into a report. Although this is technically the simplest, it is perhaps the most important.

Information that should be included in the report, information about the research organization, information about the event, starting date and end date of the research, information about the electronic evidence seized and examined, information about the hardware and software used in the research, path and methods and tactics used in the research, chain of surveillance, the results of the research. They were found deleted files, memory cards, backup files, compressed files, partitions, formatted area, encrypted fields, hidden files and fields, digital camera files, broken, lost, sector and segment, unspecified area and slack area.

Conducting research on the system by scanning the content of the crime subject. Following the determination of the research methods, the content of the crime is investigated on computer systems and media. These are partitions, application files, registry records, log files, temp files, swap area, hidden files, deleted areas and files,

content (What kind of data?), capture (complete agreement with the subject), transfer (extracting data), deleted data (recovery), keyword (word search), password decryption.

3.2.5 Evidence Organization

Documentation and presentation of the findings for judicial authorities. The first stage of the crime scene and the first response is to ensure the safety of the scene and evidence before and during the acquisition stage.

Certification (photo), the physical location of information systems, the connection of the devices with each other, the connection locations of the network devices, the documents and notes that can be found around the information systems will give information to the criminal investigator about the crime. Once the scene has been secured, the scene should be photographed in detail. During photographing, attention should be paid to the cable footage of the information systems, screenshots of the open monitors and any findings that may help the crime investigator.

Documenting the data obtained for the judicial authorities reporting the data obtained and evaluated in a language that is understandable for use by the judicial authorities. The language and content of the report should be understandable. Technique terms should be explained, exact and concrete data should be explained, the methods used to reach the evidence should be explained. All transactions should be stated in an additional report. Documentation of the data obtained for Forensic authorities, forensic authorities, documentation and presentation of the findings.

In the last part of forensic information science presentation; the data obtained and evaluated in the form of digital evidence should be reported in a comprehensible language for use in the investigation and submitted to the forensic authorities in a detailed, understandable and explanatory manner. The following issues related to the report to be prepared during the presentation phase should be considered. The language and content of the report should be understandable even for people without technical

knowledge. Technical terms and facts should be explained in detail. Final and concrete data should be included in the report as evidence. The methods of forensic informatics used to reach evidence should be explained. Evidence of proofs should be demonstrated before the integrity of the case. All operations performed during the review phase should be reported separately by preparing an additional report. In the case of information offenses and computer-related offenses described so far, it has been applied to identify possible digital evidence on information systems media that may be subject to crime.

Some requirements must be met for the preparation of the report. Information about the institution engaged in the research Information about the event date of the start of the research and expiry Information about the electronic evidence put in and examined Information about the hardware and software used in the research path and methodology and tactics used in the research chain of surveillance. The results of the research, where and how they are found. The data to be prepared shall be included in the report to be submitted to the forensic authorities. Accurate and concise data, data integrity and comprehensibility are extremely important.

CHAPTER FOUR

INFORMATICS CRIME

Information about cybercrimes is collected in this section. In addition, cybercrime allows easier understanding of cybercrime categorized.

Crimes committed using computer and communication technologies are also called white collar crimes. Common features of such crimes in general are the use of computer systems and technologies in the processing of informatics crime. As a result of informatics (IT) crime, very high earnings are obtained with easy and less risk. Due to the new crimes, the necessary laws and regulations are incomplete and inadequate. Even if there is sufficient legislation, the high probability of the execution to have incomplete knowledge and skills has more severe material and moral consequences than other types of crime.

As victims of crime are generally from unconscious users and the economy and finance sector and economic losses are high, security forces are generally not notified except for simple crimes. In the case of normal persons, the procedure to be followed is often not fully mastered in the event of the victim of such crime. Fear of losing reputation and prestige prevails if the victims are large enterprises and enterprises. The perpetrators of informatics are generally young people between the ages of 17-35. These criminals generally choose institutions that operate commercially. These victim institutions do not report in order not to be deciphered.

However, even if reported, criminals also know that there is no criminal norm to meet these acts. They continue to commit crimes because they know that their actions will remain unenforceable. Criminals can be ordinary and individual as well as organized. Informatics crime is a new type of crime that emerged after information technologies. Informatics crime and the crime committed through informatics are separated. The fight against informatics crime is a complicated process which is also a step of raising awareness.

There are special cases of IT crimes. Its scope is more difficult to determine. It is more difficult to struggle. Victim coverage is wider. The solution requires more cooperation.

4.1 Cyber Attacker Profile

Cyber criminals have some reason to commit crime. Most popular reason are taken revenge, sense of being important, financial difficulties and sense of transcending computer. Cyber criminals can be examined under different headings. These offenders, who are often separated according to their purposes, will be examined in this section.

- **Targeted and Conscious Attacker:** It is intended, planned and programmed. It is dangerous, technical knowledge and skills are high. It takes care to hide itself. Use special tools.
- **No Targeted but Conscious Attacker:** It is not intended, randomly selects the target. It is dangerous, technical knowledge and skills are high. Uses special or random tools. There is concern about arrest. Hidden.
- **Targeted but No Conscious Attacker:** It is intended, unplanned and unscheduled. Knowledge level is insufficient. Uses automatic tools. There is an effort to prove itself. It leaves a lot of track.
- **No Targeted and No Conscious Attacker:** It is not intended, randomly selects the target. Technical level is poor. Easy to follow and capture. It is dangerous. It constitutes the majority of the attacker's mass.
- **Internal Attackers:** Within the organization, attacking internal systems for specific purposes is corporate persons.
- **Cyber Activists:** They are individuals or groups who attack the cyber spaces of the public or private sector with the aim of expressing social or political problems which they see as bad or inappropriate within the framework of world views.
- **Intelligence Institutions:** In the international cyber world, countries have started to see each other as cyber threats. Because of this threat perception, countries form cyber defense and cyberattack teams and continue to attack the critical

infrastructures of the target country in addition to trying to access critical data from other countries.

- **Hacker:** Personal computers or mobile devices, or organization, company, public computer networks are the intruders.[4]. A person who uses computers to gain unauthorized access to data. They hide their identities and activities.
- **Cracker:** They usually break software passwords. They hide their identities and activities. He's on his way to becoming a hacker.
- **Lamer:** They use ready-made tools and viruses. They seek glory and fame. They claim to be hackers.
- **Script Kiddie:** An unskilled hacker who uses programs and exploits written by others or the other description is person who uses existing computer scripts or code to hack into computers, lacking the expertise to write their own.
- **Curious Ones:** People who are curious about computers, often unintentionally do harm, or seek revenge from the workplace.

4.2 Informatics Crime Categories

IT crimes can be grouped from different perspectives. These groups are given below.

- a. Informatics Technology Crimes According to the Technology Used
- b. Informatics Crime According to Their Forms of Operation
- c. Informatics Crimes According to Regulation of The Legislation (TPC)
- d. Types of Crime According to the Effect on Data
- e. IT Crimes According to Violence

a. Informatics Technology Crimes According to the Technology Used:

Information Technology Crimes according to the technology used consists of 4 different groups.

- Hi-Tech Crime
- Computer Crime
- Internet Crime
- IT Crime

- b. Informatics Crimes According to their Forms of Operation:** These crime types may be separated into two groups, “with Malware” and “with Deceptions” and given in Table 4.1.

Table 4.1 According to their forms of operation

With Malware	With Deceptions
• Trojan Horses • Virus • Worms • SpyWare • Logic Bombs • Password Breaker • Sniffer • Weakness Hunter	• Social Engineering • Spoofing (IP, ARP, DNS) • Phishing • Scam Page • Spam and Fake Mail

c. Informatics Crimes According to Regulation of The Legislation (TPC):

According to Legislation Regulation, IT Crimes are divided into 2.

- Those who can be described as a crime of informatics technology only
- Those who cannot be described as a crime of informatics technology only

- d. Types of Crime According to the Effect on Data:** These crime types are divided in four categories; unauthorized access, damage, making changes, production (Table 4.2).

Table 4.2 According to regulation of the legislation

Unauthorized Access	Damage
• Entering the System • Be Copied • Unauthorized Listening	• Deleting Data • Damage to Data • Disabling Services
Making Changes	Production
• Program codes • Steady Data • Transferred Data	• Data imitation • Adding data

- e. **IT Crimes According to Violence:** Violent crime is a crime involving physical danger to one or more people, while Non-physical informatics crimes are evaluated in the category of non-violent crimes (Table 4.3). Usually, it is a crime to obtain information such as username and password used to log into the e-bank system. This crime is made using attacks such as Phishing, Social Engineering, Malware, Keylogger, Screen Logger, Virus, Trojan Horse, DNS attack.

Table 4.3 According to violence

Violent Crimes	Non-Violent Crimes
• Cyberterrorism • Assault by Threat • Child Pornography	• Disruptive Cybercrime • Cyber Violation • Cyber Theft • Cyber Fraud • E-bank Fraud • Unauthorized Access and Listening • Computer Tamper • Computer Fraud • Unauthorized Use of a Software • Illegal Publications • Credit Card Copying and Abuse • The Other Non-Violent Cybercrime

4.3 Common Cybercrimes and Their Properties

In cyber space, there are many types of attacks and attacks that require cyber security experts to protect their computers. For example, trojans, viruses, worms, logic bombs, DDOS, social engineering, phishing. By using these attack methods, attackers can inflict various damages to the computers or computer networks they have infiltrated in the form of modifiers, destructors, service disruptors or data leaks.

Cyberterrorism: Committing, planning and coordinating terrorism crime using information systems. Such as altering the data in the computer system that controls Air Traffic, causing collisions of aircraft or changing patient records to cause incorrect

dose of medication. Terror acts for blocking purposes. It means cyberattack between countries.

Assault by Threat (Cyberstalking): To threaten a person or loved ones by using information systems as terror. Like harassing or insulting on the Internet. The use of electronic devices to obsessively harass a victim.

Child Pornography: Those who create pornography material using young children are those who distribute and access these materials.

Cyber Violation: It includes crimes that enter an information system without authorization, but do not harm or abuse the system or any object on the system. It is often pronounced as unauthorized access. It is a crime to enter a person's computer, read their e-mails, note which programs they use, and find out which websites they visit.

Computer Tamper: Clearing, destroying, modifying or using information in the intrusion computer system.

Unauthorized Use of a Software Protected by Law: Illegal copying, reproduction, sale, distribution and use of software. The sale or reproduction and distribution of pirated movies, CDs is a crime.

Illegal Publications: It is defined as the distribution and distribution of illegally accepted elements through computer systems and the Internet. Propagation of organizations deemed illegal by law is included in this crime.

Bank / Credit Card Copying and Abuse: Bank / Credit card is copied events. POS devices are realized by means of counterfeit devices that look like ATMs. There are card copying apparatus installed by the suspects in ATMs. The ATM is difficult to understand from the outside.

Cyber Theft: It is a crime committed by stealing personal information, money and similar values by using information systems. The discovered personal information is then used to illegally apply for loans, purchase goods and services, or provide access to bank accounts. There are many different types. Embezzlement by an authorized person, making unlawful allowance by someone who is not authorized, stealing trade secrets, customer information, unauthorized use of a person's writings, copying copyrighted software, music, movies and books.

Cyber Fraud: It is a crime committed by misguiding for the purpose of self-interest by using information systems. Unlike cyber theft, cyber fraud also voluntarily carries out the action voluntarily. An e-mail that asks to deposit money into an account number to help a poor person is defined as the fact that a website shopping on the internet does not serve after receiving the money, confusing, deceiving and deceiving people with computers or communication tools. For example, withdrawing money from someone else's credit cards without permission, requesting money by sending emails or messages on behalf of others.

Malware: It means malicious software. Malicious computer programs that provide access to system information to malicious computer systems or cause serious damage to computer systems. Malicious software can be used against people, processes and technologies. The purpose of the malware is to provide unauthorized access to systems or to obtain critical data. Intruders can create security vulnerabilities in order to perform unauthorized access to the system, corrupt the system, prevent service, change information, destroy information, disclose information, and steal information. They can steal email accounts, bank passwords, and personal information from computers and send them to others. They may cause operating systems or other programs to fail or malfunction. They can delete, copy, relocate, or add new files from computers. Everything is recorded including keyboard and mouse. They can erase or even format the disc. They can create pop-up windows on screens that lead to annoying or malicious websites. It falls into the category of destructive cybercrime for the purpose of disabling network systems, damaging or destroying data.

Malware is a general concept. Virus, worm, trojan horse, keylogger, adware, spyware, rootkits can find their place in this concept. Malicious software can cause e-bank fraud. This is because malicious software such as keylogger, screen logger can be used to obtain the username, password and similar information used by the user to log into the e-bank system. Malicious computer users can fraud through email by accessing correspondence with companies by controlling email traffic with malicious software they send to computers. Before negotiating with the other party, they receive agreements with the other company and change the bank account information by creating a fake proforma. Malware is consisting of virus, worm, trojan, spyware, keylogger, malvertisement, adware, rootkit, ransomware.

Viruses: It is a computer program that changes the way the computer works and tries to hide itself in other files without the user's permission or knowledge. Prevents the operation of the computer. Software designed to save, corrupt or delete data. There are employees who can slow down by spreading to other computers over the Internet. Viruses must be run by a user. It usually occurs when e-mail from a user is opened, or when USB is powered on automatically. They enter the computer and damage files and programs.

A computer virus is more dangerous than most malware. Because they directly damage files. It can be infected with programs and files downloaded or shared from the Internet. Malfunctions of programs, deletion or addition of files other than desired, and a certain slowness of the computer are usually sign of viruses. They can work automatically in the infected environment or they can become active as a result of running the infected file. Virus can access to some or all of the informatics systems, computer network or the data it contains, programs. Unauthorized access and listening to computer systems and services are done from viruses. Virus Types;

- **Viruses that infect files:** They usually include a copy of the .com and .exe files themselves in the source code. Sys, drv, bin, ovl, ovy, dll are also available viruses that infect files.

- **Boot Virus:** They are infected to the first sector and to the boot sectors of the partition.
- **Macro Virus:** It is written using macro languages of commonly used application software such as Microsoft Word and Excel. Because macros are saved in data files, the macro code of the virus starts when the infected document is opened.
- **Shortcut Virus:** A shortcut virus is a kind of Trojan/worm combination that hides all of files and folders, then replaces them all with shortcuts that look exactly the same. The inserted flash memory appears hollow even though it is empty. The files are considered to be deleted. In fact, the files are confidential. Show hidden files should be called. Need to put them in a folder when the files become visible.

Worms: A computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage. The difference from viruses is that it spreads automatically over the network. Due to the automatic spreading of the computer network over time, the slow operation of the web pages will cause late. A program that replicates itself repeatedly on the local drive or network. Its sole purpose is to constantly replicate itself. It does not damage any files or data, but it keeps the system busy by making continuous copies and affects the computer speed. It can destroy data and programs, interrupt the activities of computer networks.

The most popular worms spread by e-mail. The most important features are rapid proliferation. Some worms are spread as network packets. They enter the computer memory directly and then activate the worm code. With files sent as e-mail attachments could propagated. By links sent in message could propagated. Via Web or FTP resource connection could propagated. Peer-to-peer spread over file sharing networks can be considered. For example, tmp.exe can be worm. Computer is infected when the task manager can be run by pressing CTRL + ALT + DELETE at the same

time when the computer is locked during startup. A type of worm that copies itself into folders by creating a new folder with the same name.

Spyware: A kind of computer program that changes the way the computer works without the user's permission or knowledge and tries to hide itself in other files. Spyware is defined as software that ensures that important information about users and their actions are collected without the user's knowledge and sent to malicious people. Spyware are inadvertently infiltrated by other Internet users, especially by Internet users. Spyware, unlike viruses and worms, does not need to spread after infection. The objective was to collect information by ensuring confidentiality in the infected system. This information can sometimes even be important information such as a credit card number. In addition, commercial firms may distribute spyware on the Internet to determine user habits on the Internet.

Spyware Programs written to capture user information. They can cause endless pop-ups. It can overlay an application and secretly install itself on the internet user's computer. It can report the user's actions on the internet to other computers. A type of program that is installed on a computer without the user's permission or permission and collects information about the user or computer and sends it to a remote user. It steals personal information, slows down the Internet, sends data to the outside, and downloads advertisements from the Internet. There is the possibility of creating open on computer. They slow down computer because they work in the background. Symptoms of a spyware attack may include unwanted toolbars appearing in the browser, changing the home page of web browsers, the failure of some special keys such as the "Tab" key, random incoming error messages, and endless pop-up windows. Unauthorized access to computer systems and services may result in criminal offenses by providing access to some or all of the information systems, the computer network, or the data it contains, programs.

Trojan Horses: Trojan horse is not a virus. It is a kind of malicious program that looks like a real application which looks like a real application which are malicious software that computer users install without having in-depth knowledge of their

content. They allow access to computer with a hidden program or a special server program or send private files on computer to other centers using the Internet. They run in the background in the computer and becomes active when the time comes and damages system. Trojans appears to be non-hazardous and then does different things than expected which runs in the background in the computer and becomes active when the time comes and damages system.

Computer users install without having in-depth knowledge of their content. It may seem like useful or interesting programs to the user. Because, the characteristic of trojans is the ability to remotely control or monitor the user's computer. In general, programs that are trojan horses infect computer systems as a result of downloading the file to the system. By running e-mail attachments, they are transmitted through files downloaded from insecure sites and files in sharing environments. They do very damaging tasks, such as formatting the hard drive, deleting files, or crashing the system. The trojan horse creates a security vulnerability in computer, which opens the way for malicious programs to enter system. Deleting or overwriting data, automatically changing the settings of the computer, connecting the internet browser to unknown sites may be a symptom of the trojan horse. The trojan horse is also installed as a zombie computer. Even if the trojans copy and distribute themselves, every victim must run the trojan.

Adware: It is software that opens advertising while any program is running. The adware can automatically land on computer and browse through browser windows while browsing the web.

Malvertisement: It is an infected online add that redirects on unsuspecting user to a malicious site.

Logic Bombs: A logic bomb is a string of malicious code used to cause harm to a network when the programmed conditions are met. Logic bombs are secretly inserted into a computer network through the use of malicious code. The code can be inserted into the computer's existing software or into other forms of malware such as viruses,

worms or trojan horses. It then lies dormant, and typically undetectable, until the trigger occurs. Triggers can be categorized as positive or negative. Logic bombs with positive triggers happen after a condition is met, such as the date of a major company event. Negative triggers initiate a logic bomb when a condition is not met, such as an employee fails to enter the diffuse code by a certain time. Either way, when the conditions become true, the logic bomb will go off and inflict its programmed damage. For example, CIH virus. The CIH virus, also known as Chernobyl, has the potential to be particularly destructive in that it can make some, Windows computer unable to start by corrupting the flash BIOS. Even if CIH is unable to destroy the BIOS, it overwrites the hard disk with garbage, resulting in the loss of data.

KeyLogger: Records all keyboard movements on the computer. In this way, all kinds of passwords, credit card numbers, personal information and detectable. It is a program or hardware that records everything written on the computer and sends it to the attacker. They are generally used to capture passwords.

Ransomware: Although there are different types of ransomware, their common feature is that they encrypt user files on the infected computer, making them inaccessible and unusable, and then asking users to open the files. This malicious software is often transmitted to user systems through fishing attacks or the Internet. The most effective precaution against ransomware today is to make regular backups on the computer and keep the backups on another device.

Rootkit: A computer program that infects itself, hides itself between running processes, is a very difficult to detect computer program that provides full control of computer remotely to malicious people. The purpose of viruses like slow down system and does not spread. To take control of computer and to hide its presence in the system. Although it was originally developed and used to hide the access of ordinary users to management programs and system information in multi-user systems, it is also possible to encounter malicious use. Running a program that is believed to come from a trusted source with high-level authority such as root causes a malicious rootkit to be installed on the system. Similarly, the most common form of infection in a multiuser

system is to install rootkits using kernel. Vulnerabilities. It is difficult to determine which files the rootkit actually modifies, which module is loaded into the kernel, where the file system is stored, on which network service it will listen and act with the appropriate command. However, at certain times, methods such as storing the eigenvalues of the most basic commands and possible rootkit infection points, and checking them later, can be used.

Remote Access Trojan (RAT): It is a kind of phishing software that hackers use to gain authority on the victim's computer they target. Unlike worms and other computer viruses, RAT's are not intended to damage the system, but to leak data from the system. RAT's can be easily stored with advanced methods used and can survive in the system they enter without getting caught in security software. Even after clearing RAT files in the system, it can be extremely difficult to detect the presence of RAT.

Phishing: Illegal means of obtaining the information that users use for any system, such as username, password, credentials, credit card details. "Password" and "fishing" words are combined. Phishing is used to obtain the username, password and similar information that the user uses to log into the e-bank system. In this way, the crime of e-bank fraud is committed. E-mail comes from fake sites for invoice payment or internet banking update transactions. When click on the link in these mails, the information is stolen. These websites usually contain an introduction to internet banking, paying bills by credit card. Customer name-surname information will not be complete. The invoice amount is written too high in order to agitate the person. The link in the click to view e-invoice redirects to another page. This is a fraud with phishing.

Counterfeiting is performed by using advanced technology devices or by simple phishing. Sending emails on behalf of others, damaging commercial and private relationships, harassing people, creating websites on behalf of others is fraud. Phishing with forms, creating a fake identity and imitating personality are considered within computer fraud.

Correspondence made with the companies by controlling the e-mail traffic with the malicious software they send to the computers. This is a fraud through fake email with phishing. They receive the agreements made with the other company before they reach the other party and change the bank account information by creating a false proforma. Then, when the contracted company sends money without confirming the account number, money is withdrawn by the suspects.

Pharming: Redirecting someone to another site instead of a trusted website. In this way, log-on to a fraudulent site prepared by an attacker while think log-on to a bank site and get passwords lost. Pharming can be done with malicious code or DNS capture.

Social Engineering: Unlike approaches that basically damage computer systems by exploiting gaps in computer or computer networks, social engineering can be defined as neutralizing or bypassing cyber security processes by making use of people's communication, thinking, trust, or human weaknesses. Generally, e-banka fraud, fraud through fake e-mail, computer fraud crime is made with social engineering. Social engineering methods; producing false scenarios through various lies, introducing oneself as a reliable source to the target person, or leaking information with simple reward methods. Socially affecting the system. It causes close dialogue with the user.

Social engineering is used deceptive speeches or other means of communication and persuasion to learn important information from people. They reach the conclusion by using the weaknesses inherent in human beings. The primary objective in this technique is to provide confidence. After providing the trust, the necessary information is taken slowly. The malicious person may try to obtain small pieces of information in each conversation. Conversations are mostly in the form of friend chat. These conversations obtain important information about the names of important people, important server computers, or applications. The most effective way for social engineering is the phone. Social engineering isn't always on the phone, as well as malicious people who come to the institution as guests can also receive username and

password papers affixed to the keyboard or screen edges of computers. They can mix the places where the institution dumps their garbage. For this reason, do not throw corporate information into trash.

DDoS Attack: It falls under the scope of destructive cybercrime. This is cybercrime for the purpose of disabling network systems, damaging or destroying data. Bots are other computers are included in the attack network with or without permission. When hackers secretly control numerous individual computers to conduct illegal activities with botnet. As a result, the service is blocked.

DNS Based Feeding: It is a DNS-based routing. Redirect to another web page. DNS routing is performed to perform e-bank fraud. This method can be used when phishing. It is used to obtain the username, password and similar information that the user uses to log into the e-bank system. Malicious computer user fraud with fraudulent e-mail to control e-mail traffic and access to correspondence with companies. They receive the agreements made with the other company before they reach the other party and change the bank account information by creating a false proforma. Then, when the contracted company sends money without confirming the account number, money is withdrawn by the suspects. Sometimes this happens through the email system, and sometimes suspects open an account similar to the customer's email address. For example; “ayseoktan@egm.gv.tr” instead of “ayseokutan@egm.gov.tr”.

Evil Twin: It is a false Wi-Fi service. Evil twin attack creates a fake modem to exploit WPA / WPA2 security. When the victim enters this modem with their password, the modem is seized.

SQL Injection: SQL injection is a security problem that causes attackers to access the database. Code injection technique can destroy the database. Used to insert malicious code into SQL commands through a web page. SQL injection is usually a SQL command that runs unannounced in the database when the user is prompted for an entry, such as a username.

Sniffing: Sniffing intercepts data. Sniffer tools can be captured in the network packets can be read content. The purpose of sniffing is to capture passwords (email, web, ftp, telnet, SQL), files transferred to email text (email, ftp).

IP Spoofing: IP Spoofing is the use of an IP address for the purposes of hackers by performing IP misleading. In spite of the differences in the IP addresses they actually have, they can be hidden or emulate any other person. IP Spoofing is commonly used for free or commercially available software that is sold illegally. It is no longer valid.

Hoax Mail: An email hoax is a scam that is distributed in email form. It is designed to deceive and defraud email recipients, often for monetary gain. Phakemail is considered a computer fraud.

Spam: Too many people are sent. Its purpose is to do advertising and fraud. E-mail may contain malicious software. Illegal e-mails that come from unfamiliar persons or go to unrecognized persons without the consent of individuals.

Zero-day: Zero-day is software or hardware flaws that are previously unknown or undetected but contain vulnerabilities that will lead to serious attacks. Zero-day openings are often weaknesses that are difficult to detect until the attack occurs. The Zero-day attack occurs when developers exploit the vulnerability and spread malware before developers have the opportunity to release a patch or fix.

Advanced Persistent Threat (APT): These are target-oriented attacks aimed at collecting user or organization information. It is difficult to identify these attacks because it is aimed at a specific target or institution, can circumvent traditional security mechanisms and operate in target institutions for a long time. They are software that is stored using operating system features and architecture and cannot be found by traditional methods, acting as a spy on a computer. Antivirus, antihacker, antimalware, such as any standard protective software is not possible to detect this type of threat, spread over time, continuous and versatile.

Internal Threats: Employees do not leave traces. It occurs when employees have the right to privileged information. It's because internal security rules are sloppy.

Hacking: It is the event of unauthorized access to computer or phone via the internet by taking advantage of system vulnerabilities in order to collect general information about the system used and to access or copy all data in this tool. It is intended to stop the operation of the system. Hacking is a form of destructive cybercrime.

Server / Server Hijacking Events: Malicious computer users, companies; they capture server computers with information such as personnel records, accounting and customer records, and encrypt files. After encryption, it leaves a file named "readme.txt" on the server screen. It leaves with an e-mail address to contact within the file. After the interview, they demand money and ask that this money be sent by various payment methods.

Software Vulnerabilities: The use of counterfeit software is the most common cause (Cracking). However, updates result in editing boot programs and leaving the programmer intentionally open. The weakness of other software is the lack of spelling work. Coding errors and logical errors are examples.

Juice Jacking: The cable used to charge the phone is also used to transfer data. Common charging points can be connected to some hidden computers that are paired with device when start charging. This is because listeners can illegally access all data stored on phone during charging. Malicious codes can then be injected with malicious chargers to steal data on device.

The Other Cybercrimes: Apart from the cybercrime mentioned here, there are crimes that can be seen at different times and in different ways. However, these are not common. These;

- Listen to the environment.
- Seize the server.
- Stealing trade secrets.
- Abusing data.
- Cyber money laundering.
- Capture personal data.
- Gambling over the Internet.
- To trade cyber illegal goods.
- Unauthorized access to informatics systems.
- Physical and logical computer sabotage.
- Unauthorized use of software protected by law.
- To sell drugs and drugs over the internet.
- Unauthorized use of computer software (pirated software).
- Providing prostitution or advertising prostitution over the Internet.
- Transferring money from internet banking account through fake sites and forums.
- Making illegal publications against personal rights and freedoms that target a specific person or group.

CHAPTER FIVE

TOOLS OF INFORMATICS CRIME INVESTIGATION

Evidence must be present to identify cybercrimes. It is necessary to know where the evidence can be determined by the type of crime. The evidence should be examined. Some tools are also required for the detection of this evidence.

5.1 Digital Evidence

Information systems or electronic devices capable of processing information automatically on the data storage media on or through these media, the evidence of the crime that can carry the nature of the crime and the data to provide illumination.

Any electronic device capable of storing data or passing digital data over it has the potential to contain digital evidence, whether or not it is a computer. Nowadays, electronic data storage and processing units have become so widespread. The digital is evidence in the field of forensic science is not only in the data storage units of computer systems. These results are in the fact that forensic informatics is no longer a science that is used only to obtain evidence in cybercrimes or in crimes committed by means of informatics. For example, in a hacking event, forensic informatics can examine the data of the hacker's computer as evidence, as well as the digital data of the suspect's computer system in order to clarify the crime of forgery or murder on the document. In addition, forensic information science, whether it is a normal crime or an informational crime or an informational crime, investigates the suspect's mobile phone, digital camera, electronic personal management systems, tablet computer, etc. in order to illuminate the crime.

In addition to meeting the requirements of reason, material truth and law; to provide evidence of the offense and be legally acquired, authentic, verifiable, sufficiently convincing, relevant and available to the court; capable of storing and processing digital audio, video, data and programs; electronic, electromagnetic, electrooptic structure; disk, floppy disk, CD, DVD, mobile phone, personal management systems devices, flash memory, SIM-SD-MMC cards, computer and computer internal or

external hardware, printing, transmission and network active devices and their software and similar electronic devices maintained in the enumerated environments; audio, video, data and software. Information systems, media or digital media; any data that may constitute evidence of crime is considered as digital evidence.

There are differences between numerical evidence and paper-based evidence. It is divided into quantitative differences and qualitative differences:

- a. Quantitative differences:** There is a size difference because too many documents can be stored in a very small volume. Due to the rapidly changing technology, format differences may occur in the recovery of obsolete computers and electronic documents. Electronic documents compared to paper documents; easier, faster and much more quantities can be reproduced. Electronic documents are more difficult to understand than paper documents.
- b. Qualitative Differences:** Computer data can change over time without human intervention. Computer data may become incomprehensible when separated from their respective environments. Electronic documents can come in many different formats, they are variable. Electronic data may contain rich confidential information. In some cases, it may be difficult to identify the source of electronic documents.

5.2 Types of Digital Evidence

The technological products found at the scene are all evidence. Therefore, these devices should be examined by forensic IT teams. The data detected in the environments where digital evidence exists, constitute the types of digital evidence according to the environments in which they are received.

Types of digital evidence likely to be found on computer systems data units: In general, on computer hard disks; documents, word processing files, images, audio and video files, database files, database access records, e-mail or chat records, internet

history, access passwords and usernames. Deleted files and deleted disk areas, encrypted or encrypted files, file privileges and dates (creation, access, delete, etc.) are displayed. System registry information (Registry, Event Log, etc.), services provided by the system can be damaged by malicious software such as viruses, trojans, spyware. Software installed on the system and virtual disk space and RAM information. For this reason, all computers, laptops and tablets should be taken on or off.

CD, DVD, Floppy and USB Hard Disk with Flash Disk on: Since the operating systems that can work on USB hard disk and USB flash memory are not read-only, the media can contain digital data that can be found on computer hard disks. If such a situation is encountered, the forensic IT specialist should also look at the data that the computer systems are examining on the hard drives of the USB hard disk or flash drives running the operating system. CDs, DVDs, HD, Blu-ray media should be examined as they may contain data that may affect the resolution of the event.

On Tape / Cassette / Cartridge backup units such as ZIP, DAT, DLT: Although these units usually have backups of files or records on systems, backups are often compressed with special software in different formats.

Possible types of digital nuts on Memory Cards: Dates of existing files can be determined. In very extreme cases, some memory cards may also contain specific operating systems that can be found on USB flash drives. In such cases, it is necessary to investigate detailed data to obtain evidence, such as computer hard drives. Especially in embedded minicomputer systems, CF or SD style data storage units can be used. This means that these cards can be used as storage units on the systems they work on, such as hard drives.

USB memory cards are very popular because they are small in size and capable of storing data. All USB sticks seen at the scene should be imaged for review. Many electronic devices exceed memory requirements by using memory cards. Therefore, the data stored on these cards can be used as digital evidence.

Digital deli types likely to be in the Digital Camera, Camera, MP3 Player:

Since they contain a memory card, USB has all the types of evidence obtained from the memory card.

Types of digital evidence likely to be found in mobile phones: Any data contained in mobile phones, pagers and personal management systems is evidence. Many evidences are obtained from mobile phone data. Every cell phone data is evidence.

Digital crazy types that are likely to be found in Game Consoles: The so-called PlayStation and XBOX game consoles have developed so much that they include processors in computer systems and hard drives, the storage unit. Especially with some modifications in devices such as XBOX, the Linux operating system, which is preferred by hackers as the number one in the information society, can be installed on the data storage unit of the device. Thus, the digital evidence of almost any crime can be found on the game consoles, which are almost a PC feature.

As far as forensic IT specialist is concerned, the game consoles that can be noticed during the first crime scene investigation will not be able to obtain sound evidence as they may be overlooked in an uninformed and careless crime scene investigation. On modified game consoles discs; documents, word processing files, images, audio and video files. Database files, database access records are kept. E-mail or chat records appear on internet history. Access passwords, usernames, deleted files and deleted disk space can be seen. Encrypted or encrypted files can be accessed. File authorizations and dates (creation, access, deletion) are stored in the system log information (Registry, Temp Log).

Malicious software such as viruses, trojans, spyware can seize device dominance. Hacking software, software installed on the system, virtual disk space and RAM information can be captured. In a modified game console, it is possible to come across all kinds of digital evidence that can be found in a normal computer. As mentioned above, recognizing the game consoles at the first scene and ignoring them only for the

game without thinking that it may contain evidence will ensure that the evidence cannot be fully obtained in an existing criminal investigation.

Types of digital deli that may be present in printer and fax machines: Some models of copiers, faxes, scanners, and printer devices contain an internal hard disk, which can contain information about the documents sent for writing earlier. Internal hard drives can also be used to store data. Therefore, these devices should be examined.

Some models of copiers, faxes, scanners, and printer devices contain an internal hard disk, which can contain information about the documents sent for writing earlier. Internal hard drives can also be used to store data. Therefore, these devices should be examined.

Types of digital evidence likely to be found on network devices: Most network devices (routers, switches, hardware firewalls) can host data such as network activity, access control, and network configuration. In the examination of these devices, Forensic IT specialist must know the network systems at an advanced level. The following list shows in general terms what kind of data can be found on network devices. On network devices, the network's configuration structure, access and routing information, and access control lists can be viewed. Hardware-based device lists (MAC IDs), some malfunction information on the network, performance and usage information of the network, unauthorized access information on the network are kept in the device. The data that can be found on the network devices may vary considerably according to the characteristics of the device. Knowing the device to be examined, knowing the factory data and features of the device are considered important in terms of drawing a road map before starting the examination.

Types of digital evidence likely to exist in the Internet and Network: In forensic informatics research area; IP detection and reporting, social media crimes (Threat, Envelope, Blackmail), examination and reporting of electronic evidence, access to the file, determination of the creation and final writing times, technical reporting on the history of the internet, mobile phone review, recovering deleted files and sections,

encrypted documents, word search on data-bearing electronic evidence, hash, file signature analysis, researching documents previously printed on a computer, Facebook, Twitter, Instagram Review is required.

Types of digital evidence likely to be found on External Hard Drives: External hard drives have large capacities to store a lot of digital data on them. For this reason, all of them should be taken for examination purposes. Network storage feature should be investigated.

Types of digital evidence that may be present on the answering machine: The cassettes in which messages left on the answering machine are recorded may be evidence. Because incoming calls are activated if they are not answered for a certain period of time and they allow the caller to leave a message.

Other Electronic Devices: Besides these devices, credit card printing, duplication, card skimmer, mobile phone cloning devices, GPSs, authorization cards, controls, electronic loading tickets, contour loading devices, digital system of all kinds of machinery and equipment; all devices that may be associated with a crime can contain both evidence and themselves.

5.3 Forensics Software, Hardware and Other Tools

After determining the research methods and determining what kind of information about the crime will be searched on the target digital evidence object, technical research should be carried out in detail with the support of digital evidence analysis software. However, EnCase and FTK software, which are commonly used by law enforcement officers in our country and which are digital evidence analysis software, are suitable for this purpose. Besides, a user who has little technical knowledge about the operation of information systems will not be able to perform a hundred percent examination with this software and will be able to perform simple operations presented in the menus of these software.

Software and hardware tools, forensic examiners, investigators, prosecutors and first responders to find the defense evidence they need to perform their duties. Intelligence solutions; assists investigation teams in accessing data, making sense of data, and progressing in the incident. Enables greater collaboration between departments at every stage of investigations in the field, laboratory and court. Thus, it protects the public and makes sure that the findings can be defended.

Depending on the chosen tools, the time required to collect stronger evidence may be shortened by solving the intelligence aspects of digital data. Industry-leading, award-winning digital forensic solutions are used. These tools provide the ability to make meaning and analysis. Improves workflows, streamlines processes and achieves higher throughputs making data accessible, collaborative and actionable across departments. It makes the decision faster and more confident by showing the whole picture more quickly. The means used to find evidence can be grouped as follows.

- Image Retrieval Tools
- Analysis Tools
- Make Inferences Tools
- Control Tools
- Platform Tools
- Additional Tools
- Accessories

5.3.1 Image Retrieval Tools

There are many tools to get the image. in order to prevent cyberattacks, to prevent IT crimes, to detect easily when there is a crime, our society and the personnel working during the progress of these processes need to be raised. Investigators should be able to identify mobile device hardware and have a general understanding of the judicial review process. They should inform about the JTAG process, electrical theory, methodologies and purpose. The two most important of these are Encase and FTK. Below, some tools are examined.

EnCase: EnCase is written by Guidance Software. Digital data analysis and analysis program. Performs image acquisition and reporting. It is used by many law enforcement agencies around the world for evidence review and evidence linking. In almost all courts in Europe and the United States, the reports and data submitted have been accepted as evidence (Software, 2019).

Forensic Tool Kit (FTK): Forensic Tool Kit is digital data analysis and analysis program. It can take images. Reporting. It is extensively used by security forces and courts. The reports and data submitted to the court are accepted as evidence. Forensic Informatics (Fight Against Cyber Crime - Cyber Policing) use rate is high. It is paid. FTK Forensic Toolkit Password can break (AccessData, 2019).

- Lists the contents when the image of the inserted disc or an image taken in supported formats is added.
- Everything is in category. Deleted files, files by extension, files by type.
- Collects email data on disk. It collects and reports all known e-mail formats from all over the disk.
- All images can be collected in the disc. Different lists can be made by filtering.
- Everything can be gathered together and reported.
- Performs fine search within the disc. Credit card number format, phone number format, date format, identification number format, such as plate format.
- Word search. Filters all data, whether deleted or not. Where it came from, when it was deleted, how it was encrypted.
- It filters and examines the information taken from the computer's ram image. There may be data not found on hard drives or deleted areas.

Forensic Tool Kit Imager: FTK Imager is developed by AccessData. It is free software. FTK is a complete computer criminal software. With FTK Imager, image retrieval can be performed by taking write protection measure. FTK Imager pre-examines digital evidence files and forensically extracts these images. With this software, local hard drives, USB memory cards, zip drives, CD and DVDs, directories or a single file can take the image. FTK Imager can analyze disk images. It also mounts

the corresponding disk image files as Read-only and prepares the media to be treated as a hard disk drive through Windows Explorer and allows the directory or files to be copied out from within the image files. It can also recover files that have been deleted and sent to the trash but have not yet been overwritten by another file. FTK Imager can generate Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1) hashes for the files to be analyzed. It can generate hash reports for normal files and disk images. Versions are available to run on Ubuntu, Fedora and Mac (AccessData, 2019).

Linux-dd: Linux-dd (2019) is using the dd tool on the Linux operating system, a raw image of a storage unit can also be retrieved. The image of the dd tool can be read by many digital evidences review software, including EnCase, ILook and FTK. Linux does not inherently access any data that is not mounted in the context of writing. Therefore, image acquisition and processing can be performed with write protection. Computer criministic research can be carried out with a lot of software already on Linux operating system.

Image Master Solo: Made by Intelligent Computer Systems. Just Copy. Quick and BIT-based copies. Gets the value of Hash with MD5 and SHA1 (ICS, 2019).

Logicube: Logicube (2019) makes one-to-one copy on a BIT basis. Gets the hash value. There is IDE-SATA support.

EnCase Boot Disk/CD: EnCase Boot Disk/CD (2019) is software for writing protection, image acquisition and digital evidence analysis. It is the most frequently used computer criminal software preferred by many police organizations including FBI.

Forensic Replicator: Forensic Replicator Paraben is a software image acquisition solution offered by Forensics Software. Paraben has software for digital evidence review and write protection equipment (Paraben Corporation, 2019).

Digital Intelligence Tools: Digital Intelligence Tools is one of the largest and oldest companies in the field of computer evidence making digital evidence inspection and acquisition devices. Inspection and image acquisition equipment specially designed for all types of data storage units are available within Digital Intelligence (Products Services Training, 2019).

Image Master Solo: Image Master Solo device takes perfect image. Hash import uses a variety of compression algorithms, except one-to-one copying (ICS, 2019).

Forensic Computers: It is a high-quality company in which computer criminal devices are supplied to the Turkish Police for the first time. It has the support of the US Air Force and the FBI (Forensic Computers, 2019).

LC-technology: Ready digital evidence review systems are useful. Digital Evidence is the most widely used tool in the field of examination in the European Union. However, it may be insufficient in some cases (LC Technology, 2019).

5.3.2 Analysis Tools

There is intelligence in the raw data. The event proceeds quickly and complex analysis is automated by means of tools. This saves time and it can generate tips. Data is combined and visualized in an integrated cross-resource format to quickly identify critical relationships and connections. Work in coordination. It is collected the strongest evidence possible. The findings are easily shared with the entire investigation team.

Cellebrite Field: It provides intuitive and judicially valid tools for staff to quickly access digital evidence and prioritize evidence. Whether in the vehicle, on a durable device or at a police station, border control point or airport, field personnel and investigators can take action when even minutes are important (Cellebrite, 2019).

Analytics Series: It allows to get rid of time-consuming analyzes and convert raw data into intelligence that can take action. Large amounts of different mobile, cloud, computer, and telephony companies automatically consolidate data sources so that users can quickly and accurately detect patterns by organizing, searching, matching, visualizing, and managing data simultaneously (Cellebrite Analytics, 2019).

Analytics Desktop: Converts raw data to digital intelligence. Advanced text and image analysis engines instantly detect images and videos related to important categories such as weapons, nudity, faces or suspicions of child abuse. It combines, associates, analyzes, and cross-references data sets from computer, cloud, and telephony companies. Reveal name, address, location and more information from inheritances such as e-mail, website and text messages. Automatically detects related or blacklisted images by comparison of digital signatures (UFED Analytics Desktop, 2019).

Analytics Enterprise: Mobile, cloud, computer and library to collect a single image. Find critical evidence hidden in text, images, video and so on. It automatically indexes, stores and manages all digital evidence belonging to hundreds of events in a single center. Perform cross-case analysis by subject, crime type or time interval. Reveals and visualizes common connections, patterns and trends. Enables seamless integration into the organization's existing IT ecosystem, programs, hash value databases including Project VIC and Child Abuse Photo Analysis (CAID) (UFED Analytics Enterprise, 2019).

Reader: Provides in-depth data exploration using advanced analysis functions such as advanced search, filtering, timeline and labels. Generates and customizes reports in multiple formats (Cellebrite Reader, 2019).

5.3.3 Make Inferences Tools

Access data from the latest iOS and Android digital devices using strong encryption. It extracts critical evidence from sensitive devices, including those that are crushed,

broken, burned or damaged by water. The tools used to make inferences are given below.

UFED Ultimate: Usually used in mobile reviews. It finds critical evidence and shares the findings with the investigation team. Has advanced digital forensic review capabilities. The pattern overcomes the difficulties of bypassing and encrypting password or PIN passwords. It provides access to active, confidential and even deleted data from smartphones, new phones, tablets, players, GPS devices, SIM cards, smart watches, mass storage devices and more (UFED Ultimate, 2019).

UFED InField: First responders and investigators, whether on-board, on a durable device or at a police station, border control point or airport, can take actionable data when minutes are important. Maintains data integrity and accelerates investigation. Reveals real-time hint generation and actionable insight. The contact selects only the relevant information from information such as e-mail and telephone. Copies only certain evidence from witnesses or victims' phones (UFED InField, 2019).

5.3.4 Control Tools

The management of forensic tools should be simplified. Since digital evidence collection has become an integral part of many incidents and investigations, it should improve the use and maintenance of the placement of forensic tools both in the laboratory and in the field.

Central Management System: Remotely manage devices and systems by deploying and updating software, changes, and permission controls from a central location, collecting usage statistics and reporting to demonstrate operational efficiency and demonstrate effectiveness. Automatically backups the metadata of each extraction process and maintains activity logs to ensure the integrity of evidence (Central Management System, 2019).

5.3.5 Platform Tools

The intelligence need should be accessed whenever and wherever need it. Support unmatched workflows and environments, whether in the laboratory, on-site or in the central office.

4PC: It is a software-only solution that can be used on any hardware. Laboratory review, field investigation, review of findings in the office, or management of digital forensic tools in an IT department is used. UFED 4PC application was developed by Cellebrite. It is a widely used software for forensic investigations on mobile devices. It could accessed the history of calls made via a smartphone, recordings of conversations made through chat applications, lists of applications installed on the smartphone, which addresses are visited on the internet, and much more. It is preferred by law enforcement officers to be used in the forensic information laboratory thanks to the wide mobile device support it provides (UFED, 2016).

Appliance: With the plug-and-play equipment, the distribution, preservation and procurement of digital forensic investment is facilitated.

Kiosk: Provides easy extraction and use of mobile data in specific locations, such as outposts and border checkpoints, with front-line teams. It gives strength to the teams with intuition.

5.3.6 Additional Tools

Digital forensic review operations can be enriched with a number of tools to organize the process and complete the workflow. Provides reliable access to digital intelligence that can advance the event and protect our communities (Cellebrite, 2019).

UFED Chinex: Chipsets extract data from a large number of phones in use. Automatic pinout recognition (UFED Chinex, 2019).

UFED Camera: It supports the process of collecting evidence by capturing data, device, or screenshots even when data extraction is not possible. The device captures images and videos as evidence (UFED Camera Kit, 2019).

5.3.7 Accessories

In addition to software tools, there are a number of tools that seem to be insignificant, which actually assist in the identification, analysis and resolution of evidence (Products Updates, 2019).

End and Cable Set Organizer: A complete set of UFED cables and compact end connectors with main cables for extraction and charging.

Faraday Bag: Used to isolate the mobile device from any external network signal.

Multi SIM Adapter: Universal NanoSIM, MicroSIM and SIM card adapter for cloning and removal.

Telephone Power Cord: A cord that charges the mobile device through an UFED device when disconnecting from a discharged, non-battery or non-charging device, or during extended extraction operations.

Write Protected UFED Memory Card Reader: A multi-format card reader that provides read-only or read / write access.

Car Charger Adapter with Phone Power Cord: This adapter enables the UFED to be used in the vehicle.

UFED 4PC Device Adapter: Extracts data from some connection types using the USB port of computers; SIM card, USB, RJ45 (UFED,2016).

Bags: The UFED device is protected with ruggedized and standard bags. Peripherals and accessories are supported.



CHAPTER SIX

A FRAMEWORK FOR CYBER CRIME INVESTIGATION

The detection of perpetrators in investigations initiated due to crimes committed through social sharing platforms or websites varies according to the means used. In this section referred primarily to an unusual situation that needs to be done when encountered. After determining the type of crime that causes this situation, it will cover the steps taken to find cyber criminals. In addition, it will be covered what the experts fighting cyber criminals need to do to improve themselves.

6.1 Confronting Crime

Following exposure to an offense, people understand when a loss. People who do not follow technology closely may take a long time to identify the cause of this change. Because each crime has its own effects. With the actions of unconscious people, the arguments that will help to identify the perpetrator may be lost or they may damage the device completely. In this section, the steps to be taken according to the unusual situation are very briefly mentioned. A draft has been prepared, which will allow to determine which offense the problems are faced by considering the crimes that the thesis provides (Figure 6.1). When a link or sharing with malicious content is received over e-mail, when a non-real content site is encountered, when an insult is exposed via social media, when threat messages that encrypt the device are received, when data loss occurs during data transmission or when don't access to the system is shown in this diagram.

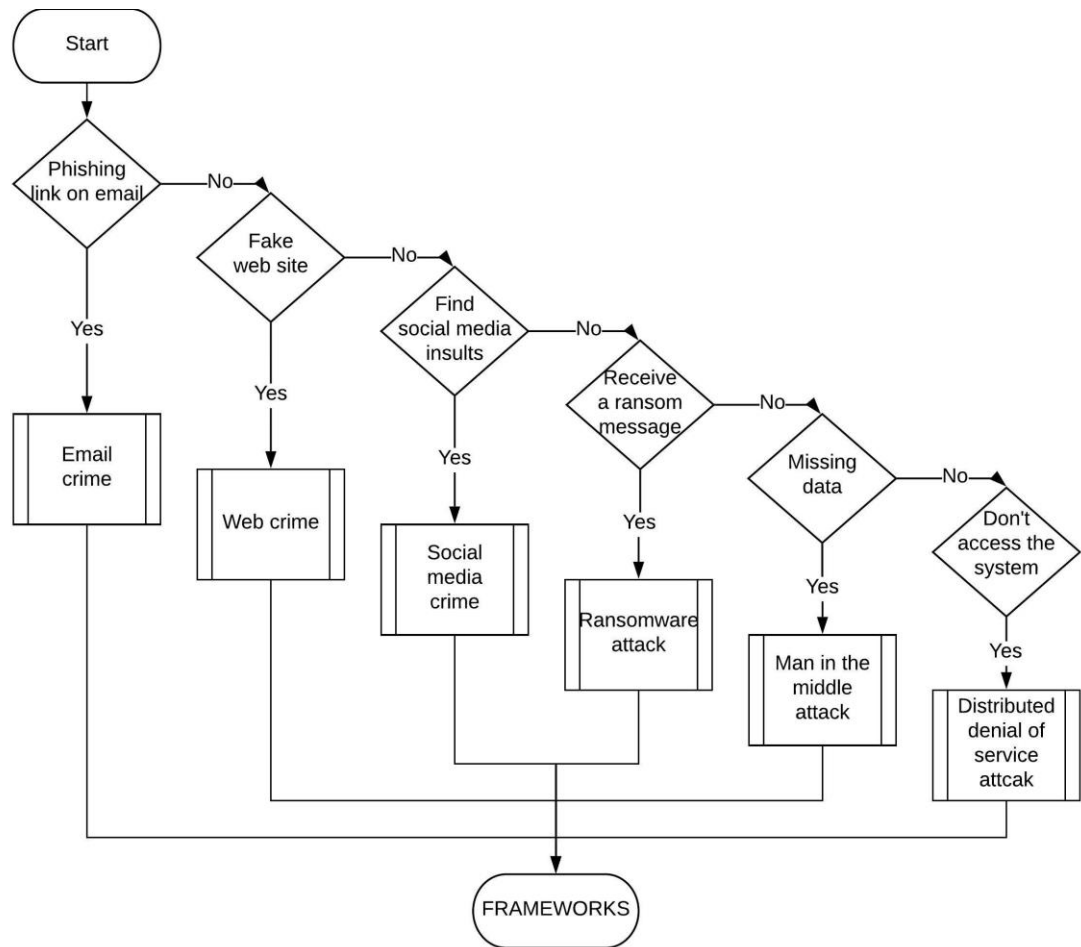


Figure 6.1 Confronting crime

When the victim encounters any negative situation via email, web, social media, it is relatively simple to do compared to other crimes. There is no situation that should intervene except that it delivers the date, time and most importantly the information of the crime to the relevant law enforcement officers. The procedure is shown in Figure 6.2. For these three offenses, the user needs to communicate easily accessible information, such as time, date and link, to the law enforcement agencies without extra effort.

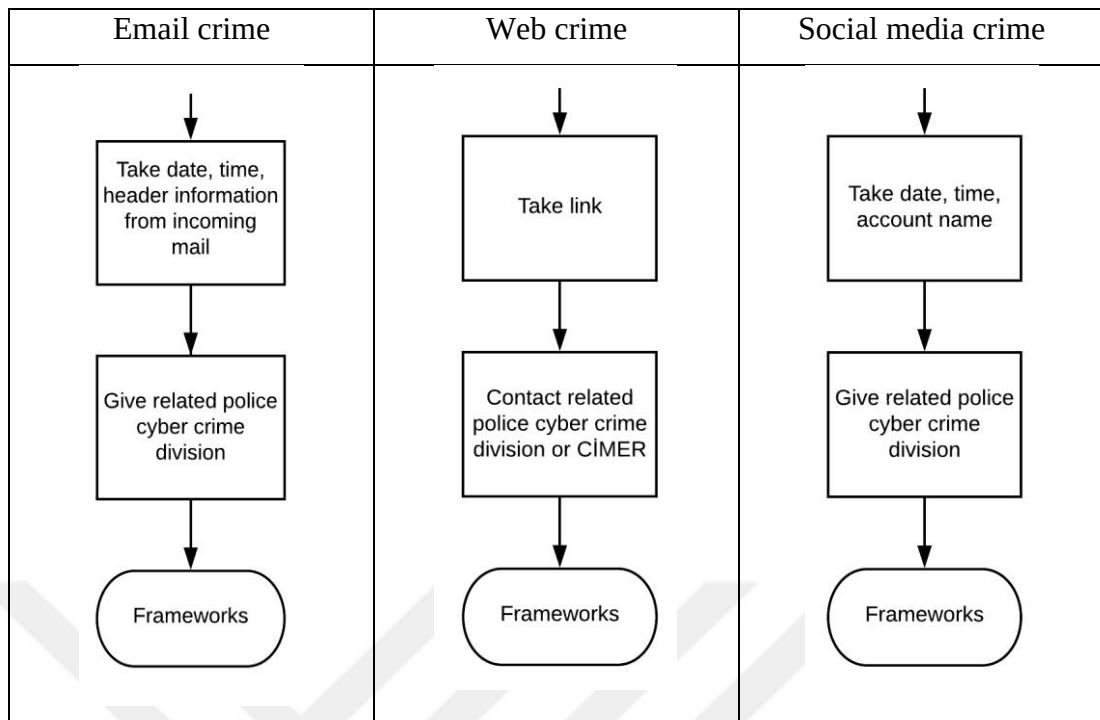


Figure 6.2 What to do when faced with cybercrime

If there is no access to the system, a message is sent to the device, a ransom is requested, or there is a disconnection during the communication, a missing packet is transmitted; one needs to take on some responsibilities. It should not interfere with the device at all, especially the device. Related analysis or needs to get help from technical units to make the purchase log. Victims who do not receive technical support from IT experts or law enforcement agencies do not seem to be able to complete this process in a positive way. This is because the necessary evidence consists of log and analysis results collected during this period. These issues are summarized in Figure 6.3.

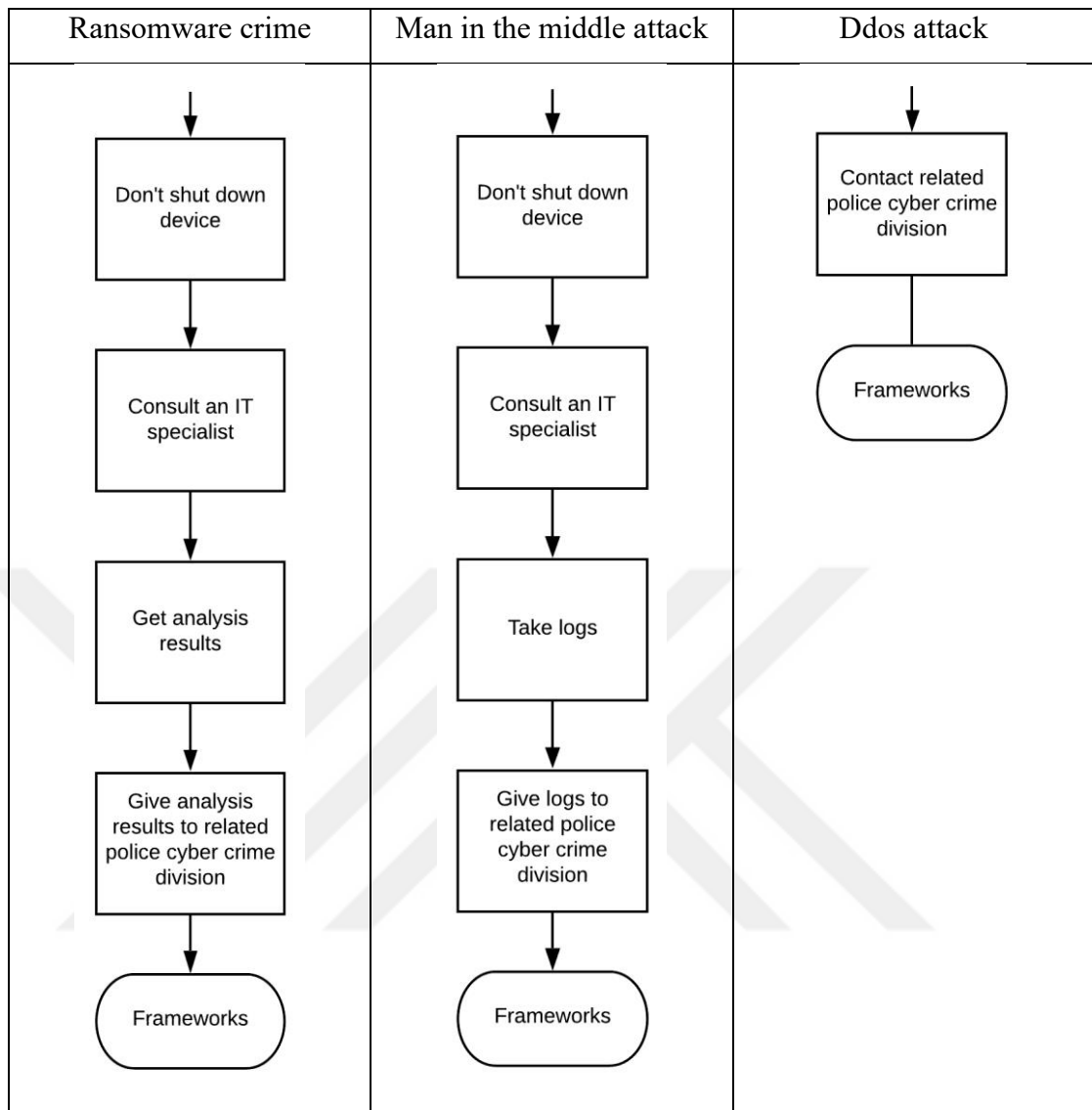


Figure 6.3 What to do when faced with cyber attacks

6.2 Steps to Find Cyber Criminals

6.2.1 Detecting a person who commit a crime with e-mail

One of the most common ways of committing crimes on the internet is through the e-mail address. Entering the system by breaking the e-mail password of another person can be defined as “Crimes in The Field of Informatics” (TPC 243-244).

In this case, the first step in finding the virtual criminal who sends these emails is to find out from which IP address the incoming mail came from. Incoming e-mails are

opened to find IP address from incoming mails. If the mail tool used is Gmail, click show original from “Other Options” above the opened message. Yahoo users click on the “View Full Headers” information of the incoming mail options. Outlook users can access Header information by clicking “Show message source”. The mail header is given in Figure 6.4.

```

dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=isbank.com.tr
Return-Path: <9d676be8-dba4-47c2-acbd-aaa400fcf98a@ileti.isbank.com.tr>
Received: from amanos.isbank.com.tr (amos.isbank.com.tr. [213.161.149.42])
    by mx.google.com with ESMTPS id q1si3676996wmj.38.2019.08.09.05.21.19
    for <ayseokur@gmail.com>
    (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
    Fri, 09 Aug 2019 05:21:20 -0700 (PDT)
Received-SPF: pass (google.com: domain of 9d676be8-dba4-47c2-acbd-aaa400fcf98a@ileti.isbank.com.tr designates
213.161.149.42 as permitted sender) client-ip=213.161.149.42;
Authentication-Results: mx.google.com;
    dkim=pass header.i=@ileti.isbank.com.tr header.s=ileti2 header.b="BHLrgs+/"
    spf=pass (google.com: domain of 9d676be8-dba4-47c2-acbd-aaa400fcf98a@ileti.isbank.com.tr designates
213.161.149.42 as permitted sender) smtp.mailfrom=9d676be8-dba4-47c2-acbd-aaa400fcf98a@ileti.isbank.com.tr;
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=isbank.com.tr
DKIM-Signature: v=1; a=rsa-sha256; d=ileti.isbank.com.tr; s=ileti2; c=relaxed/relaxed; q=dns/txt;
i=@ileti.isbank.com.tr; t=1565353303; x=1567945303; h=From:To:Date; bh=BnXT/RIANPDDvNIYeA8byAVIjSGLcQhG81W9eQnjWwA=;
b=BHLrgs+/wzROBzuA/hmr4Ybcw58vPV8KKEZox5M98gffBkJyQbpV2x18iEA05xMp
3/xMqDspI3/918YKJ3d7h4EWXQg1GqMwZVhjl0YvFuC8hCqmgYD3et66dHN/254 Au3azQ3N7J79tgmy7XF3VrnsPZCW09kyTgo1gLEYjzo=;
X-AuditID: 0a505220-370ba9e000003eaa-1e-5d4d6557d953
Received: from KWSMCAAPP08 (Unknown_Domain [10.80.82.42]) by amanos.isbank.com.tr (ISBANK SMTP K) with SMTP id
A6.F2.16042.7556D4D5; Fri,
    9 Aug 2019 15:21:43 +0300 (AST)
mime-version: 1.0

```

Figure 6.4 IP by "Received from"

As seen from the line starting with “Received: from”, it could be determined which IP address it comes from. The methods shown in the phishing detection section are followed to detect if the IP address is the known offender. Once the IP address has been identified, there are several different methods to be followed in order to reach the offender (Figure 6.5). Of these methods, the most appropriate one is preferred and it is tried to determine who the IP address belongs to.

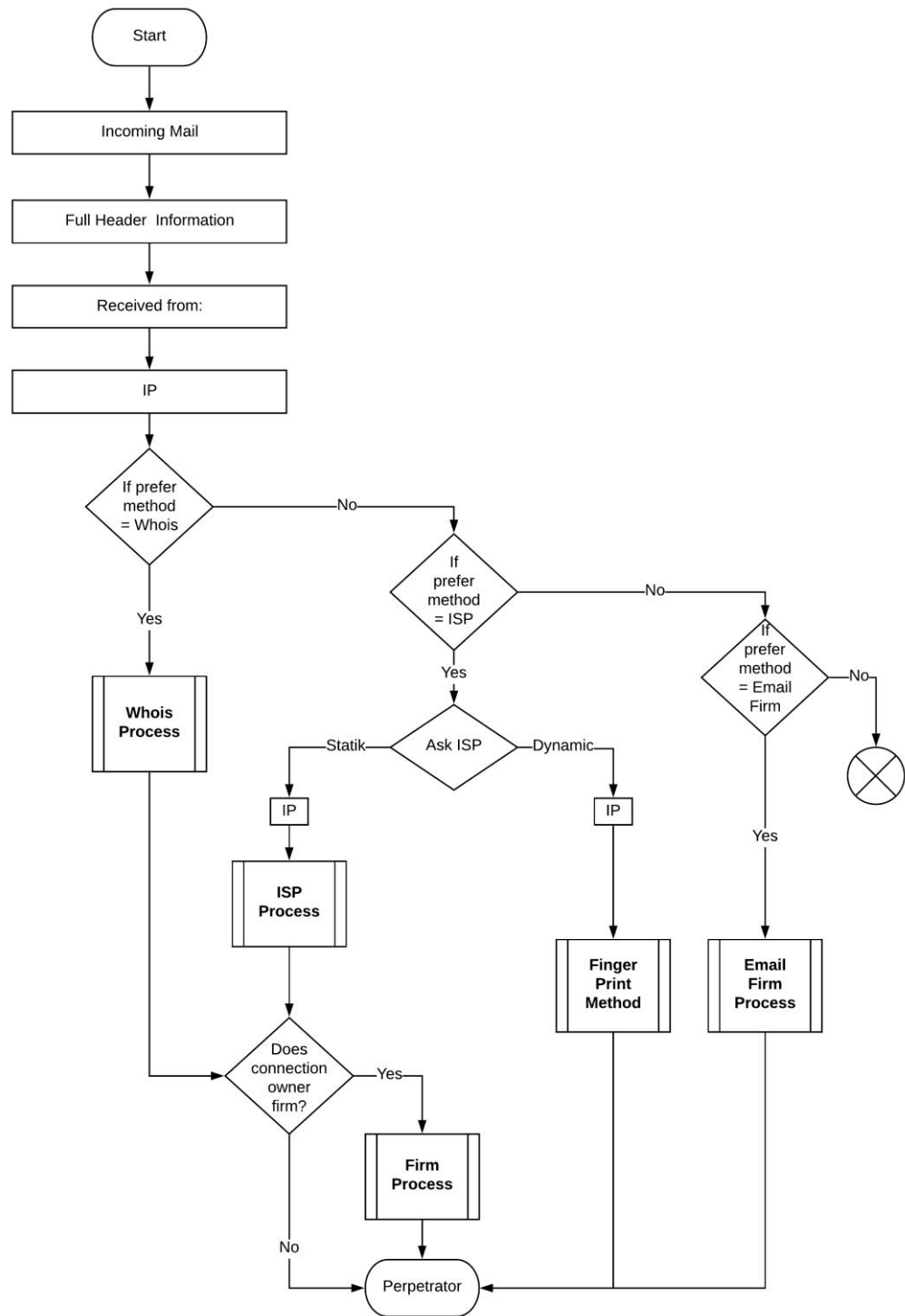


Figure 6.5 Framework for identifying an offender by e-mail

The first method a person who has been attacked via email should investigate is whois in Figure 6.6. The “WHOIS” query provides the domain name and identity information from the IP address in Figure 6.7 and Figure 6.8.

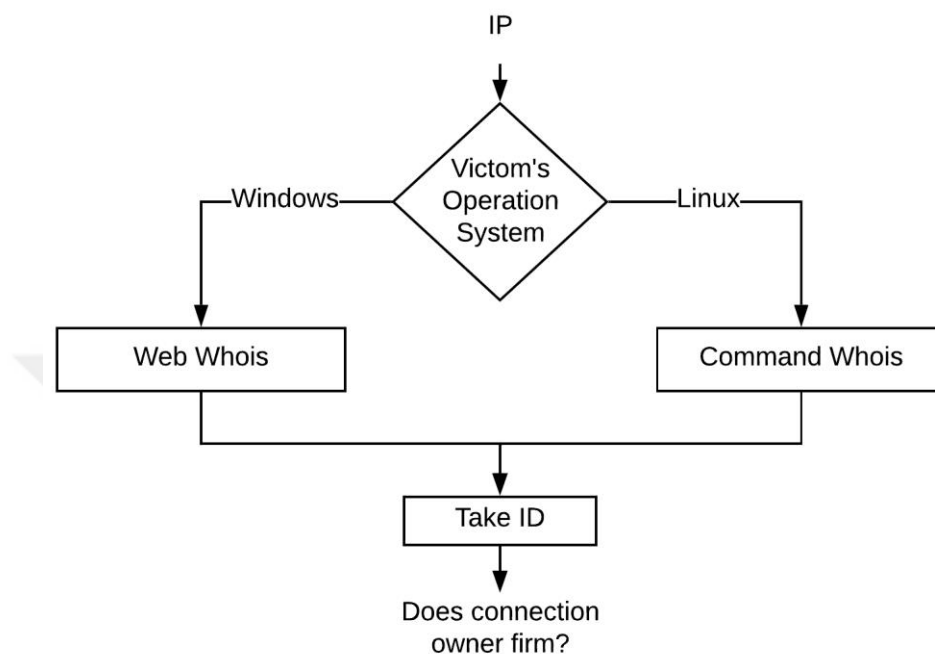


Figure 6.6 Whois Process” in e-mail framework

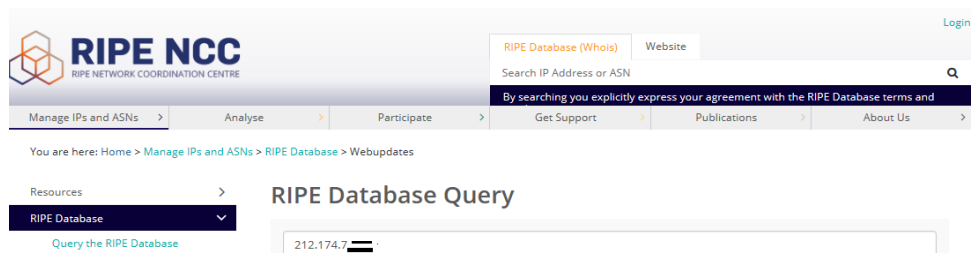


Figure 6.7 Query with IP address

route: 212.174.74
descr: TURKTELEKOMCOMPANY
origin: AS19905
mnt-by: MAINT-AS7786
source: RADB-GRS
remarks: *****
remarks: * THIS OBJECT IS MODIFIED
remarks: * Please note that all data that is generally regarded as personal
remarks: * data has been removed from this object.
remarks: * To view the original object, please query the RADB Database at:
remarks: * http://www.radb.net/
remarks: *****

RIPEstat

Responsible organisation: Turk Telekomunikasyon Anonim Sirketi
Abuse contact info: abuse@ttnet.com.tr

inetnum: 212.174. - 212.174.
netname: Gayrettepe_Interface_IP
descr: Gayrettepe Interface IP
country: TR
admin-c: DUMY-RIPE
tech-c: DUMY-RIPE
status: ASSIGNED PA
mnt-by: AS9121-MNT
created: 2009-03-23T09:30:22Z
last-modified: 2009-12-02T13:11:40Z
source: RIPE-GRS
remarks: *****
remarks: * THIS OBJECT IS MODIFIED
remarks: * Please note that all data that is generally regarded as personal
remarks: * data has been removed from this object.
remarks: * To view the original object, please query the RIPE Database at:
remarks: * http://www.ripe.net/whois
remarks: *****

RIPEstat

route: 212.174.
descr: TurkTelecom
origin: AS9121
mnt-by: AS9121-MNT
created: 2004-12-14T13:04:10Z
last-modified: 2004-12-14T13:04:10Z
source: RIPE-GRS
remarks: *****
remarks: * THIS OBJECT IS MODIFIED
remarks: * Please note that all data that is generally regarded as personal
remarks: * data has been removed from this object.
remarks: * To view the original object, please query the RIPE Database at:
remarks: * http://www.ripe.net/whois
remarks: *****

RIPEstat

Figure 6.8 Domain and IP information with RIPE

If the website that communicates with the victim is followed, the offender can be accessed. For this, IANA web, which is a reliable source, can provide the necessary information (Figure 6.9). This allows access to the IP address information. This query; site information, domain name credentials, IP credentials, such as the identification of the offender will help to learn the most important information. With this information, the Directorate of Anti-Cyber Crimes Department of the Police Department determines who the site owners are.

IANA WHOIS Service

The IANA WHOIS Service is provided using the WHOIS protocol on port 43. This web gateway will query arguments are domain names, IP addresses and AS numbers.

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:      whois.verisign-grs.com

domain:     COM

organisation: VeriSign Global Registry Services
address:    12061 Bluemont Way
address:    Reston Virginia 20190
address:    United States

contact:    administrative
name:       Registry Customer Service
organisation: VeriSign Global Registry Services
address:    12061 Bluemont Way
address:    Reston Virginia 20190
address:    United States
phone:      +1 703 925-69^^
fax-no:     +1 703 948 39^^
e-mail:     info@verisign-.com

contact:    technical
name:       Registry Customer Service
organisation: VeriSign Global Registry Services
address:    12061 Bluemont Way
address:    Reston Virginia 20190
address:    United States
phone:      +1 703 925-69^^
fax-no:     +1 703 948 35^^
e-mail:     info@verisign-.com

nservers:   A.GTLD-SERVERS.NET 192.5.1.2001:503:a83e:0:0:0:2:30
            B.GTLD-SERVERS.NET 192.33.1.2001:503:231d:0:0:0:2:30
            C.GTLD-SERVERS.NET 192.26.9.2001:503:83eb:0:0:0:0:30
            D.GTLD-SERVERS.NET 192.31.8.2001:500:856e:0:0:0:0:30
            E.GTLD-SERVERS.NET 192.12.9.2001:502:1ca1:0:0:0:0:30
            F.GTLD-SERVERS.NET 192.35.5.2001:503:d414:0:0:0:0:30
            G.GTLD-SERVERS.NET 192.42.9.2001:503:eea3:0:0:0:0:30
            H.GTLD-SERVERS.NET 192.54.1.2001:502:8cc:0:0:0:0:30
            I.GTLD-SERVERS.NET 192.43.1.2001:503:39c1:0:0:0:0:30
            J.GTLD-SERVERS.NET 192.48.2001:502:7094:0:0:0:0:30
            K.GTLD-SERVERS.NET 192.52.1.2001:503:d2d:0:0:0:0:30
            L.GTLD-SERVERS.NET 192.41.1.2001:500:d937:0:0:0:0:30
            M.GTLD-SERVERS.NET 192.55.2001:501:b1f9:0:0:0:0:30
            ds-rdata: 30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184

whois:      whois.verisign-grs.com

status:     ACTIVE
remarks:    Registration information: http://www.verisigninc.com

created:    1985-01-01
changed:    2017-10-05
source:     IANA
```

Figure 6.9 “Whois” query with domain name

Another method is to obtain information from the company of the e-mail address used by the perpetrator (Figure 6.10). If it is possible to obtain crime date and time information from companies, it is easy to reach the perpetrator from the IP address. This information can be requested from e-mail companies. But the same problems are likely for email companies as described in their social media accounts. To determine the perpetrator's e-mail account information from official branch in Turkey is still not difficult. But by the judicial authorities to the branch, writing said the company is providing information to the Turkey branch demand a warrant and specifying the time of the crime date, that date to this e-mail address may be asked providing connections from any IP address and can be detected in this way IP address.

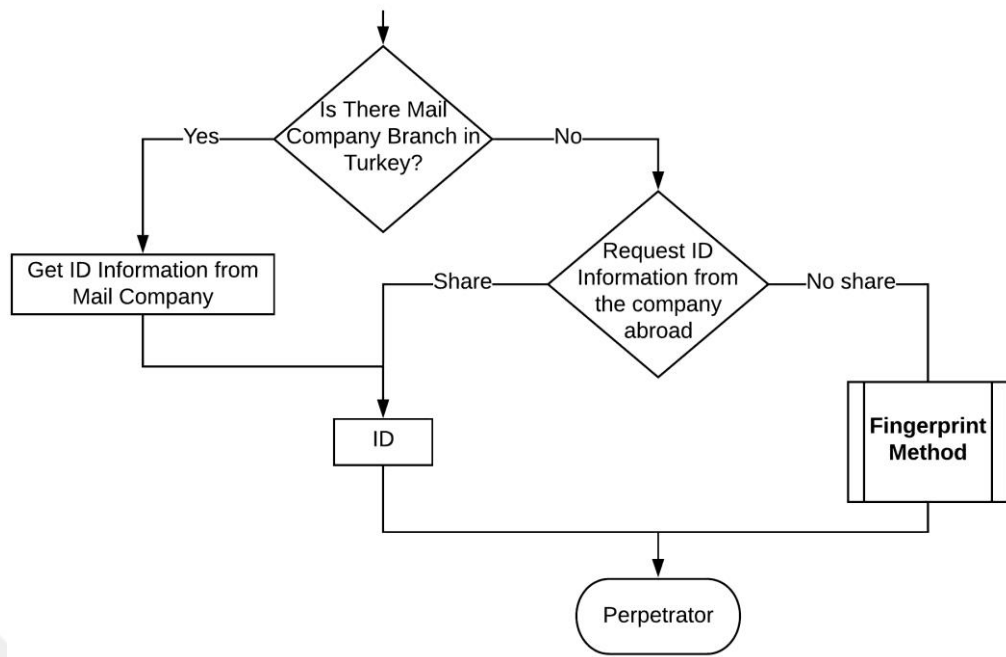


Figure 6.10 “Email Firm Process” in e-mail framework

Another method that can be applied after learning the IP number is using internet service providers (Figure 6.11). After finding out the IP number, it should be determined which internet service provider the perpetrator receives service from. (Such as Türk Telekom or Superonline). By contacting the service provider company, the identity of the perpetrator can be obtained by asking the name of the identified IP address.

Another option with the use of bulk IP addresses is workplaces. Businesses can have hundreds of computers. However, every computer in the workplace is represented by a single IP outside because it runs through a single service provider. It may be necessary to find out which computer has committed a crime in the company. Each computer has its own unique IP within the company. This private IP number is also available from the company. If the IP address belongs to a home, if the perpetrator sent the e-mail from his personal computer at home, the IP number will belong to any service provider (Türk Telekom, Superonline, Turk.net, etc.). Service providers know when a person connects to the Internet with which IP number, but reserves it. The IP must be requested through the prosecution office.

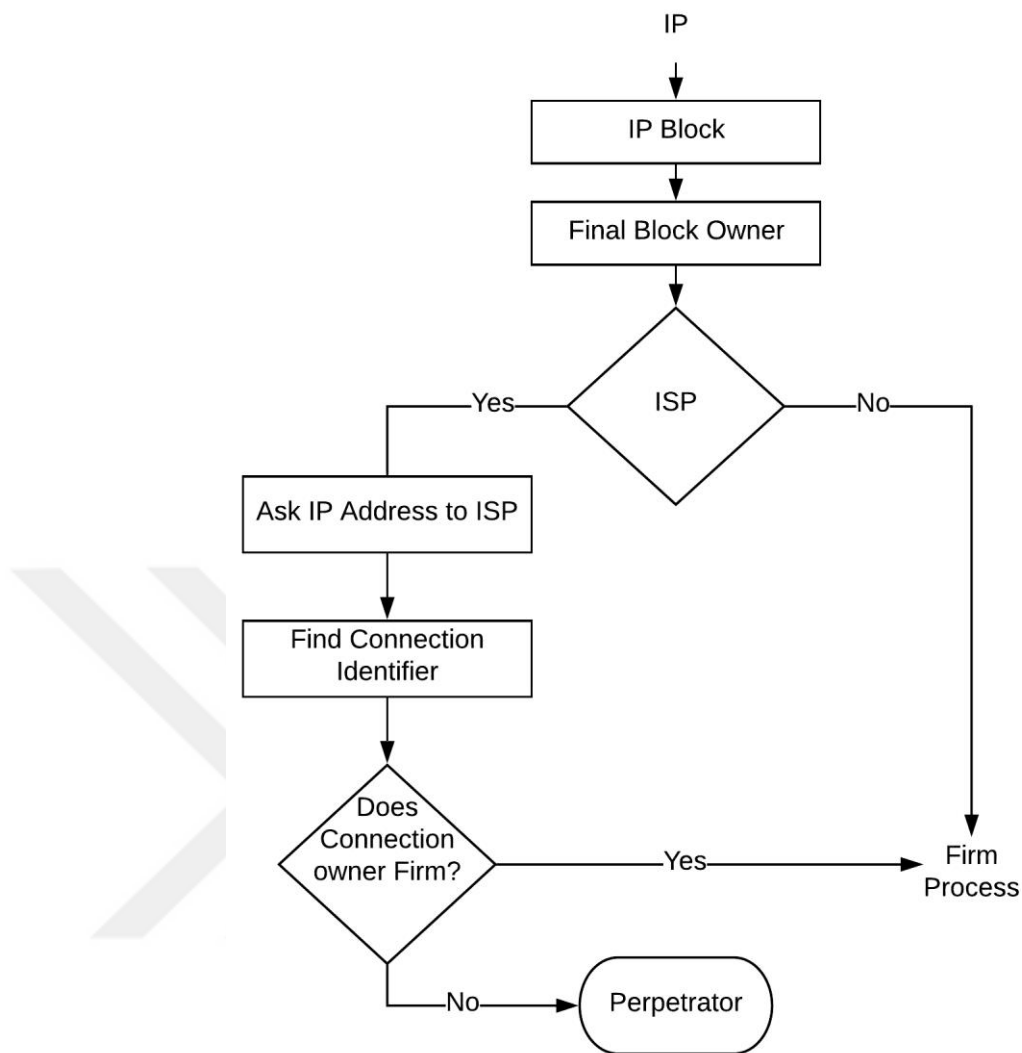


Figure 6.11 “ISP Process” in e-mail framework

IP addresses can be detected using all these methods. But IP addresses are divided into Dynamic IP and Static IP. The addresses of computers with static IP addresses do not change. The IP addresses of the user who connects to the Internet with dynamic IP addresses change each time they connect to the Internet. Each connection is assigned an IP address that is currently empty at the service provider. In this respect, the IP addresses found by the mentioned processes may not reach the correct result. For this reason, it should be learned from companies whether the person whose IP result is detected uses dynamic IP or static IP. If the perpetrator uses a dynamic IP that is changing, the IP address should be determined by the classic methods written above, along with the date and time of the offense.

Each IP address obtained does not show the correct result. Because this IP address may be taken from places such as cafes, parks and libraries where mass internet use is made. If sent e-mails are sent from places such as cafes, hotels, student dormitories with internet connection, IP detection will target this place of mass use. Since the IP information of the Internet cafe or the temporarily located site is accessed, it is difficult to access user information and thus the perpetrator. To avoid such problems, access providers need to take preventive measures to access criminal offenses. Most importantly, the internal IP distribution logs must be recorded electronically in the system. In this case, when a crime is committed through a mass-use provider, internal IP distribution logs should be obtained from them and the date of the crime should be reached on time. The perpetrator is then accessed from the internal IP of the user using the internet connection (Figure 6.12).

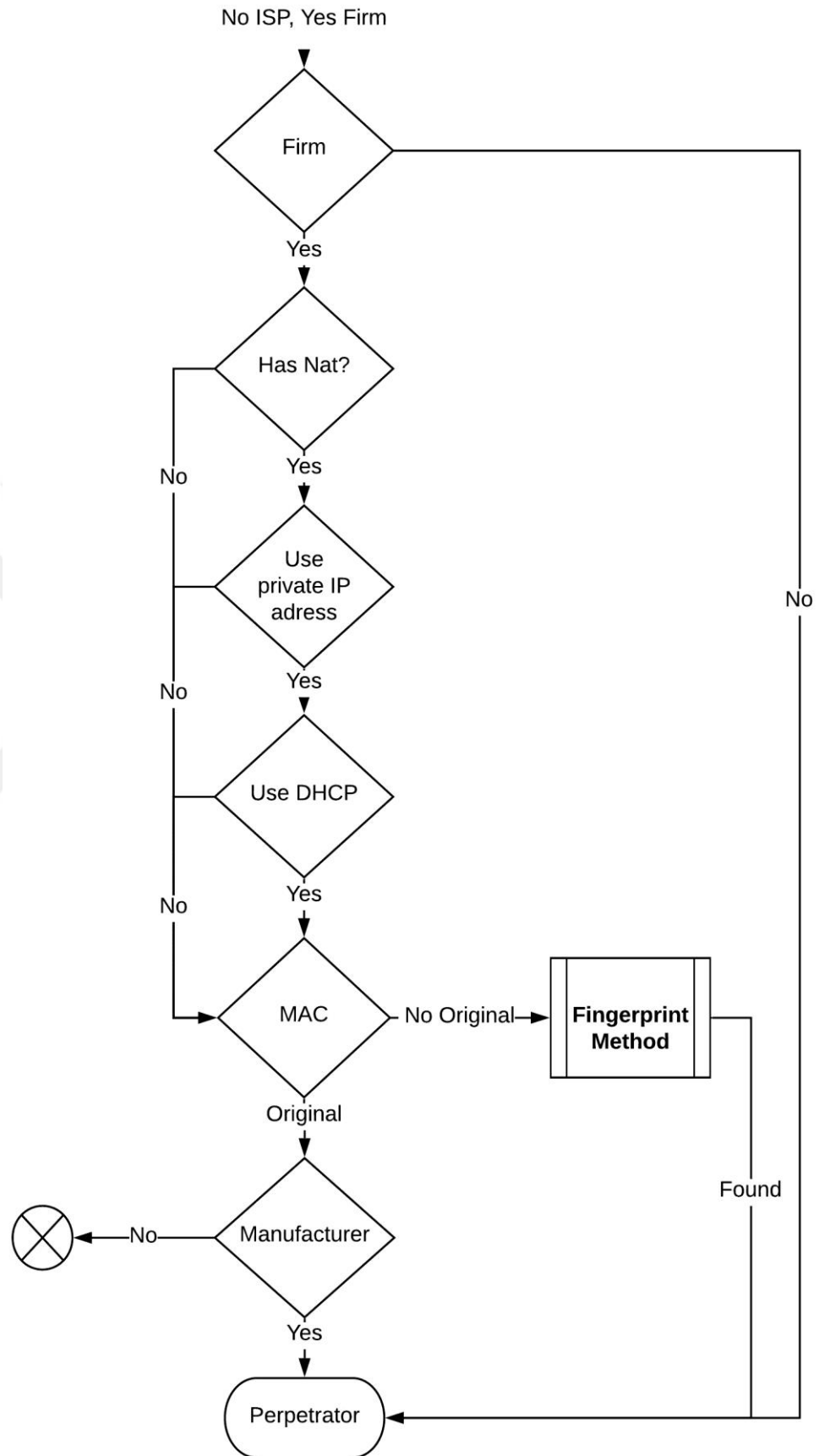


Figure 6.12 “Firm Process” in e-mail framework

6.2.2 Detecting a person who commit a crime with web

The web process is somehow similar to the process carried out for emails (Figure 6.13). But there are some important tips to consider. When these details are taken into consideration during the evidence stage, it will be easy to reach the conclusion. For a crime committed through a web site, it should not specify the address of the site “www.ayse.com.tr”, but the “http://www.ayse.com.tr” URL address indicating where the news is published. In the case of offenses committed through social media, the content entered by the user must have at least date information.

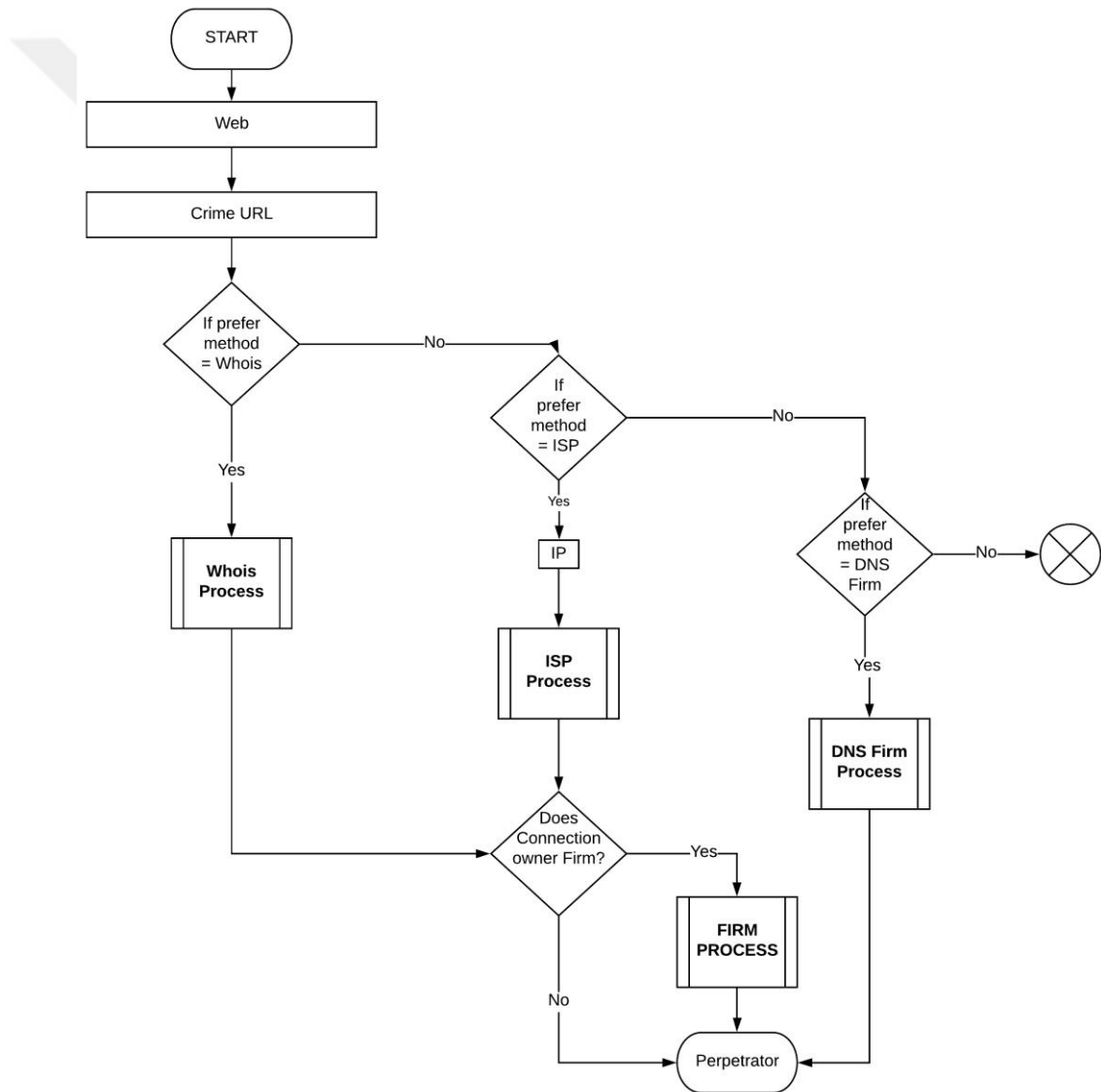


Figure 6.13 Framework for identifying an offender by web

There should be a time stamp indicating that certain data existed at that time in case the content of the crime was removed from the publication. This can prevent loss of evidence. Seizure provisions can be applied in crimes committed on the computer. In case of important crimes, if a complaint is made, it is important to make backup and to obtain hash value. Because numerical evidence from technological devices is difficult to obtain.

In this case, it becomes difficult to enlighten the crimes of informatics. Therefore, in our law, computers, computer programs, search, copy and seizure are also regulated.

In addition, another method is to obtain information from the company of the e-mail address used by the perpetrator. If it is possible to obtain crime date and time information from companies, it is easy to reach the perpetrator from the IP address like Figure 6.14. This information can be requested from e-mail companies. But the same problems are likely for email companies as described in their social media accounts.

The screenshot shows the 'GeoIP2 Precision Service Demo' web application. The browser address bar displays 'https://www.maxmind.com/en/geoip2-precision-demo'. The page features a navigation bar with links for PRODUCTS, SUPPORT, DEVELOPERS, COMPANY, and BLOG. The main content area is titled 'GeoIP2 Precision Service Demo' and includes a sidebar with links for 'GeoIP2 Precision Services' (Country, City, Insights, Free Trial Account) and 'GeoIP2 Databases' (Country, City, City Database by Continent, ISP, Domain Name, Connection Type, GeoLite2 Commercial Redistribution). The main search area is labeled 'IP Addresses' and contains a text input field with the IP '176.33.23.1'. Below the input field is a 'Submit' button. The search results are displayed under the heading 'GeoIP2 Precision: City Results' in a table format.

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	M C
176.33.23.1	TR	Izmir, Izmir, Turkey, Asia	35280	38.4067, 27.14	20	Superonline ADSL	Superonline ADSL	superonline.net	

Below the table, a note states: 'ISP and Organization data is included with the purchase of the GeoIP2 ISP database or with the purchase of the GeoIP2 Precision City or Insights services.'

Figure 6.14 Example of questioning in which city IP is located

To determine the perpetrator's e-mail account information from official branch in Turkey is still not difficult. But by the judicial authorities to the branch, writing said the company is providing information to the Turkey branch demand a warrant and specifying the time of the crime date, that date to this e-mail address may be asked providing connections from any IP address and can be detected in this way IP address.

The user's mail account may not always be obtained from the IP number. In these cases, it is more appropriate to contact DNS registrator firm (Figure 6.15). "I forgot my password" section can be learned even. The next steps can be taken by taking the perpetrator.

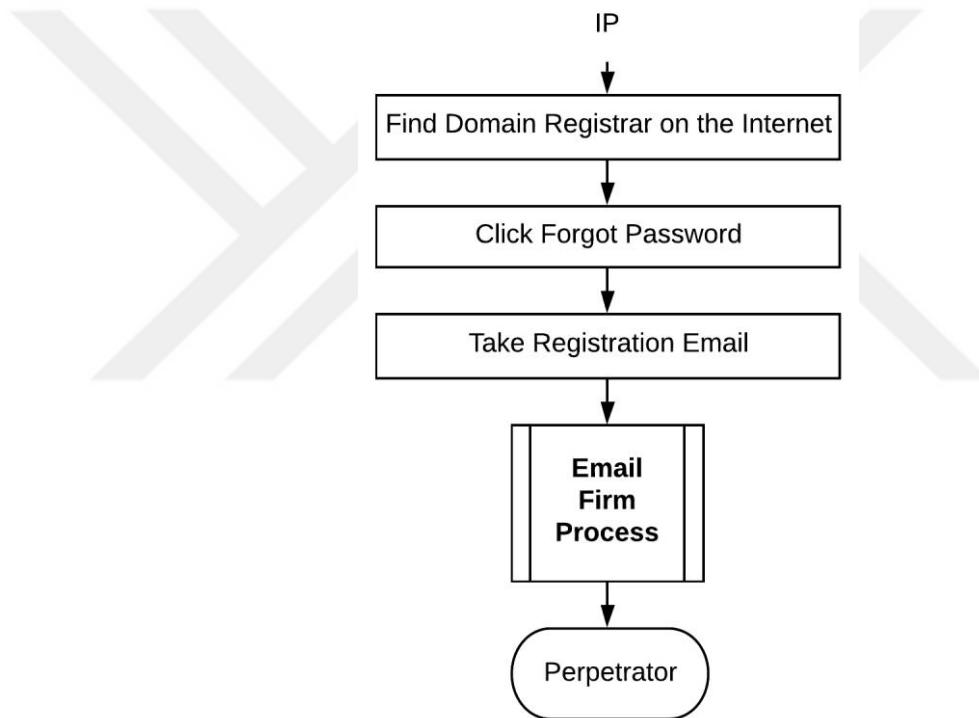


Figure 6.15 “DNS Firm Process” in web framework

If the perpetrator cannot be reached from here, it is also possible to identify the person who committed the crime with any e-mail account over the internet connection of the mass-use provider by investigating which IPs previously entered the same e-mail account. These browsers can be done by fingerprint method. The most practical and simple method used by the security units is now the Fingerprint method (Figure 6.16). Fingerprint is a method available in recent time browsers. Since the browser is installed on the device, an id belongs to this browser and following this id, the

monitoring of criminals has become quite easy. Since the awareness of this method is not yet widespread, the offenders do not take the necessary measures. This method can be explained as follows. The offense should be open in different accounts than the browser. These accounts can be identified and the person's identity can be reached.

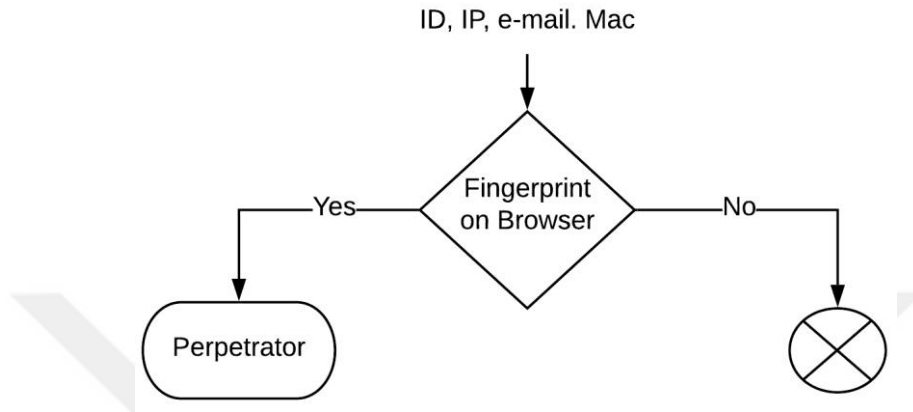


Figure 6.16 “FingerPrint Method” in web framework

6.2.3 Detecting A Person Who Insults on Social Media

Today, one of the most common crimes is insulting through social media. It is more difficult to determine the true identity of the perpetrators of insult crimes committed by users of Instagram, Twitter, Facebook and social media than websites. This is because an account can be opened with false names or an account can be opened using incorrect information. Since these social media companies are located in the US, the IP information of the perpetrators can only be obtained by contacting their headquarters in the USA. However, there is a problem with companies headquartered in the United States. Among the countries that will be requested information with Turkey, it requires a bilateral agreement for legal assistance. However, the crime investigated here should also be defined as a crime in the laws of the country where information is sought. At this point the problem arises. Because, in our country, the verb as “insult”, in many cases is not a crime in the United States. When companies request information about the offense, they are rejected.

However, the perpetrators' IP information can be obtained from the headquarters of these companies in cases of threat, harassment and child pornography, which are defined as crimes in both countries. In this way, the culprit can be detected.

People who publish their credentials are frequently seen in social media such as Instagram, Twitter and Facebook. Therefore, the priority is to use this path if it is possible to reach the result through the user's personal profile. However, it is not always known whether the personal username is the actual identity of the person. Because social media users often don't use their real credentials. In this case, the most practical way is to search for the person from Google to get social media information. As a matter of fact, social media users often use their account information in connection with each other. The real identity of the person can be determined in this way. If people can be identified through social media profiles, this can be taken, but if there is no result, it will be necessary to request IP information from corporate headquarters in the USA.

Wolfram Alpha has an answering engine which can be used as a social media verification tool and it can be used as social media analysis. Wolfram Alpha is asked a question. Wolfram Alpha researches its own database and brings certain results to the question. Wolfram Alpha is a mathematical and knowledge-based systematic search engine. Uses Mathematica computer program which is used in departments such as scientific, engineering and mathematical fields. The user must ask appropriate questions to verify their contents. The source can be learned by asking the question who uploaded the content. Exif information can be accessed whenever the content is generated.

Another method used by the security units may be fishing offenders (Figure 6.17). The attacker sends the username and password wants as correct and incorrect. It is made entering the correct information for safety. It is prevented to log in to the system by sending the wrong information. The attacker who sees that he is unable to login becomes panic and tries to enter the system with his own account. In this way, the offender is determined by learning own account.

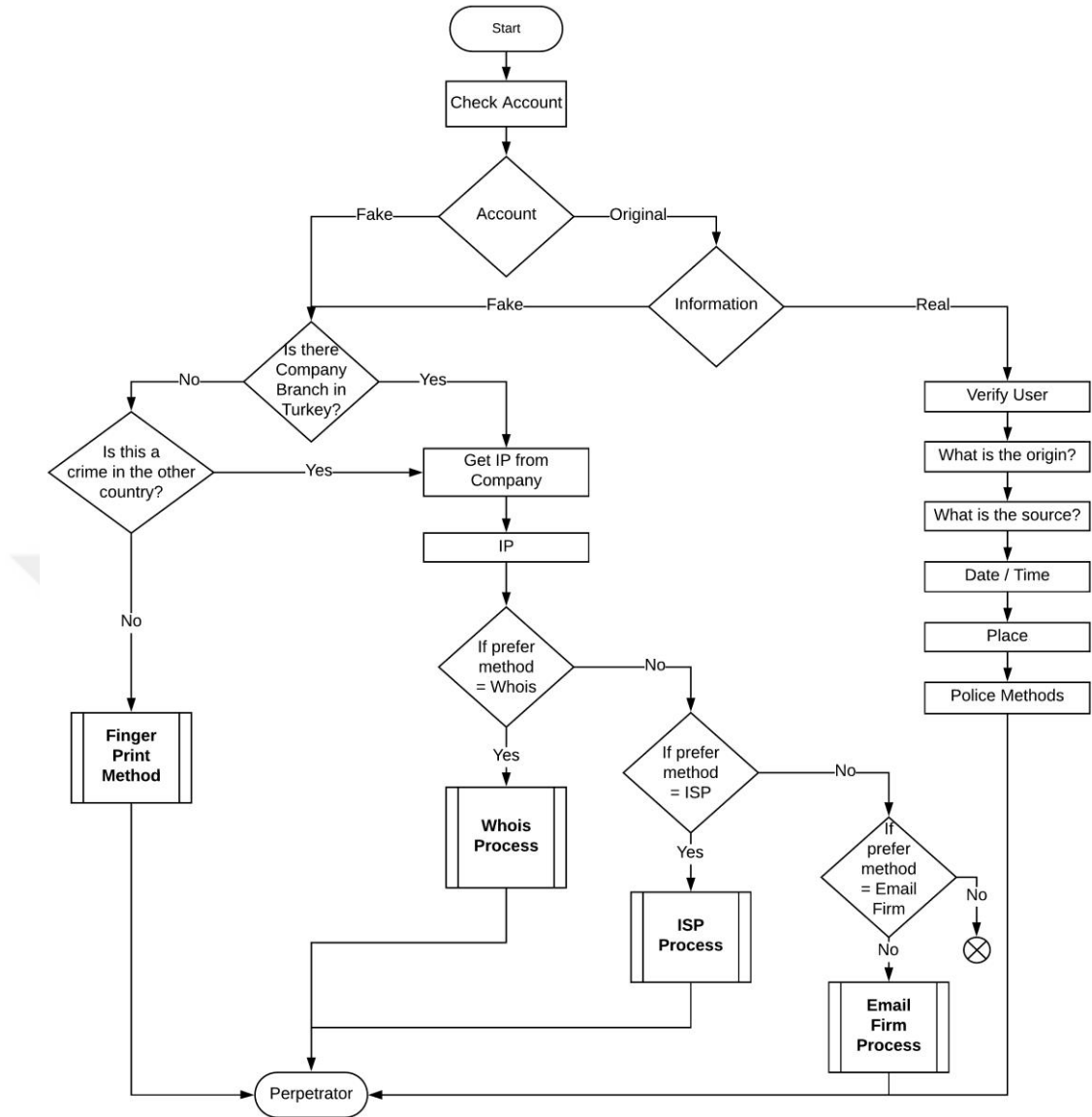


Figure 6.17 Social media framework

6.2.4 Detecting Man in the Middle Attacker

In different LAN networks, if the necessary security measures are not taken; with some simple operations, it can be included in the network of wireless access points such as access point. In this way, the desired users can be monitored. Even the control panel can be seized. In particular, it is easier to steal data from sites that do not use https instead of https. In a local network system, sniffing is performed on the computers by third parties using related applications. In the network, the desired user on the web sites entered, username, password information, accounts entered sites can

be seized. The attacker can obtain the username and password information if they are not encrypted. When this is considered to be the case, law enforcement officers want to be burned by this aggressor, they often use the Wireshark or Cain & Able program to listen to the victim computers (Figure 6.18, Figure 6.19). Detection of Man in the Middle attack with ARP Poisoning can be found by examining data packets via ARP filter with Wireshark program. If the Wireshark output obtained during the attack is examined, it is seen that the gateway is in contact with all ports. Generally, the attacker's IP is also in contact with the victim's IP. When this contact is examined, it is seen that the victim's data is directed to the attacker's IP address. The computer name and MAC address of the attacker's IP number detected on the local network from another computer on the network is detected using this program. ARP filtering can be used to detect the attacker over the IP number. The username of the detected IP number is determined by determining the computer name.

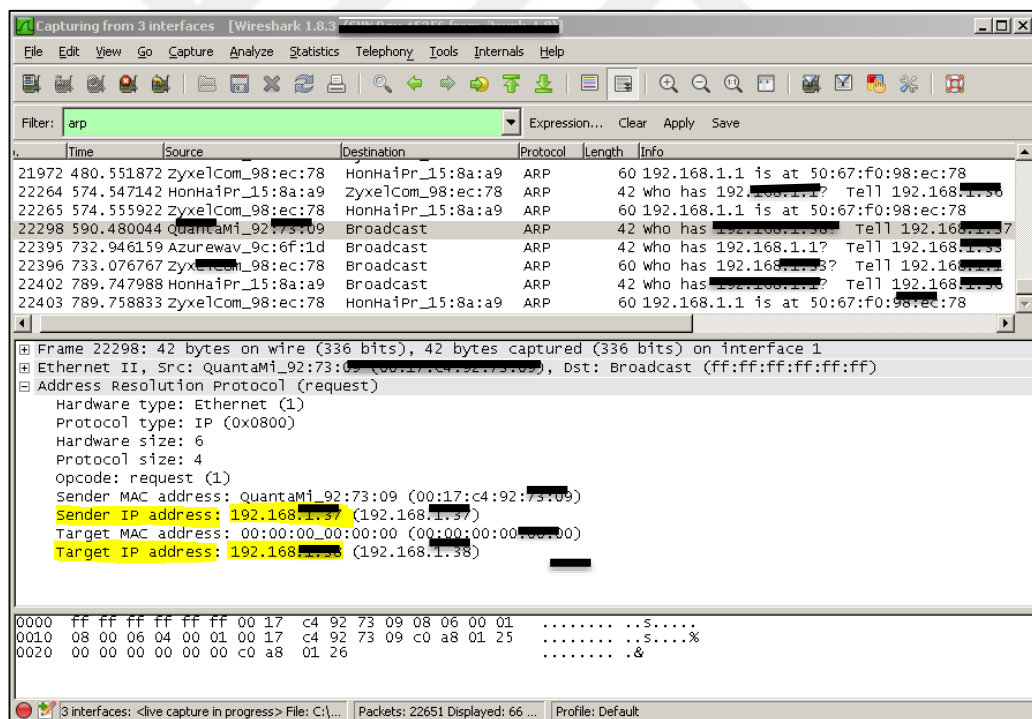


Figure 6.18 Detecting the attacker's IP address with Wireshark

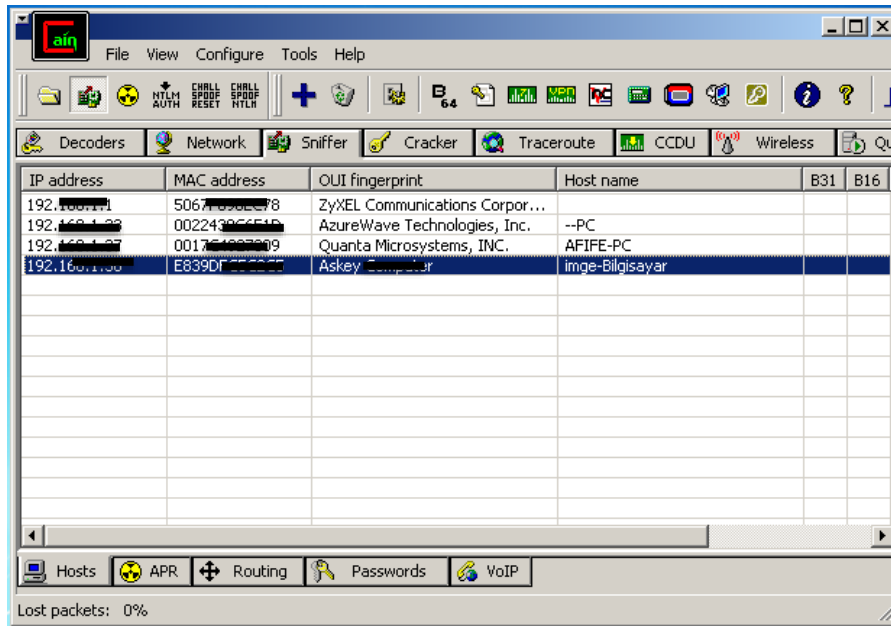


Figure 6.19 Detecting the attacker's computer name with Cain & Abel

Criminals determine their victims according to some criteria (Figure 6.20). Their priority is that wireless network users have not set a password. It is also aimed at users who do not use VPN, which means Virtual Private Network. Because VPN allows to connect to the internet through another IP address. VPN secures the connection and encrypts the connection when connecting to any network. It also encrypts all received data itself, sent to the VPN system. For this reason, criminals do not target encrypted and VPN users on the network. They start to follow the posts of the people they follow. They capture packets sent. As a result, some internet interruptions may occur. Often in such cases the victim understands that he is facing an attack. The client actually logs in to the website on the server, and only sends the data to the attacker in the middle. Some important steps must be taken to identify the offender.

First of all, it should be looked at the firewall logs. For example, the firewall may have switched the relevant hours. If important logs cannot be retrieved from this step, IPS logs should be checked. In these logs, the movements of the firewall are observed. For example, if the MAC duo of the Firewall changes, IPS may intervene and block the IP address of the Firewall. Because it is responsible for reporting machines that are included in the network.

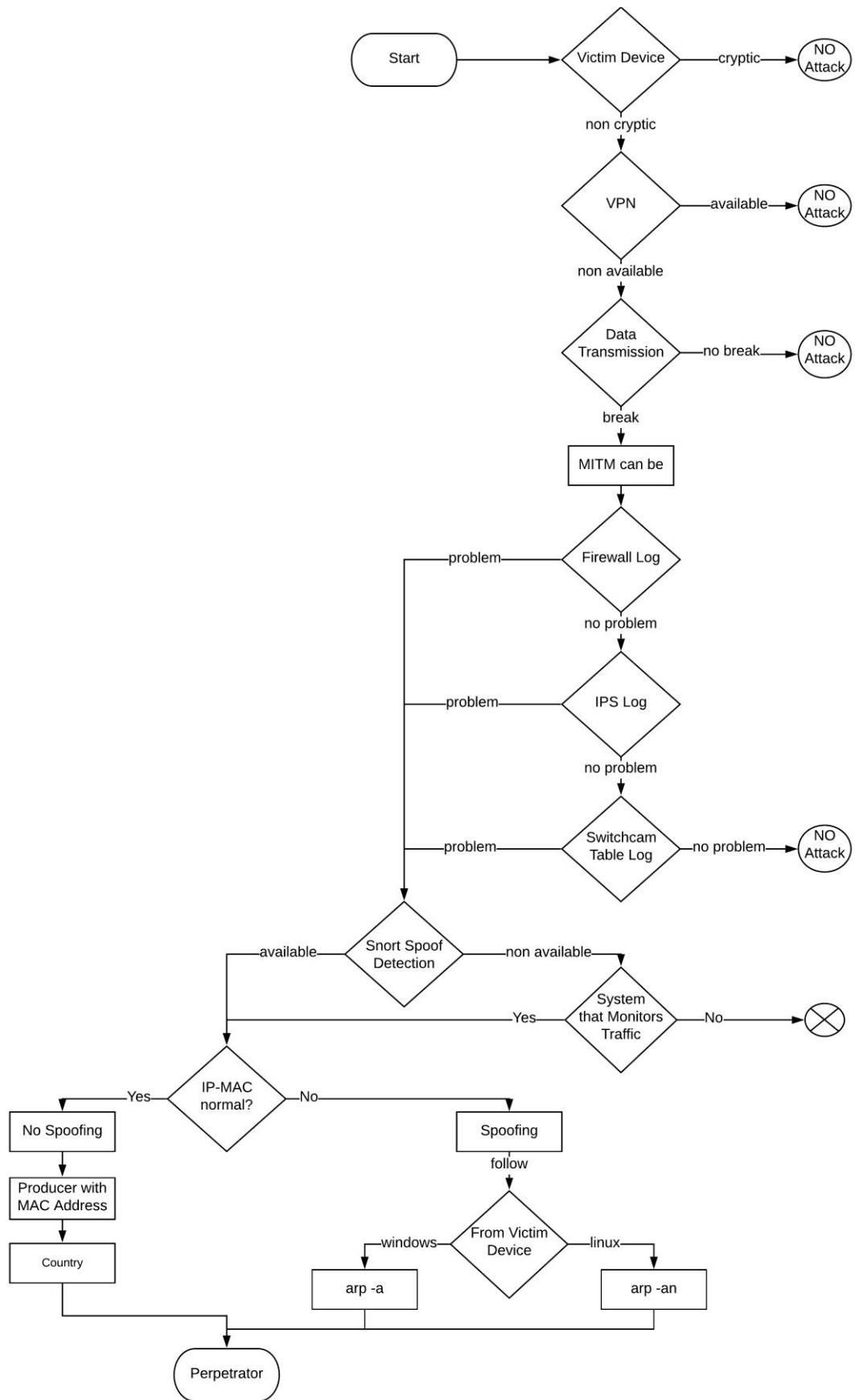


Figure 6.20 MITM framework

The IP and MAC duo have the ability to report changing systems. The logs of the Switch CAM tables are used to capture ARP Spoofer's (Figure 6.21). If these logs cannot be provided, another monitoring device may be examined. If an IP address appears with more than one MAC address, ARP Cache Poisoning or ARP Spoofing is performed. Or, if an IP address appears when it appears with another MAC address, it is ARP Cache Poisoning or ARP Spoofing. Then the false MAC address is detected. Which of these differences is determined by the original IP or MAC. The attacker is detected by the manufacturer or by Whois queries (Figure 6.22).

```

C:\Users\ayseo>arp -a

Interface: 192.168.1.1 --- 0x4
Internet Address      Physical Address      Type
192.168.1.1           ec-23-3d-d4-58-7a    dynamic
192.168.1.2           60-31-3b-13-f2-b4    dynamic
192.168.1.3           ff-ff-ff-ff-ff-ff    static
224.0.0.1             01-00-5e-00-00-02    static
224.0.0.2             01-00-5e-00-00-16    static
224.0.0.3             01-00-5e-00-00-fb    static
224.0.0.4             01-00-5e-00-00-fc    static
239.255.255.255       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\ayseo>

```

Figure 6.21 Monitoring the MAC address of a system in communication

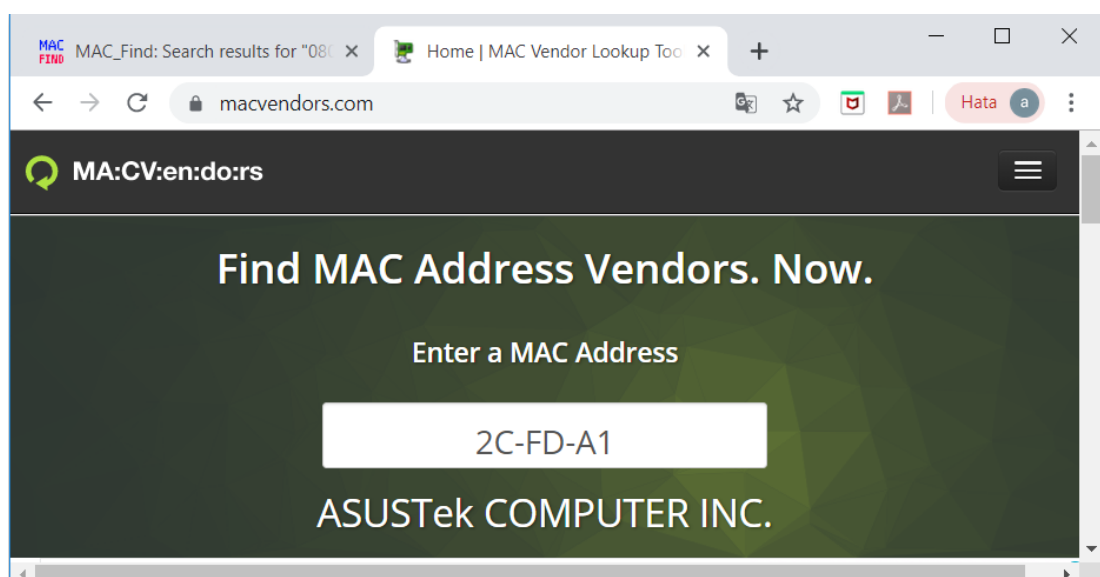


Figure 6.22 Finding a manufacturer with MAC address

6.2.5 Detecting Ransomware Attacker

For ransomware attack, download games from the Torrent, provide remote desktop access, or use social media; provides the environment for the encryption software to infiltrate the device. But my most preferred site is usually emailing. Using the phishing method, the e-mail is shown as a document from the official institution. To do this, it is prepared with special designs to attract the victim's attention or to scare the victim. The email attachment contains malware. The aim is to enable the user to activate the .exe extension malicious software in the email attachment. As soon as the user executes this file, the malware starts to be active on the target system and settles on the bottom layer of the system and encrypts the file. When it was clicked, it reached its goals. The malware that is activated on the target system first copies itself into the "C:/Windows/" directory with random names. It generates a key entry in the system's registry to be automatically activated each time the system is turned on. The malware then encrypts all the files in the target. The accused encrypts the device in two ways.

First, the software that reaches the device encrypts the data. After encrypting the files on the target system, the user sends a message informing them that the files are encrypted, and for the decryption of the passwords, a ransom is requested. Virtual money is generally preferred.

The second is worse. They make passwords. They also have the information on the device. If they do, they threaten to share data. Mostly ransomware attacks are mostly successful. They are also very difficult to catch. It is also very difficult to open encrypted computers. Some studies can be done by losing the information. In this way, the perpetrator of the crime can be reached.

The ransom software uses encryption methods such as a 256-bit standard algorithm in the AES (Advanced Encryption Standard) encryption method. In order to get rid of ransomware threats and develop an effective fight against this software, the threat must be defined in detail.

In Figure 6.23, for fixing procedures, some analysis methods should be used. First, static analysis should be performed without running malware. Behavioral movements (file-directory movements) should then be monitored by running malware in a controlled environment with dynamic analysis. Finally, code analysis should be performed to analyze the architecture of the malware. Control of the malware on the victim computer (live system) is difficult. In general, the examination is not performed so that the damage does not reach larger dimensions. Therefore, it is necessary to take copies of the victim computer and continue the analysis on different computers.

The computer that was subjected to ransomware attack is copied with FTK Imager program. The device under investigation must be run in virtual machine mode, as the ransomware being reviewed will attack user data quickly after execution. The characteristic behavior analysis of the ransomware can be analyzed by FTK. There is no standard for malware analysis. But generally, all information that can be obtained without running malicious software is reached, and then the malicious software is run in a controlled environment after the behavioral movements are examined, the code architecture of the malicious software is examined.

It is necessary to obtain information about the victim computer by using FTK or Process Explorer programs. The total capacity of the device, the total number of sectors, MD5 and SHA1 value and MD5 Verification and SHA1 Deliver values are required like Table 6.1. It is also necessary to collect information about the product's operating system name, username, system root, current version, CSD version, installation date and last shutdown date through these programs like Table 6.2.

Table 6.1 Device information description

Total Capacity	1.000.204.886.016 Bytes (931,5 GB)
Total Sector	1.953.525.168
MD5 Value	5ebd653ee347d236356914371e8c6174
MD5 Verification	5ebd653ee347d236356914371e8c6174
SHA1 Value	6f316c8a661fd83a6ee04caggb87d1a3c715ab0
SHA1 Verification	6f316c8a661fd83a6ee04caggb87d1a3c715ab0

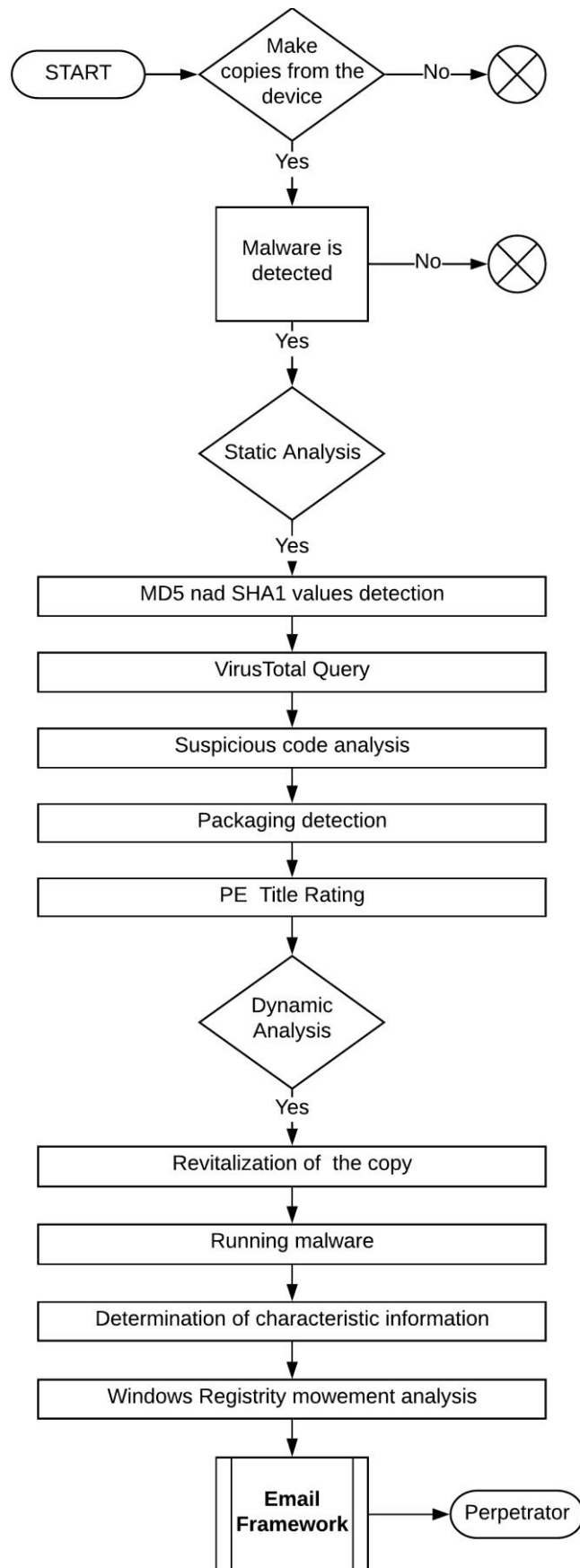


Figure 6.23 Ransomware framework

Table 6.2 Operating system information product name

Name of the product	Windows 7 Ultimate
Registered Owner	user
System Root System Root	C:\Windows\
Current Version	6.1
CSD Version	Service Pack 1
Installation Date	19.01.2019 11:55:39 UTC
Last Closed Date	16.08.2019 10:57:10 UTC

Based on this information, relevant versions and features of the programs to be used for analysis are selected. In addition, the information obtained from the malicious software to predict the possible character movements. In the next stage, dynamic analysis is performed. When the copy taken for dynamic analysis is run, the attacker's message is seen on the screen of the victim computer like Figure 6.24. From the message, the cause of the attack is understood, ransom software is detected. The first trace of the ransomware, which is activated in the target system, is usually foreign files under the respective directory. After this step, the examinations are carried out on the files found here like Table 6.3.

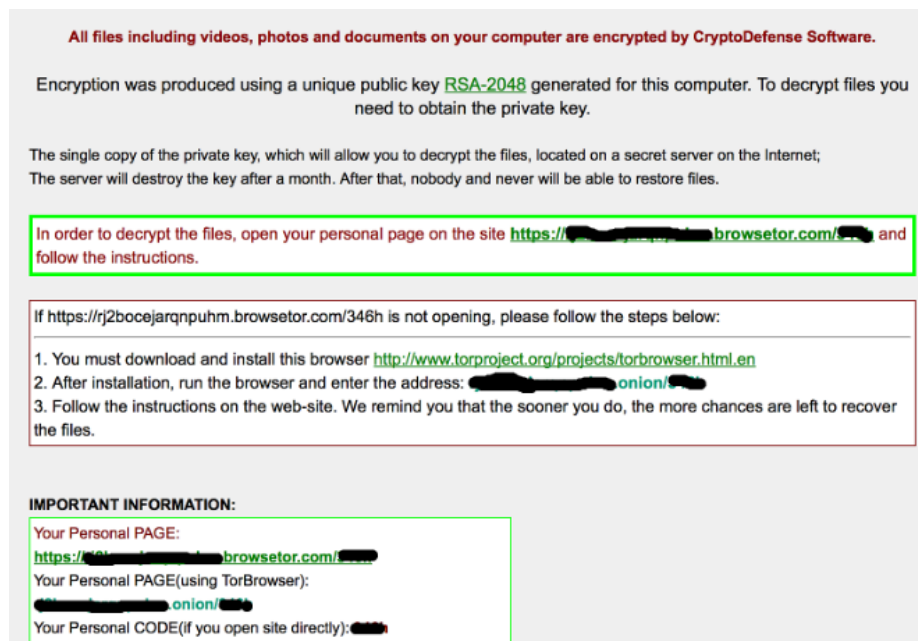
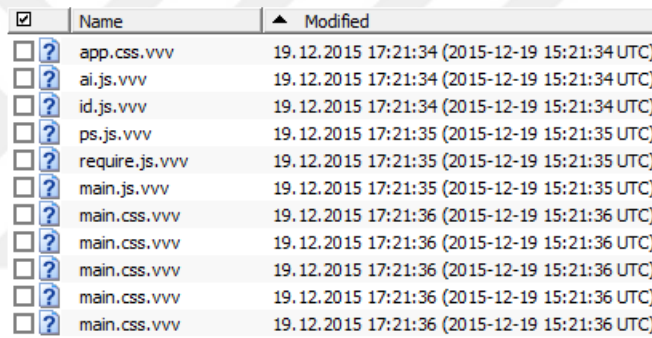


Figure 6.24 An example of an attacker's message on the computer with virus

Table 6.3 Technical information of the offender file obtained by FTK.

File name	Howto_Restore_FILES.HTM
Creation Time	10.08.2019 13:57:55 (2019-08-10 11:57:55 UTC)
Access Time	10.08.2019 13:57:55 (2019-08-10 11:57:55 UTC)
Replacement Time	10.08.2019 13:57:55 (2019-08-10 11:57:55 UTC)
File Size (Bytes)	10.631 bytes (10,38 KB)
MD5 Hash Value	38e36d32d8e26e44415437c4492d6207
File Path	IMAGE.E01/Partition2/NONAME [VSC]/[Current]/[root]/Users/user/Desktop/

In the examinations made on the copy file encryption operations start date is determined. Inspections are performed on files that run on that date. The .exe file that is run from the date of the event is searched like Figure 6.25.



☒	Name	Modified
☐ ?	app.css.vvv	19.12.2015 17:21:34 (2015-12-19 15:21:34 UTC)
☐ ?	ai.js.vvv	19.12.2015 17:21:34 (2015-12-19 15:21:34 UTC)
☐ ?	id.js.vvv	19.12.2015 17:21:34 (2015-12-19 15:21:34 UTC)
☐ ?	ps.js.vvv	19.12.2015 17:21:35 (2015-12-19 15:21:35 UTC)
☐ ?	require.js.vvv	19.12.2015 17:21:35 (2015-12-19 15:21:35 UTC)
☐ ?	main.js.vvv	19.12.2015 17:21:35 (2015-12-19 15:21:35 UTC)
☐ ?	main.css.vvv	19.12.2015 17:21:36 (2015-12-19 15:21:36 UTC)
☐ ?	main.css.vvv	19.12.2015 17:21:36 (2015-12-19 15:21:36 UTC)
☐ ?	main.css.vvv	19.12.2015 17:21:36 (2015-12-19 15:21:36 UTC)
☐ ?	main.css.vvv	19.12.2015 17:21:36 (2015-12-19 15:21:36 UTC)
☐ ?	main.css.vvv	19.12.2015 17:21:36 (2015-12-19 15:21:36 UTC)

Figure 6.25 Example that files on the victim computer are encrypted

It is determined what kind of ransomware application .exe is found. The held registry log is examined. The activity of this exe is determined. The types of malware detected should be investigated. Often this malware encrypt files and then destroy themselves. After this stage, research should be carried out to recover the encrypted files caused by the ransomware. The brute-force method can be used to crack a password, but it may not provide a solution for powerful software. Using the word list method, which contains the passwords of the ransomed solutions, is successful in some cases. There are programs like “AccessData Registry Viewer” to recover encrypted files. AccessData Registry Viewer is a program developed by AccessData for the windows operating system and is associated with FTK program in Figure 6.26. As a result of the analysis made with the prepared word list successfully recovered encrypted files.

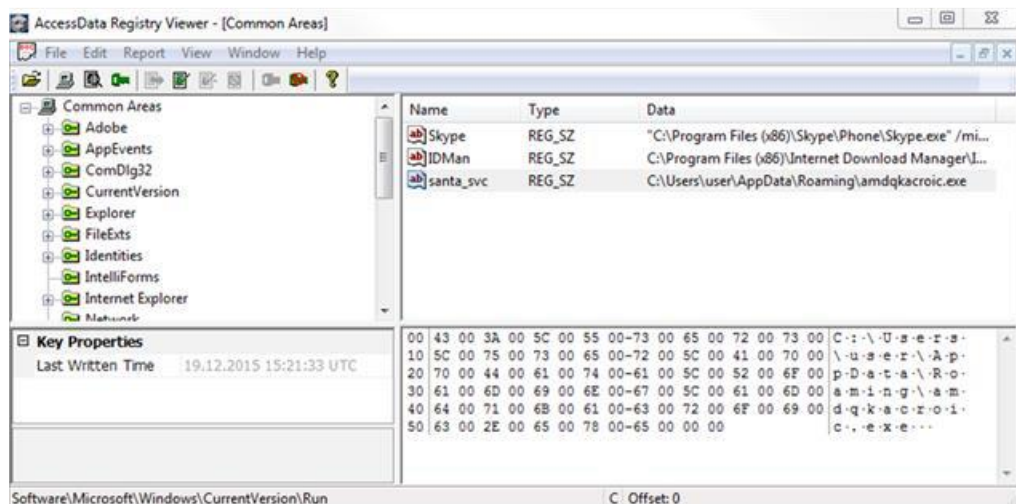


Figure 6.26 Example of running malicious software “amdqkacroic.exe”

VirusTotal is a URL and file review service. Web sites that are suspected to be suspicious or harmful will scan the files for free and analyze them. Detects all malicious software such as Virus, Worm, Trojan like Figure 6.27. VirusTotal uses multiple different antivirus services when analyzing and scanning the URL or Files submit to analyze, so it is much easier to identify malicious files. The frequencies are updated as antivirus solutions in VirusTotal are developed and distributed by virus protection companies.

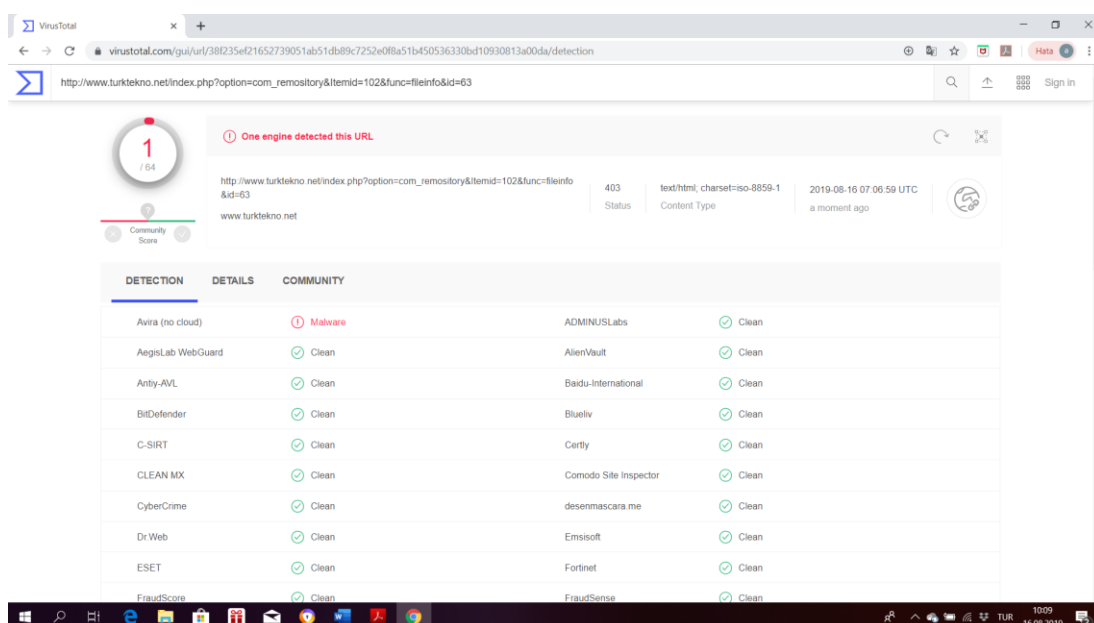


Figure 6.27 Screenshot of a virus-detected site in VirusTotal

6.2.6 Detecting DDoS Attacker

DDoS attacks are attacks that make any system inoperable. This type of attack is usually done using thousands of different computers and sends more traffic than the capacity of the target system can handle (Figure 6.28).

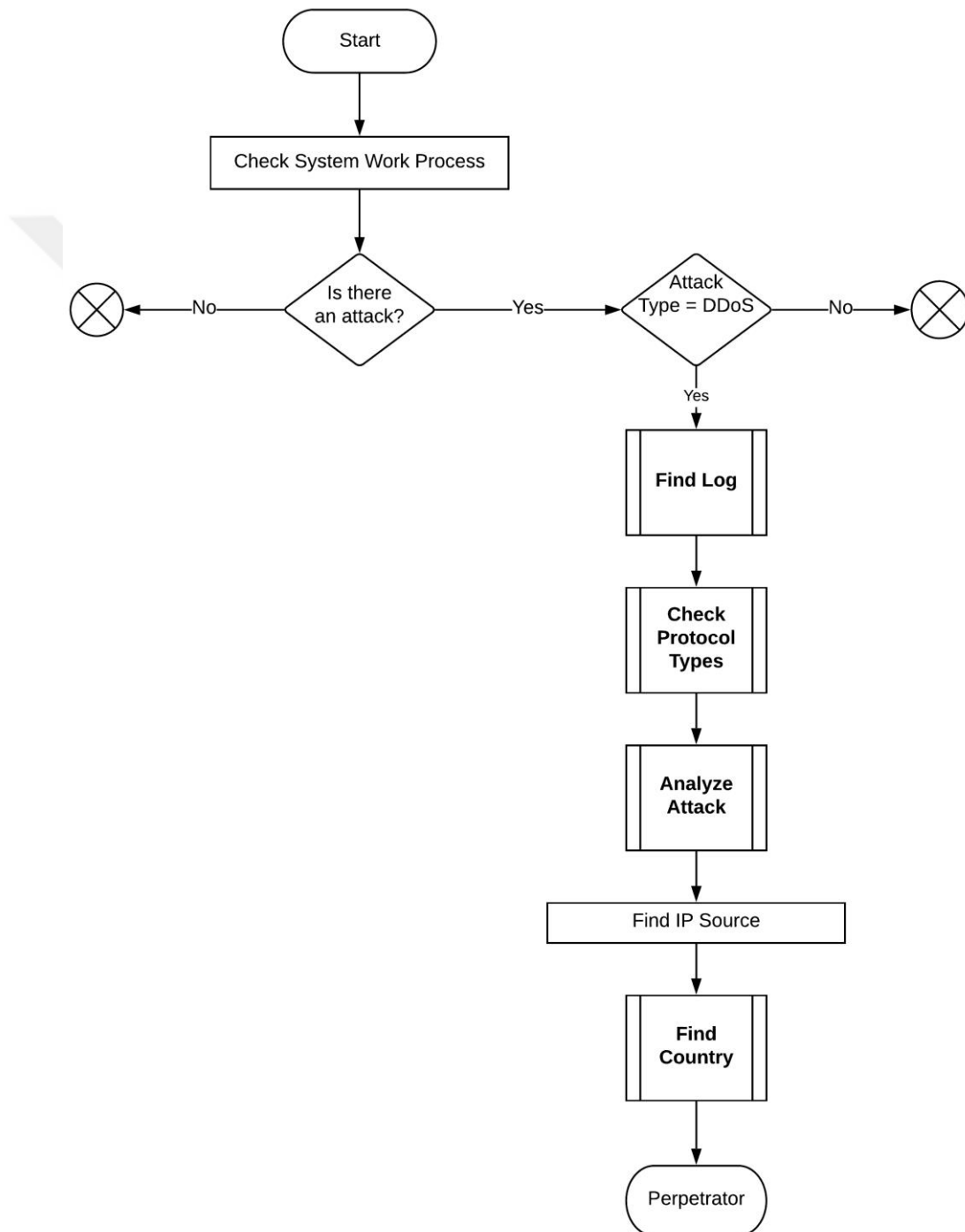


Figure 6.28 Framework for identifying an offender by DDoS

An attack may occur if the system does not turn on or does not work. Some tools (tcpdump, wireshark) are used to determine the type of attack. There are two important situations for DDoS attacks. Preventing the attack and identifying who did it. Because, if the follow-up is not done after the attack, it is normal to encounter the same situation. For this, packets must be recorded at the time of the attack. Packet registration can be done via the TAP port on the target system (Figure 6.29).

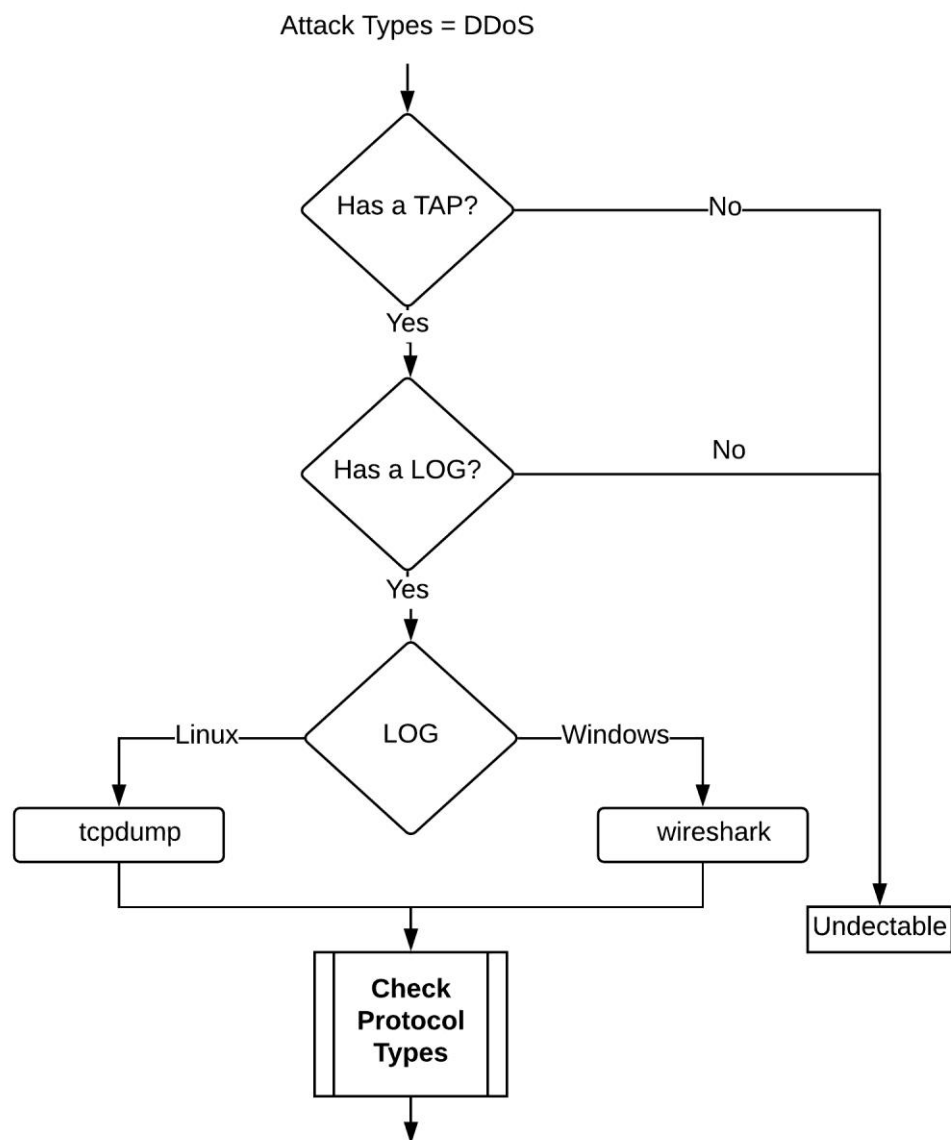


Figure 6.29 “Find Log” part in DDoS framework

Windows devices can be registered with Wireshark application and Linux devices can be registered with tcpdump. For this, after Linux computers become root;

“tcpdump -n -w ddostest1.pcap” the package record is created by running the command.

The recorded packages should be reviewed later. TCP, UDP, ICMP protocols have been used to decide which attack has been conducted. For this to be detected; # **“tcpdstat -n ddos.pcap”** command should be run (Figure 6.30). This command will provide information about the type of DDoS attack. Because it is said which protocol is used and at what rate. The high rate protocol reveals the type of attack. Also, “netstat -n” when is looked at the command with a lot of waiting time and the same IP continues to be said that the UDP attack. At the same time, the CPU, RAM and network usage of the server increases considerably when there is a UDP attack.

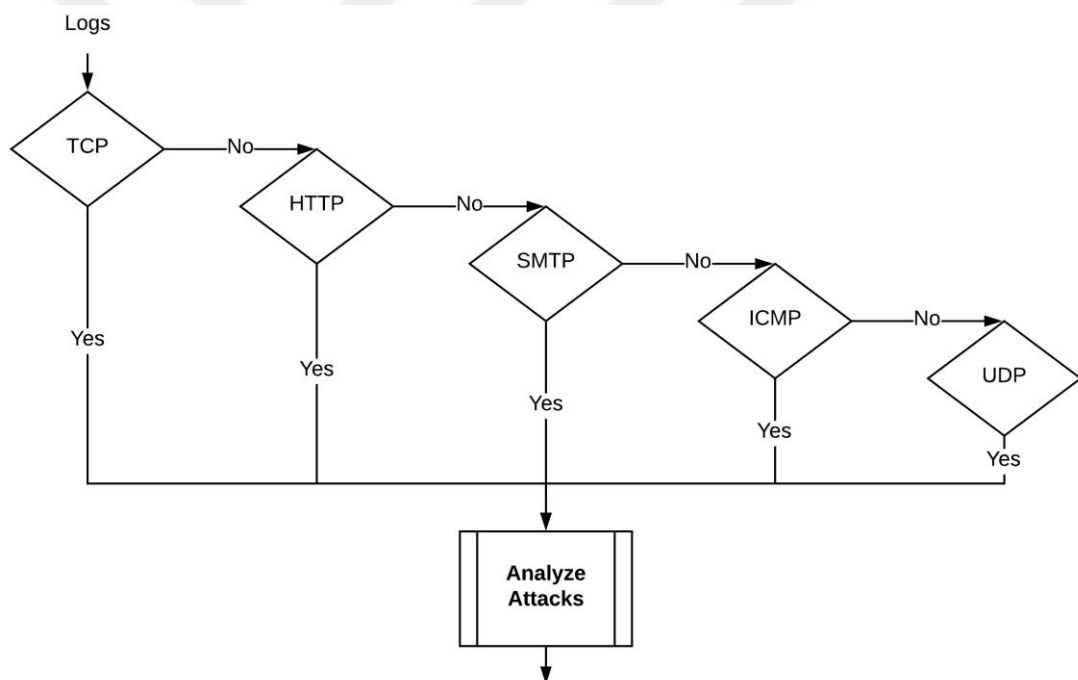


Figure 6.30 “Check Protocol Types” part in DDoS framework

The next step is to find the attack method. Attack methods, mainly; SYN Flood, HTTP GET Flood, ACK Flood, FIN Flood, UDP Flood, DNS Flood (Figure 6.31, Figure 6.32 and Figure 6.33). There are some commands to determine which of these methods are used. If the result of these commands is null, it means no attack. But if there is value like 2-7-87-876 next to the IPs, there is an attack. The higher the number, the greater the severity of this attack.

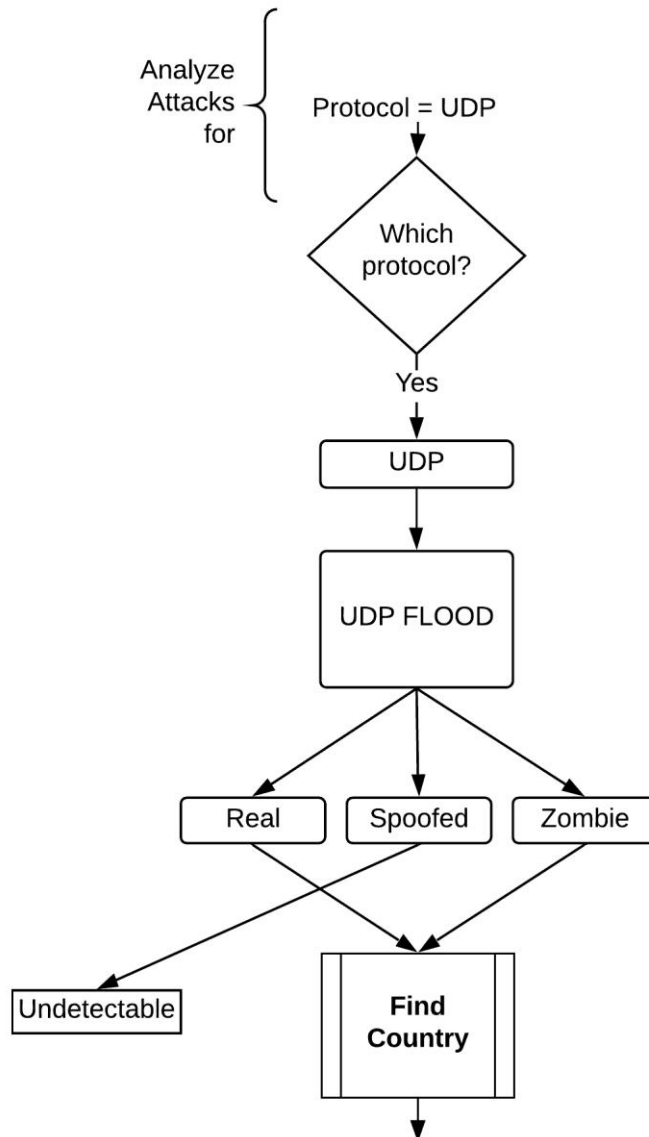


Figure 6.31 “UDP” part for analyze attacks in DDoS framework

Using this commander, the attack tube is detected. HTTP GET Flood contains exception. Because of the triple handshake procedure, which is a feature of the TCP

protocol, the attack with the original IP always occurs. And this is provided by TCP. A similar situation applies to UDP. UDP Flood occurs only with UDP.

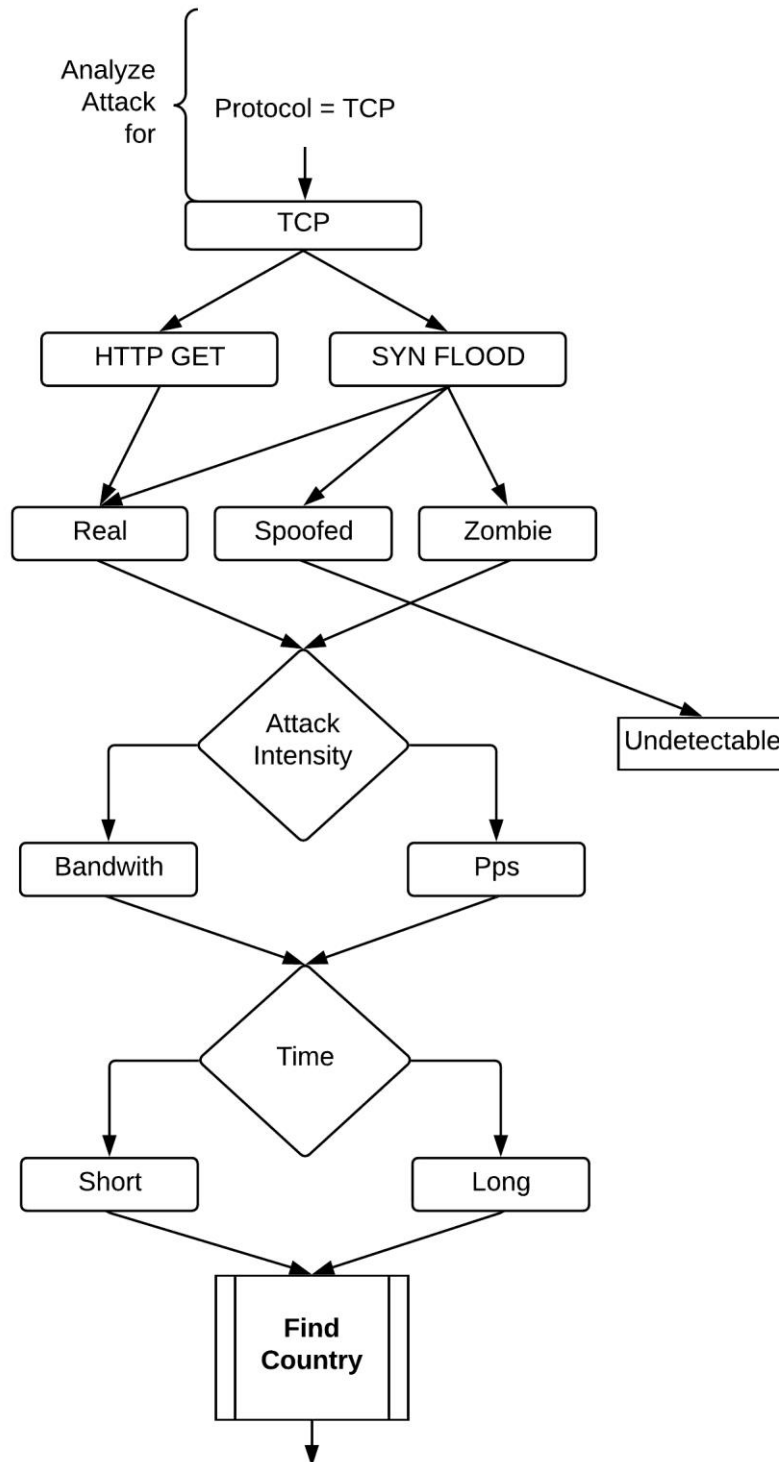


Figure 6.32 “TCP” part for analyze attacks in DDoS framework

The severity of the attack should be examined. The severity of the attack is examined in two groups. The amount of bandwidth the incoming traffic is spent and the “Packet Per Second” value of the incoming traffic. The tcpstat tool is also used to detect the severity of the attack.



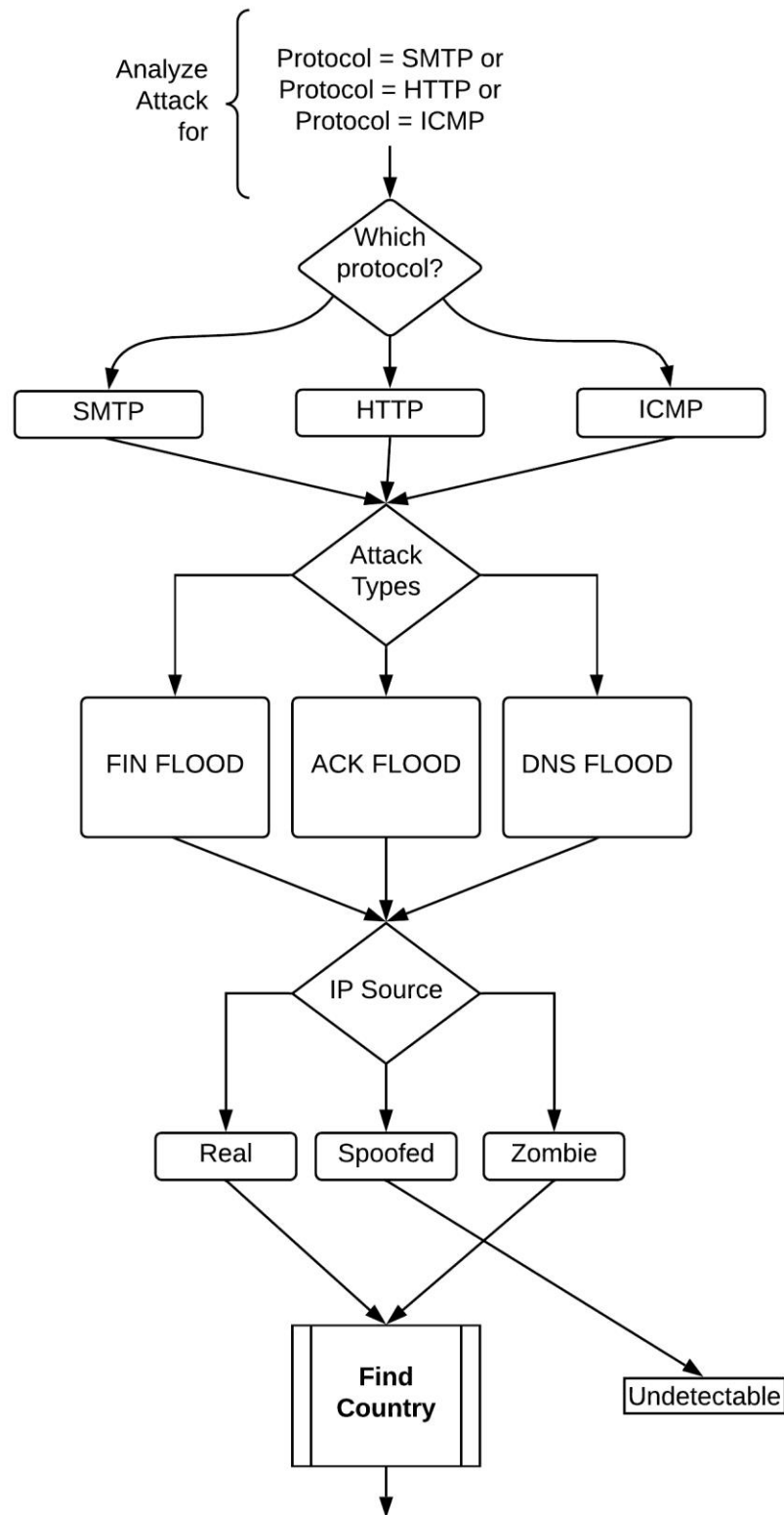


Figure 6.33 “SMTP, HHTTP, ICMP” part for analyze attacks in DDoS framework

The most important step in detecting the criminal in DDoS attacks is to identify the source of the attack. The source of the attack can be difficult to identify. Because IP

spoofing is done with resources or botnet to attack with zombie systems. Attack analysis can determine whether the IP addresses used are real or not. If the file recorded during the attack was examined, the attack was spoofed. If more than one connection is established with the same IP, it is the original IP. If attacks are carried out with the original IP and botnets, the country of attack can be detected (Figure 6.34). By following these steps, the perpetrator can be identified over IP.

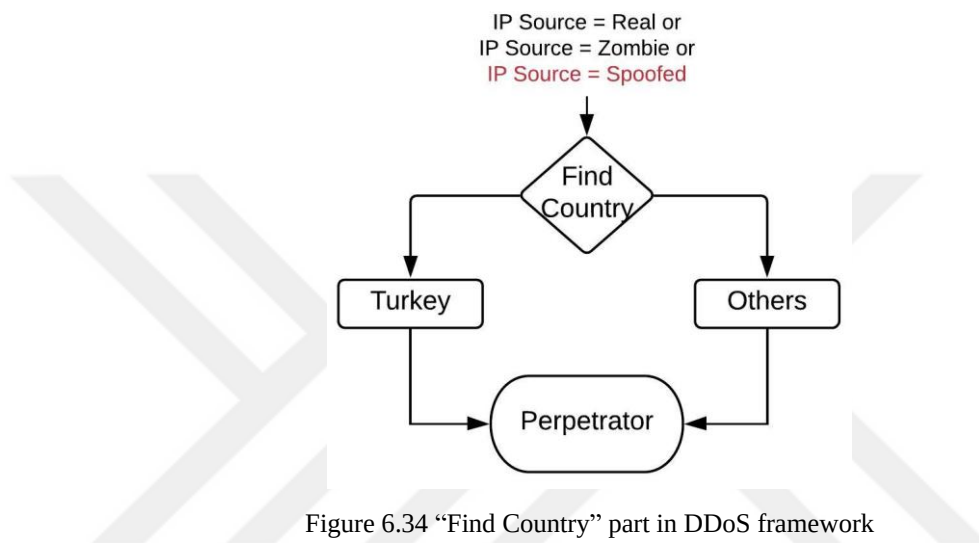


Figure 6.34 “Find Country” part in DDoS framework

6.3 Training Recommendations for Those Who Fight Cybercrime

Research in the process of creating this framework shows that there is an urgent need to perceive the information security roles required by today, to train the personnel with the necessary knowledge and skills and to increase the capabilities of conscious people. Although our security devices, security architectures and cyber-defense tactics are considered to overcome many threats, their defense and detection capabilities; it is often inadequate against customized and combined threats. The best defense against such threats is; to form a knowledgeable, skilled and skilled workforce in a methodological way and to use this team's capabilities again methodologically. (to train qualified personnel) In the field of cyber security, the missing personnel needs to be met. Field and job based training services should be provided in order to train and strengthen the cyber security workforce. Brand / product independent technology trainings should be given in order to train and strengthen the cyber security workforce

of organizations. The trainings should be aimed at raising the awareness of the participants, teaching the basics of security and providing technical knowledge in the most important areas of information security.

Education in Forensic Information: The training, recruitment and the skills of the existing personnel should be increased. The latest technologies, product updates and global trends in the forensic information sector should be communicated to the staff. The trainings to be taken should be as follows

Forensic Informatics Expertise Training: Forensic IT staff, especially law enforcement personnel or forensic investigators, to determine the use of information systems in crime by means of hardware and software used in forensic informatics field, to obtain evidence from information systems, to obtain evidence from information systems. training should be provided.

First Response to Digital Evidence Training: The collection, seizure and packaging of the digital evidence detected at the scene. Hardware and software (including open source programs) used in the field of Computer and mobile forensics should be applied during image acquisition training of volatile evidences and hard disks and portable memories.

Computer Forensics Training: Forensic informatics, training should be provided to use hardware and software systems that enable the acquisition and examination of images of computer and data storage units.

RAM Review: To obtain RAM image in an open computer system with licensed programs or open source programs, licensed and open source programs of a RAM image prepared as an example within the scope of the scenario should be examined.

Malicious Software Forensic Analysis: Cyberattack or malicious software by sending financial companies, especially to damage computer systems, personal or financial data produced and distributed in order to protect against malicious software

such as viruses and Malware to be taken to protect against malicious software and to determine the working systems.

Mobile Forensics Training: Training for the use of hardware and software systems that enable the acquisition and examination of the image of mobile systems within the scope of forensic computing.

Windows Forensics Training: Forensics is a computer forensics program forensic analysis of Windows operating systems, files and data from how and how to collect and report the training is explained.

Linux Forensics Training: This is a forensic analysis of Linux operating systems using computer forensics programs, and how and how to collect and report evidence from files and data.

MacOS Forensics Training: Forensic analysis of MacOS operating systems by using Computer Forensics Programs, is a training on how and how to collect and report evidence from files and data.

Network Forensics Training: It is the training to control the network traffic, capture and examine the packets over the network with the network systems used by the public institutions and private companies that exchange information over the network.

Computer and Data Security Training: It is the practical training that is used to ensure the security of the computers and data used in companies with personal computer usage, measures that can be taken against harmful software, and the systems used to ensure the security of data stored in the computer environment.

Video and Image Enhancement Training: Training of making images obtained from security cameras or other systems that cannot be fully understood due to the

quality of the images. Attack Techniques Training, DDOS Attacks and Protection Methods Training

Network Forensic Analysis Training: There are trainings on attack techniques and protection methods, network forensic analysis. Through these trainings, it is necessary to learn the weaknesses of information technologies and to gain competence in methods of protection against Dos DDoS attacks.

Penetration Testing Training: Penetration testing provides information and competence on the technical and administrative processes of penetration testing. Cyber Incidents Response Team Installation and Management Training, Information Systems, Forensic Analysis Training, Secure Configuration Audit Training: Cyber events and response team installation and management, information systems forensic analysis, IT configuration training should be done. These trainings should provide the ability to control the basic configuration methods and secure configuration settings of information security devices.

Intrusion Detection and Record Management Training, Central Security Monitoring & Incident Management Training: Training on log analysis and intrusion detection should be provided. These trainings should provide the necessary knowledge and skills to make corporate records management more efficient and effective intrusion detection.

Computer Forensic Analysis & In-depth Windows Training, Malware Analysis Methods Training: There are trainings on computer forensic analysis and malware analysis methods. Thanks to these trainings.

Enterprise management of information security; all these items should be implemented by the management as an “Information Security Policy”. User responsibilities should be expressed in this policy. The duties of IT staff should also be included in the policy. User awareness studies should be repeated regularly. The Internal Audit Unit should regularly monitor the implementation. It is important to

avoid legal gaps in information and computer security. However, due to the rapidly changing nature of the subject, whether the current situation in information and computer security is legally relevant, it should be continuously monitored by the authorized persons and the necessary arrangements should be reviewed and updated.

Advances in information and communication technologies, increasing use of the Internet, and changes in products and services in financial markets have made intermediary institutions information-based organizations. Working in a reliable environment by intermediary institutions is one of the necessary conditions to ensure stability in the capital market. In the absence of this condition, the owners of the savings may be harmed, the confidence in the capital market may be shaken and the intermediation process between the financial sector and the real sector may be impaired by decreasing the saving rate. Therefore, the operational risks arising from information systems of intermediary institutions operating as a trust institution in the capital market need to be managed.

The intermediary institutions should complete the controls related to information systems, establish effective systems and put these issues in writing both during the establishment phase and in carrying out their activities. One of the most important processes of corporate governance is IT Governance and IT management should be established to support business objectives. Thanks to the intermediary institutions where risks arising from information systems are managed, confidence in the capital markets will increase and speed, confidentiality, continuity, integrity, traceability can be added to the processes.

IT professionals should work more on the technical aspects of crimes and in particular produce programs that can be used to collect, protect, recover, analyze, verify and present digital evidence and provide technical support to relevant departments.

In universities, centers, working groups, departments, specialization trainings should be opened on subjects such as cybercrime, forensic informatics and the latest

developments in the scientific field should be followed, studies on cybercrime within the country should be initiated and standard procedures should be set.

The state should organize all the work done, support the relevant employees in the country financially and morally, and commissions should be established to enact appropriate laws. In addition, a central unit should be established to ensure the coordination of crimes. With cyber security technologies, public and financial institutions with critical technology infrastructure and sensitive data should be provided services in the field of customized technology solutions, cyber security services and application development. Experienced trainers and public personnel should be provided with network and communication systems, data center solutions, intrusion simulations and vulnerability detection, malware detection and analysis, cyber threat intelligence and strategic cyber security training.

6.4 Legal Requirements in the Fight Against Cybercrime

In this framework, it was concluded that some regulations are needed in the field of law as well as those that need to be developed in the technical field. Deficiencies in the field of law should be eliminated. International regulations are required. The issue of digital signature, digital identity and evidence of digital data should be regulated. Data Protection (Data Protection) arrangements should be made. Taxation of electronic commerce should be regulated and standardized. New types of crime should be identified and necessary legal arrangements should be made.

It is necessary to expand the scope of crimes committed through social media. With the developing technology, different fields of activity have emerged in the field of informatics. Social media is undoubtedly one of the effective means of reflecting this field of activity on our daily lives. Social media is a part of our social life. It has been the opportunity to reflect almost any kind of personal information and social life to social media by creating written and visual data. Having this opportunity is the usual result of being a part of the modern global world. Undoubtedly, all of these opportunities can include elements that may lead to material / moral losses, personal attacks and victimization of individuals and society. Informatics offenses and social

media offenses, which can be examined as a sub-branch, are among the problems that need to be clarified. For these problems, both the individual and the state should take some precautions and these measures should be reinforced with the laws to be enacted.

Also taken a number of measures in the context of our own domestic law and domestic law are in the top in the hierarchy of norms in the Constitution of the Republic of Turkey is located 'privacy and the protection of private life,' 'the necessity given the location. The constitution was not satisfied with the protection of international treaties, and the protection of the international community was extended to the scope of these protections and thus gained a global character. Council of Europe Convention on Cybercrime is one of the most important international agreements in our law. The European Cyber Crime Convention, which was signed by our country on 10.11.2010, was approved by the Law una Approving the Approval of the Crimes Committed in Virtual Environment dated 22.4.2014 and numbered 6533 and was published in the Official Gazette dated 2.5.2014 and numbered 28988. With this agreement, new articles have been added to the domestic law and studies have been carried out in order to ensure the effectiveness of this agreement. Another point to be mentioned in this context is Art. 90, paragraph 5 of the Constitution. According to this International treaties put into force according to the procedure are in the provision of the law. They cannot be applied to the Constitutional Court for alleged contradiction to the Constitution. (Additional sentence: 7.5.2004-5170 / 7 article) International treaties on fundamental rights and freedoms that have been put into force according to the procedure and the disputes that may arise due to the fact that the laws contain different provisions on the same subject shall be taken as basis.

The provisions of the Constitution and the Convention are very abstract provisions but will be put into effect by the provisions of the law and will become operational. In this direction, the TPC No. 5237 has tried to solve these problems and put forth the relevant provisions that include information crimes. In the TPC No. 5237, new types of crimes are regulated. Although these provisions are intended to prevent future grievances, their adequacy is controversial. These regulations narrowly regulated the scope of very comprehensive IT crimes. A commission was established by the

Ministry of Justice to deal with the subject of Informatics Crimes. Law no. 5661 The Turkish Criminal Code no. Because of this law, the TCK aims to accommodate unregulated elements, but the content of the law cannot meet this need.

For the reasons explained, new regulations should be made in the scope of meeting the needs by the individual law regarding very comprehensive information crimes. Or at least the part of the TPC concerning the crimes in the field of informatics should be rearranged within the scope that meets the needs. For example: “Personal Data has been tried to be defined by the prevailing views in the doctrine and explanations in the grounds of the article. However, within the scope of the TPC, data is not considered as movable property. So, the data will not be the subject of theft. According to TCK 141/1, the subject of theft should be a movable property. For this reason, “Data” and “Personal Data” should be defined in information crimes.

The scope of the provisions to be introduced should include explanations, regulations and sanctions that meet the information security needs of technological developments. In this respect, just as individuals should take measures for their privacy, the state should reinforce these measures by using its central authority. These measures should be deterrent and prevent any damages in case of interference. In this context, considering the prevalence of the impact of information crimes, the use of these information systems and tools should be regulated as a condition that increases the penalties in terms of crimes committed or may be committed through information systems and devices. The legislator has already foreseen this factor in terms of some offenses, but it does not have sufficient deterrence.

The concept of crime scene in forensic informatics is often not limited to the borders of the country. Before an operation launched from America to China, and then from there to South Korea and Sweden may at the end to Turkey. Therefore, even the best domestic legal regulations related to cybercrimes will often be insufficient. For this reason, international regulations, conventions and treaties should be made which contain more effective provisions, especially in the fields of detection, procurement, preservation and transfer of evidence related to cybercrimes. In fact, these international

regulations and conventions should include provisions that solve the problems that arise in cases where the act is considered a crime in one country and not a crime in the other country and meets the needs.

Finally, despite some deficiencies in our legislation, there are provisions on information technologies, but even these provisions have not been effectively implemented. It is therefore important to avoid legal gaps in information and computer security. However, due to the rapidly changing nature of the issue, it is more important whether the current situation in information and computer security meets the legal framework and should be continuously monitored by trained and equipped authorized persons and the necessary revisions and revisions should be made more quickly. Computer-related crimes, forensics and computer security are the main pillars of informatics. Law enforcement officers, prosecutors and judges should be familiar with these three areas. Lawyers should educate themselves on information technology crimes, especially digital evidence, and be able to punish them fairly and effectively. Non-governmental organizations should work on informational crimes and especially critical issues such as child pornography and inform our people more. The media can educate our citizens by creating programs on cybercrimes, ways to protect them and what can be done during the crime.

CHAPTER SEVEN

CONCLUSION AND FUTURE WORK

7.1 Conclusion

Informatics crimes that have been investigated so far have been tried to be conducted from a single point of view. Legal staff examined legal crimes, forensic IT experts forensic and IT experts examined IT crimes from a technical point of view. Even if all these examiners have achieved success in their fields, they cannot achieve full performance unless they are able to coordinate legal, technical and forensic informatics. For this reason, interruptions occur in the examination of different fields such as law, technology, security, risk and telecommunications chained together in the cyber world. This makes it difficult to identify the perpetrators and prolongs the process. In order to overcome these difficulties and determine the perpetrators in a short time, the processes in the cyber crime evaluation should be well documented and a road map should be developed considering the crime types.

In this study, the legal, technical and forensic informatics for cyber crimes were analyzed. But using the information obtained from different associations, six different crime types were selected, the procedures used for analyzing these crimes were defined frameworks were developed. The main contributions of this thesis can be given as follows:

- The types of information crimes are defined and the profile of IT criminals were examined. Information offenses were then categorized and information on the details of information offenses were given. Digital evidence and types of evidence have been announced. Then, the software and hardware tools used to obtain evidence were mentioned.
- Six different frameworks have been created for six different IT crimes known as web, e-mail, MITM attack, ransomware attack, DDoS (Distributed Denial of Service) attack, and social media insult crimes. These frameworks are designed to be understood by all experts in different fields and to ensure the

progress of legal processes. Since, these frameworks have visuality, they can be easily followed. From the moment the crime was detected, it was designed to be tracked step by step to identify the offender. This is of great benefit to law enforcement. It helps catch criminals faster. Provides information on how to obtain evidence to identify the perpetrator. Because the steps that followed the law enforcement to identify the perpetrator were announced.

- Move importance should be given to international treaties in terms of law applicability. Juridically, the most important result is that the existing system is not sufficient in the field of law and the laws need to be more specific.
- Training recommendations required by technical personnel to be successful in identifying the perpetrator were presented. Besides, the fields in which the persons defining IT offenders should be specialized, were described and the training types were suggested.

7.2 Future Work

In this thesis, six different types of crime have been investigated in order to detect information offenders. These types of crimes are crime committed via e-mail, crime committed via web, crime committed by social media, crime committed by ransom software, crime committed by man in the middle attack and DDoS attacks. In the future, additional frameworks can be created for existing crime types such as Worms, Trojan, KeyLogger, SQL Injection, Virtual Credit Card Theft and, Account Stealing. In this way, the actions to be taken in order to identify the perpetrator for each type of crime are determined and the result is reached in a short time. As requirements and expected results are clear, more stable and clear results are achieved in the detection processes.

REFERENCES

- Abdulai, M. A. (2016). *Determinants of fear of cybercrime victimisation: A study of credit/debit card fraud among students of the University of Saskatchewan*. MSc Thesis, University of Saskatchewan, Saskatchewan.
- Achille, M. M. (2012). Multi-perspective cybercrime investigation process modeling. In *International Journal of Applied Information Systems*, 2(2), 14-20.
- AccessData, (2019). Retrieved September 8, 2019 from <https://accessdata.com/>
- Ademu, I. O. (2013). *A comprehensive digital forensic investigation model and guidelines for establishing admissible digital evidence*. MPhil Thesis, University of East London Architecture Computing and Engineering, London.
- Akgün, Y. M. (2016). *Bilişim suçları ve IP delilinin yeterliliği*. Retrieved September 7, 2019 from <https://www.bahadirhan.com/adli-bilisim-dergisi-3-sayisi-yayinlandi/>
- Akyıldız, M. A. (2013). *Siber güvenlik açısından sızma testlerinin uygulamalar ile değerlendirilmesi*. MSc Thesis, Süleyman Demirel University, Isparta.
- Alaca, B. (2008). *Ülkemizde bilişim suçları ve internetin suça etkisi (Antropolojik ve hukuki boyutları ile)*. MSc Thesis, Ankara University, Ankara.
- Alkaabi, A., Mohay, G., McCullagh, A. & Chantler, N. (2010). Dealing with the problem of cybercrime. *Information Security Institute, Queensland University of Technology*, 1(18), 1867-8211.
- Altunok, E. & Vural, A. F. (2011). Bilişim suçları. *Denetim*, (8), 84-74.
- Ansar, M. (2016). *Kalıcı casus faaliyetleri ile mücadele*. Retrieved September 7, 2019 from <https://www.bahadirhan.com/adli-bilisim-dergisi-3-sayisi-yayinlandi/>

Ashcroft, J. (2011). *Electronic crime scene investigation: a guide for first responders*. Retrieved September 7, 2019 from <https://www.ncjrs.gov/pdffiles1/nij/187736.pdf>

Aslay, F. (2017). *Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi*. Retrieved September 7, 2019 from <https://dergipark.org.tr/download/article-file/375131>

Bariki, H., Hashmi, M. & Baggili I. (2010). Defining a standard for reporting digital evidence items in computer forensic tools. *Digital forensics and cyber crime*, 78-95.

Bielecki M. and Quirchmayr G. (2010). A prototype for support of computer forensic analysis combined with the expected knowledge level of an attacker to more efficiently achieve investigation results. *International Conference on Availability, Reliability and Security*, 696-701.

Bolat, Y. (2015). *Memory Forensics*. MPhil Thesis, İstanbul Bilgi University, İstanbul.

Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, 9(1), 55.

Cellebrite, (2019). Retrieved September 8, 2019, from <http://www.cellebrite.com/>

Cellebrite Analytics, (2019). Retrieved September 8, 2019, from <https://www.cellebrite.com/en/analytics/>

Cellebrite Reader, (2019). Retrieved September 8, 2019, from <https://www.cellebrite.com/en/cellebrite-reader/>

Central Management System, (2019). *Cellebrite*. Retrieved September 8, 2019, from <https://www.cellebrite.com/en/central-management-system/>

Ceza Muhakemesi Kanunu (No: 5271). Retrieved October 8, 2019, from <http://www.ceza-bb.adalet.gov.tr/mevzuat/5271.htm>

Chen W. & Liu C. (2010). The analysis and design of linux file system based on computer forensic. *International Conference on Computer Design and Applications*, (2), 2-60.

Ciampa, M. (2007). Security awareness: Applying practical security in your world. *Cengage learning* (2nd ed.). Boston: GEX.

Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, 3(1), 1-22.

Cole, E., Krutz, R., Conley, J., Reisman, B., Ruebush, M., Gollman, D., & Reese, R. (2007). *Wiley pathways network security fundamentals*. Retrieved September 6, 2019, from https://www.researchgate.net/publication/320613636_A_Proposal_to_Detect_Computer_Worms_Malicious_Codes_Using_Data_Mining_Classification_Algorithms

Çakmak, H. & Altunok, T., (2009). *Suç, terör ve savaş üçgeninde siber dünya* (137-162). Ankara: Barış Platin Kitabevi.

Çakmakaya & Akpınar (2018). Bilişim suçları ile mücadelede karşılaşılan sorunlar. *Balkan and Near Eastern Journal of Social Sciences*, 04 (03).

Çifci, H. (2012). *Her yönüyle siber savaş* (134-135). Ankara: Tübitak.

Dija S., Balan C., Anoop V. & Ramani B. (2011). Towards successful forensic recovery of bitlocked volumes. *6th International Conference on System of Systems Engineering*, 317-322.

- Dokurer, S. (2016). *Atık alanlar*. Retrieved September 5, 2019, from https://halilozturkci.com/pdf/adli_bilisim_dergisi_sayi_1.pdf
- Elektronik İmza Kanunu. (2014). *Resmi Gazete (No: 25355)*. Retrieved January 23, 2014, from <http://www.resmigazete.gov.tr/eskiler/2016/04/20160420-16.htm>
- Ercan, M. (2015). *Kritik altyapıların korunmasına ilişkin belirlenen siber güvenlik stratejileri*. MSc Thesis, Gebze Technical University, Gebze.
- Ermeydan, D. (2018). *Türk ceza kanunu'nda bilişim suçları*. MSc Thesis, Çağ University, Mersin.
- Fikir ve Sanat Eserleri Kanunu (No: 2393)*. Retrieved October 8, 2019, from <http://www.mevzuat.gov.tr/MevzuatMetin/1.3.5846.pdf>
- Flory, T. A. (2016). Digital forensics in law enforcement: A needs based analysis of Indiana agencies. *Journal of Digital Forensics, Security and Law*, 65-77.
- Forensic Computers, (2019). *Forensic workstations, hardware, and software, forensic computers*. Retrieved September 8, 2019, from <http://www.forensic-computers.com/>
- Frank Y.W. Law, Patrick P.F. Chan, S.M. Yiu, K.P. Chow, Michael Y.K. Kwan, Hayson K.S. Tse & Pierre K.Y. Lai (2011). Protecting digital data privacy in computer forensic examination, In *2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 1-6.
- Gao, Zhiqiang & Ansari, Nirwan (2005). Tracing cyber attacks from the practical perspective. *IEEE Communications Magazine*, 43(5), 123-131.
- Garfinkel, S. (2007). Anti-forensics: Techniques, detection and countermeasures. *2nd International Conference on I-warfare and Security*, 77-84.

- Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7, S64-S73.
- Gladyshev, Pavel & Almansoori A., (2010). Reliable acquisition of RAM dumps from intel-based Apple Mac computers over firewire. In *International Conference on Digital Forensics and Cyber Crime* (55-64). Berlin: Springer.
- Gönen, S., Ulus, H. İ. E. & Yılmaz N. (2016). Bilişim alanında işlenen suçlar üzerine bir inceleme. *Bilişim Teknolojileri Dergisi*, 9(3), 239-236.
- Gönenç, E., (2014). 5651 Sayılı internet kanunu'nda yapılan değişiklikler üzerine değerlendirme. Retrieved September 8, 2019, from https://www.dropbox.com/s/1ys9z7a0m6mt93u/adli_bilisim_derigisi_sayi_1.pdf?dl=1
- Grobler, C.P., Louwrens C.P., & Solms, S.H. (2010). A Multi-component view of digital forensics. In *2010 International Conference on Availability, Reliability and Security*, 647-652.
- Gündüz, M. Z. (2013). *Bilişim suçlarına yönelik IP tabanlı delil tespiti*. MSc Thesis, Fırat University, Elazığ.
- Güngör, M. (2015). *Ulusal bilgi güvenliği: Strateji ve kurumsal yapılanma*. MSc Thesis, Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı, Ankara.
- Hati, M., Goodison, S.E., Davis, R.C. & Jackson, B.A. (2016). Cyber crime: A threat to the nation and its awareness. *International Journal of Advanced Research in Computer and Communication Engineering* 5(7), 690-692.
- Hayes, B., Jeandesboz, J. & Ragazzi, F. (2015). *The law enforcement challenges of cybercrime: are we really playing catch-up?* (30-32). Brussels: European Parliament.

Hekim, H. & Başbüyük O., (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 135-158.

Koops, B. J. (2010). The internet and its opportunities for cybercrime. *Transnational Criminology Manual*, 744-745.

ICS, (2019). Retrieved September 8, 2019, from <http://www.ics-iq.com/>

İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınla yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun (No: 5651). Retrieved October 8, 2019, from <https://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm>

Husain, Mohammad Iftekhar, Baggili Ibrahim & Sridhar Ramalingam, (2010). A simple cost-effective framework for iPhone forensic analysis. In *International Conference on Digital Forensics and Cyber Crime*, 27-37

Jain, Dr. N., Bhanushali N., Gawade, S. & Jawale, G. (2016). Physical and cyber crime detection using digital forensic approach: a complete digital forensic tool. *International Journal of Advance Research, Ideas and Innovations in Technology*, 834-841.

Kaçakçılıkla Mücadele Kanunu (No: 25173). Retrieved October 8, 2019, from <http://www.mevzuat.gov.tr/MevzuatMetin/5.5.4926.pdf>

Kahved'zi'c, D. & Kechad T. (2016). Semantic modelling of digital forensic evidence. In *International Conference on Digital Forensics and Cyber Crime*, 149-156.

Kangogo, C. I. (2008). *Cybercrime in Kenya: myth or reality*. MPhil Thesis, University of Nairobi, Nairobi.

Karagülmez, A. (2009). *Bilişim Suçları ve Soruşturma, Kovuşturma Evreleri* (74-80). İstanbul: Seçkin Yayıncılık

- Kaur, M., Kaur, N. & Khurana, S. (2016). A literature review on cyber forensic and its analysis tools. *International Journal of Advanced Research in Computer and Communication Engineering*, 5(1), 23-28.
- Kirwan, D. (2017). *Cybercrime: An investigation of the attitudes and environmental factors that make people more willing to participate in online crime*. MSc Thesis, Dublin Institute of Technology, Dublin.
- Kuhl, M.E., Sudit, M., Kistner, J. & Costantini, K. (2007). Cyber attack modeling and simulation for network security analysis. In *Proceedings of the 39th Conference on Winter Simulation: 40 Years! The Best is Yet to Come*, 1180 -1188.
- LC Technology, (2019). *Int'l: recovery software & services*. Retrieved September 8, 2019, from <http://www.lc-tech.com/>
- Lechner, Zoe (2017). *Facing 21st century challenges: an assessment of the EU's security provisions in the light of increasing cybercrime*. Bachelor Thesis, University of Twente, Netherlands.
- Leukfeldt, E. R., Lavorgna A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, 23 (3), 287-3000.
- Lewis, J. (2011). Cyberwar thresholds and effects. *IEEE Security & Privacy*, 9(5), 23-29.
- Li, Xingan (2015). Regulation of cyber space: an analysis of chinese law on cyber crime. *International Journal of Cyber Criminology*, 9(2).
- Linux-dd, (2019). *Full metal backup using the dd command*. Retrieved September 8, 2019 from <https://www.linux.com/tutorials/full-metal-backup-using-dd-command/>

- Lipson, H. F. (2002). *Tracking and tracing cyber-attacks: technical challenges and global policy issues*. Retrieved September 6, 2019, from <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5831>
- Leukfeldt, R., Veenstra, S. & Stol, W. (2013). High volume, cybercrime and the organization of the police: the results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology*, 7(1), 1.
- Logicube, (2019). Retrieved September 8, 2019, from <http://www.logicube.com/>
- Mohammed, K. H., Mohammed, Y. D. & Solanke, A. A. (2019). Cybercrime and digital forensics: bridging the gap in legislation, investigation and prosecution of cybercrime in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*, 2(1), 56-63.
- Mohammed, K., Mohammed, Y. & Solanke, A. (2019). Cybercrime and digital forensics: bridging the gap in legislation, investigation and prosecution of cybercrime in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*, 2 (1), 56-63.
- Mugisha, D. (2015). *Role and impact of digital forensics in cyber crime investigations*. Msc Thesis, Gujurat Forensic Sciences University, Gujurat.
- Norden, S. (2013). *How the Internet has changed the face of crime*. MPhil Thesis, Florida Gulf Coast University, Florida.
- Nouh, M., Nurse, J. R. C. & Goldsmith, M. (2016). Towards designing a multipurpose cybercrime intelligence framework. In *2016 European Intelligence and Security Informatics Conference*, 60-67.

- Nouh, M., Nursey J. R.C., Webb H. & Goldsmith M. (2019). *Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement*. Retrieved September 7, 2019, from <https://kar.kent.ac.uk/71674/>
- Nurse, Jason R. C. & Bada, Maria, (2018/19). *The group element of cybercrime: Types, dynamics, and criminal operations*. Retrieved September 7, 2019, from <https://arxiv.org/pdf/1901.01914.pdf>
- Orakcı M., Kök İ. & Çakır H. (2016). Adli bilişim eğitiminin gereksinimi ve genel olarak değerlendirilmesi. *Bilişim Teknolojileri Dergisi*, 9 (2), 137.
- Orta, M. (2015). *Bilişim Suçlarında adli analiz*. MPhil Thesis, Selçuk University, Konya.
- Önok, Murat., (2013). Avrupa konseyi siber suç sözleşmesi ışığında siber suçlarla mücadelede uluslararası işbirliği. *Marmara Üniversitesi Hukuk Araştırmaları Dergisi*, 19(2), 1229-1270.
- Özüdoğru, U. (2011). *Siber suçlar ve mücadele yöntemleri dünya uygulamaları ve Türkiye için çözüm önerileri*. MSc Thesis, BTK, Ankara.
- Palmer, G. (2001). A road map for digital forensic research. *First digital forensic research workshop* (27-30). New York: Utica
- Paraben Corporation, (2019). *Forensic replicator download*. Retrieved September 8, 2019, from <https://www.paraben-forensics.com>
- Park, J., Kim, M., Noh, B. & Joshi, J. B. D. (2006). A similarity based technique for detecting malicious executable files for computer forensics. In *2006 International Conference on Information Reuse & Integration*, 188-193.

- Pavlik, K. (2017). Cybercrime, hacking, and legislation. *Journal of Cybersecurity Research*, 2 (1), 13-16.
- Payel, H. (2015). MD5 hash değerinin hukuken geçerliliği sorunu, *Adli Bilişim Dergisi*. Retrieved September 8, 2019, from http://www.halilozturkci.com/pdf/adli_bilisim_dergisi_sayi_1.pdf
- Peterson, J., Johnson, D., Sommers, I. & Baskin, D. (2012). Use of forensic science in investigating crimes of sexual violence: Contrasting its theoretical potential with empirical realities. *Violence Against Women*, 18 (2), 193-222.
- Pilli, Emmanuel S., Joshi R.C. and Niyogi, R. (2010). An IP traceback model for network forensics. In *International Conference on Digital Forensics and Cyber Crime*, 129-136.
- Polat, Ç. (2016). *Penetration tests and security solutions for corporate networks*. MSc Thesis, Dokuz Eylül University Graduate School of Natural and Applied Sciences, İzmir.
- Povar, Digambar & Bhadran V. K. (2011). Forensic data carving. In *International Conference on Digital Forensics and Cyber Crime*, 137-148.
- Product Updates, (2019). *Cellebrite*. Accessed September 8, 2019. <https://www.cellebrite.com/en/support/product-releases/>
- Products Services Training*, (2019). Retrieved September 8, 2019, from <http://www.digitalintelligence.com/>
- Raghavan, S. and Raghavan, S. V. (2013). A study of forensic & analysis tools. In *Eighth International Conference on Systematic Approaches to Digital Forensic Engineering*, 1-5.

- Rana, N., Sansanwal G., Khatter K. & Singh S. (2017). *Taxonomy of digital forensics: investigation tools and challenges*. Retrieved September 7, 2019, from <https://arxiv.org/abs/1709.06529>
- Reith, M., Carr, C., & Gunsch, G. (2011). *An examination of digital forensic models*. *International Journal of Digital Evidence*, 1(3), 1-12.
- ResGaz 3, (2012). *Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı*. Retrieved September 8, 2019, from <https://www.sibersan.com/ulusal-siber-guvenlik-stratejisi-ve-2013-2014-eylem-planı/>
- Rogers, M. & Siegfried, K. (2004). The future of computer forensics: A need analysis survey. *Computer and Security*. 23 (1), 12-16.
- Rogers, M. & Siegfried, K., (2012). Digital forensics and cyber crime. *4th International Conference, ICDF2C*, 114.
- Rowlingson, R. (2004). A ten step process for forensic readiness, *International Journal of Digital Evidence*, 2(3), 1-28.
- Schreier, F. (2015). *On cyberwarfare: DCAF horizons 2015 working paper*. Retrieved September 8, 2019, from <https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf>
- Sindhu, K. K. & Meshram, B. B. (2012). Digital forensics and cyber crime datamining. *Journal of Information Security*, 3 (03), 196-201.
- Software, G. (2019). *Most trusted endpoint detection & response solution*. Retrieved September 8, 2019, from <http://www.guidancesoftware.com/>

- Şenol M., (2016). Siber güçle caydırıcılık ama nasıl? *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2(2), 10-17.
- Singh, G., Eian, M., Willassen, S. Y., Mjølunes, Fr. S., Zhang, L., Zhou, Y. & Fan, J. (2014). The forensic analysis of encrypted truecrypt volumes. In *2014 IEEE International Conference on Progress in Informatics and Computing*, 405-409.
- Taşcı U. & Can A. (2015). Türkiye’de polisin siber suçlarla mücadele politikası. *Fırat University Journal of Social Science*, 25 (2), 229-248.
- Taşkın, Ş. C. (2009). Bilişim hukuku uluslararası uyumsuzluklar. *Türkiye Barolar Birliği Dergisi*, 85, 332-372.
- The Council of Europe*, (2001). Retrieved September 8, 2019, from <https://www.austria.org/the-council-of-europe>
- Trabelsi, Z., Al-Hemairy, M., Baggili, I., and Amin, S., (2010). Towards more secure biometric readers for effective digital forensic investigation. In *International Conference on Digital Forensics and Cyber Crime*, 65 - 77.
- Turhan, O. (2006). *Bilgisayar ağları ile ilgili suçlar*. MSc Thesis, Devlet planlama teşkilatı müsteşarlığı hukuk müşavirliği, Ankara.
- Tübitak*, (2013). Retrieved September 8, 2019, from <https://www.tubitak.gov.tr/tr/haber/siber-saldirilara-karsi-yerli-savunma-araci-gelistirildi>
- Türkay, Ş. (2013). Siber savaş hukuku ve uygulama sorunsalı. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 71(1), 1177-1227.
- Türkiye Cumhuriyeti Anayasası*, (2011). Retrieved October 8, 2019, from https://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf

Türk Ceza Kanunu, (2004). Retrieved October 8, 2019, from <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf>

UFED, (2016). *UFED 4PC*. Retrieved September 8, 2019, from <https://www.forensicmag.com/products/ufed-4pc>

UFED Analytics Desktop, (2019). *Live product demonstration*. Retrieved September 8, 2019, from <https://www.digitalforensics.com/blog/ufed-analytics-desktop-live-product-demonstration/>

UFED Analytics Enterprise, (2019). *Pandacom forensic solutions*. Retrieved September 8, 2019, from <http://www.forensicsolutions.co.za/products/cellebrite/ufed-analytics-enterprise>

UFED Camera Kit, (2019). Retrieved August 26, 2019, from <http://www.forensicsolutions.co.za/products/cellebrite/ufed-camera-kit>

UFED Chinex, (2019). *Teel technologies*. Retrieved September 8, 2019, from <https://www.teeltech.com/mobile-device-forensic-tools/cellebrite/ufed-chinex/>

UFED InField, (2019). *Cellebrite*. Retrieved September 8, 2019, from <https://www.cellebrite.com/en/ufed-infield/>

UFED Ultimate, (2019). Retrieved September 8, 2019, from <https://www.cellebrite.com/en/ufed-ultimate/>

Ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar. Retrieved October 8, 2019, from <https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf>

- Yang, C. & Yen, P. (2010). Fast deployment of computer forensics with USBs. In *Proceedings of International Conference on Broadband, Wireless Computing, Communication and Applications*, 413-416.
- Yaycı, E. (2007). *Bilişim suçları*. MSc Thesis, Gazi University, Ankara.
- Yıldırım, K. (2016). *Building cyber operation scenarios for cyberwarfare simulations*. Msc Thesis, Yaşar University, İzmir.
- Zeadally, S. & Flowers, A. (2014). Cyberwar: The what, when, why, and how. *Technology and society magazine*, 33 (3), 14-21.
- Zhou, Y. and Jiang, K., (2012). An analysis system for computer forensic education, training, and awareness. In *International Conference on Computing, Measurement, Control and Sensor Network*, 48-51.

APPENDICES

Appendix 1: Definitions

Internet: The Internet is a gigantic network of computer networks that span each other around the world.

Informatics Network: Communication system in technical, economic and social fields.

Informatics Technology: It is the system of all tools and equipment used in information technology.

Informatics System: They are the systems involved in the presentation of all kinds of services, transactions and data provided through information and communication technologies.

Information Security: It is a field of study aiming to protect the integrity and continuity of information products / devices and the data being processed in these devices. The purpose of information security is to protect data integrity, to prevent unauthorized access, to protect privacy and confidentiality, to ensure the continuity of the system.

Cyber security: To protect the information systems that constitute cyber environment from attacks, to ensure the confidentiality, integrity and accessibility of the information processed and environment. Detect attacks and cyber security are incident to initiate the response mechanisms against these determinations.

Key Concepts of Information Security: There are three basic items.

Privacy: Informatics system and service is only accessible by authorized person or systems. Confidential data belonging to or in information systems should not be disclosed by unauthorized persons or systems.

Integrity: Informatics and information can only be changed by authorized personnel or systems.

Accessibility: Access to informatics systems and information by authorized persons and transactions within the required time and quality required.

The Concept of Attack in Information Security: Any act made by using information systems in order to gain unauthorized access to, damage to, and material / moral gain of all values and information owned by institutions and individuals can be defined as digital attacks.

Law: It is all of the rules of social behavior that govern the socially important behaviors of the people living in the society, and the orders and prohibitions that provide the peace, tranquility and mutual trust of the common life.

Crime: Acts prohibited by the criminal threat of the law.

Informatics Crime: It is any kind of behavior that is performed against or with a system which processes the information automatically or serves for the transfer of data.

Forensic Informatics: It is a new science that tries to find answers to the questions of what, who, where, when and how by using computer. “Forensic Information, the use of computer research and analysis techniques to eliminate potential evidence that can be used during a trial. “Forensic Information, information in a computer or information system to be used to prove guilt or innocence in court.”

Appendix 2: List of Abbreviations

ACK	Acknowledgement
ACPO	The Association of Chief Police Officers
AES	Advanced Encryption Standard
ALT	Alternate
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
ATM	Automatic Teller Machine
BIOS	Basic Input-Output System
CAM	Computer Aided Manufacturing
CF	Compact Flash
CIA	Confidentiality, Integrity, Availability
CIH	Chernobyl
CPU	Central Processing Unit
CTRL	Control Key
DAT	Type of Tape Cartridges
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLT	Type of Tape Cartridges
DNS	Domain Name System
DoS	Denial of Service
DVD	Digital Versatile (Video) Disc
EU	European Union
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
HTTP	Hyper-Text Transfer Protocol
HTTPS	Secure Hyper-Text Transfer Protocol
GB	Gigabyte
GPS	Global Positioning System
IBAN	International Bank Account Number
ICMP	Internet Control Message Protocol
ID	Identification Number

IDS	Intrusion Detection Systems
IP	Internet Protocol
IPsec	Internet Protocol Security
IPS	Intrusion Prevention System
ISO	Type of File Format
ISP	Internet Service Provider
ISS	Internet Service Provider
IT	Information Technology,
JTAG	Joint Test Action Group
LAN	Local Area Network
MAC	Media Access Control
MD5	Message-Digest 5
MITM	Man-in-the-middle
MMC	Multimedia Card
MP3	MPEG-1 Audio Layer 3
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NIC	Network Interface Card
NTFS	New Technology File System
PC	Personal Computer
POS	Point of Sale
RAM	Random Access Memory
RAT	Remote Administration Tool
RFC	Remote Function Call
ROM	Read Only Memory
OECD	Organization for Economic Co-operation and Development
SD	Secure Digital
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SYN	Synchronize
TAP	Test Access Points
TCP	Transmission Control Protocol

TPC	Turkish Panel Code
UAE	United Arab Emirates
UDP	User Datagram Protocol
UK	United Kingdom
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USA	United States of America
USB	Universal Serial Bus
XML	Extensible Markup Language
VBR	Variable Bit Rate
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WPA	Wi - Fi Protected Access
ZIP	Type of Lossless Data Compression