

**Digital Forensics:
Guidelines and Tools for a Digital Evidence
Investigation Process
A Case Study for a Business Data Leak**
BACHELOR'S THESIS

Bachelor of Engineering, Information and Communications Technology

Author: Perla Rocío Ramírez Sanabria

Tutor: Jarkko Paavola

Tutor UPV: José Enrique López Patiño

Course 2019-2020

Foreword

First and foremost, I would like to thank both the institutions I have been a part of which are the Polytechnic University of Valencia and the Turku University of Applied Sciences. The teachers in the School of Telecommunications Engineering in my home university as well as the teachers and staff in the ICT City campus and the supervisor of this thesis, Jarkko Paavola.

This document is dedicated to my mother, who has supported me in this journey since the very first day I decided to grow in the field that I am passionate about.

Special thanks go for my friends and colleagues that walked hand in hand with me since the beginning of my degree as well as in the writing process of this document. I would like to especially thank Ana and Alberto for being the greatest supporters during these years in several aspects of my life. I would like to thank Álvaro for being my biggest companion during my study years at my home university. Significant mention also goes for Mónica, Francisco and Martín that have accompanied and supported me over the years through the highs and lows in the degree as friends as well as classmates.

Abstract

The objective of this thesis was to provide a suitable and admissible analytical framework for a digital forensic analysis carried out by an investigator. In this thesis these concepts are explained in-depth to provide what could be considered as a guide for the execution of a digital evidence investigation. It is important to note that this investigation can usually, or rather must, end in a judicial process. The theoretical framework of this thesis has been developed by consulting books written by specialists in the field of digital forensics, ISO/IEC standard documents, as well as models described by different government organizations and user guides for the required tools. In the case study, the concepts explained previously are exposed in the case of an insider threat performing a data leak to a company in the competition. After performing the analysis of the evidence acquired for the case, it was possible to determine that a data breach performed by an insider threat took place. The results of the practical analysis are decisive in a judicial court if the procedures of the analysis have been followed, hence the importance of the proper application of the methods and use of the tools.

Keywords: Digital Forensics, Cybersecurity, Expert Examiner, Investigation, Digital Evidence, Cybercrime

Resumen

El objetivo de esta tesis es proveer de un marco analítico idóneo y admisible para una investigación forense digital ejecutado por un perito informático. En este documento estos conceptos son explicados en profundidad para proporcionar lo que podría ser considerado como una guía para la ejecución de una investigación de evidencia digital. Es importante remarcar que dicha investigación usualmente puede o más bien debe acabar en la vía judicial. Es aquí donde se produce la convergencia. Un punto crucial de este estudio se ha basado en subrayar la relación entre tecnologías de la información y las leyes. Es fundamental tener en cuenta que el peritaje ha de estar realizado siguiendo unas pautas en concreto para que los evidencias puedan ser admitidas dentro del marco legal que dicta la ley del territorio donde se ha producido la ofensa. El marco teórico de esta tesis ha sido desarrollado mediante la consulta de libros de especialistas en el campo, documentos estándar ISO/IEC, así como modelos descritos por diferentes organizaciones gubernamentales y guías de usuario para las herramientas requeridas. En el marco práctico, los conceptos explicados anteriormente están expuestos en un caso de *Insider Threat* llevando a cabo una filtración de datos corporativos a una compañía de la competencia. Los resultados del análisis práctico son decisivos en un tribunal judicial si se han respetado los procedimientos, de ahí la importancia de la correcta aplicación de los métodos y el uso de las herramientas.

Palabras clave: Digital Forensics, Cybersecurity, Expert Examiner, Investigation, Digital Evidence, Cybercrime

Contents

Contents	v
List of Figures	ix
List of Tables	xi

1 Introduction	1
1.1 Cybercrime	2
1.2 Digital Forensics	3
2 Digital Evidence	5
2.1 Locard's Principle	5
2.2 Best Evidence Rule	6
2.3 Hearsay	7
2.4 Characteristics of Digital Evidence	7
2.5 Chain of Custody	8
3 Digital Evidence Investigation Process	9
3.1 Phases	10
3.1.1 Evidence Preparation, Policy and Procedure Development	10
3.1.2 Evidence Assessment	11
3.1.3 Evidence Acquisition	13
3.1.4 Evidence Examination	14
3.1.5 Documenting and Reporting	15
3.2 Methods	16
3.2.1 RFC 3227	16
3.2.2 ISO/IEC 27037:2012	17
3.2.3 ISO/IEC 27041:2015	18
3.2.4 ISO/IEC 27042:2015	19
3.2.5 ISO/IEC 27043:2015	20
3.2.6 ISO/IEC 27050	20
4 Tools for Digital Forensics Analysis	22
4.1 Autopsy	23
4.2 PhotoRec	24
4.3 FTK Imager	24
4.4 The Volatility Framework	25
4.5 Advanced Digital Forensics Workstations	25
4.5.1 Ondata	26
4.5.2 ADALID	28
4.6 Portable Hardware Devices for Digital Forensics	30
4.6.1 Logicube: Forensic Talon Ultimate	30
4.6.2 Tableau Forensic Imager TX1	31
4.6.3 Ditto Forensic FieldStation by CRU	31
5 Case Study: Insider Threat - Data Leak	33
5.1 Description of the case	33
5.2 Assessment	34

5.2.1	Materials	34
5.2.2	Insider Threat: Definition and Indicators	34
5.2.3	Interview with other employees	35
5.3	Acquisition: Disk Image creation with FTK Imager	36
5.4	Examination: Data analysis with Autopsy	39
5.4.1	Web Search	42
5.4.2	Web Downloads	42
5.4.3	Web History	43
5.4.4	Windows Artifacts	44
5.4.5	E-Mail Messages	50
5.4.6	Tags	50
5.5	Reporting	53
6	Discussion	54
7	Conclusion	55
	Bibliography	56
A	NIST: Computer Forensics Tools and Techniques Catalog	59
B	Other Forensics Tools	73
B.1	Acquisition and Memory Analysis	73
B.2	Disk Mounting	73
B.3	Carving and Disk Tools	74
B.4	File System Utilities	74
B.5	Malware Analysis	74
B.6	Frameworks	75
B.7	Windows Registry Analysis	75
B.8	Password Recovery	76
B.9	Mobile Devices	76
C	Autopsy – Installation and User Guide	77
C.1	Installation	77
C.2	Analysis Modes	79
C.2.1	Input Formats	79
C.3	Analysis Features	79
C.4	Evidence Search Techniques	81
C.5	Case Management	82
C.6	Reporting	83
C.7	User Interface (UI) Layout	83
D	PhotoRec – Operating Systems, File Systems, File Formats	95
D.1	Operating Systems	95
D.2	File Systems	95
D.3	File Formats Recovered By PhotoRec	96
E	FTK Imager – Installation, Features, User Guide	103
E.1	Installation	103
E.1.1	Locally	103
E.1.2	Portable Device	104
E.2	Running FTK Imager	104
E.2.1	Command-Line Options	104
E.3	Features	104
E.4	User Interface	105
E.4.1	Menu Bar	105
E.4.2	Toolbar	107
E.4.3	View Panes	107

E.5 File Systems and Drive Image Formats	107
F Volatility – Operating Systems, Formats	110
F.1 Operating Systems	110
F.2 Formats	111
G RFC 3227 – Guidelines for Evidence Collection and Archiving	112
H Talon Ultimate – Datasheet	123
I Tableau Forensic Imager TX1 – Datasheet	126
J Ditto Forensic FieldStation – Datasheet	132
K Report generated by FTK Imager	135
L Report generated by Autopsy	137

List of Figures

1	Graphical representation of the Locard's Principle Casey (2011)	5
2	Two files on a Windows machine that differ by only one letter have significantly different MD5 values Casey (2011)	7
3	A comparison of terminology related to digital investigation process models Casey (2011)	9
4	Application of different ISO/IEC standards in the phases of a digital forensics investigation	17
5	Zeus workstation	29
6	Hades workstation	29
7	Poseidon workstation	30
8	Talon Ultimate Imaging Device	30
9	Tableau Forensic Imager TX1	31
10	Ditto Forensic FieldStation	32
11	E-Mail received from Bioert's CEO Calvin Morgan	33
12	Select Source Wizard in FTK Imager	36
13	Select File Wizard in FTK Imager	37
14	Select Image Type Wizard in FTK Imager	37
15	Evidence Item Information Wizard in FTK Imager	37
16	Select Image Destination Wizard in FTK Imager	38
17	Creating Image process in FTK Imager	38
18	Drive/Image Verify Results in FTK Imager	38
19	Initial Wizard to create a case in Autopsy	39
20	New Case Information Wizard in Autopsy	39
21	Add Data Source Wizard in Autopsy	40
22	Select Data Source Wizard in Autopsy	40
23	Ingest Modules Configuration Wizard in Autopsy	41
24	Adding Data Source in Autopsy	41
25	Tree Viewer of the case in Autopsy	42
26	Web Search in Autopsy	42
27	Web Downloads in Autopsy	43
28	Web History in Autopsy	43
29	Web History in Autopsy	44
30	Open/Save MRU Artifact in Autopsy	44
31	Open/Save MRU Artifact in Autopsy	45
32	Database:ActivitiesCache.db schema	45
33	User information tables: 'Activity', 'ActivityOperation' and 'Activity_PackageID'	46
34	Windows Timeline Process	46
35	Table 'Activity': Opening original downloaded files	47
36	Table 'Activity': Opening renamed files and modifying 'random 2'	47
37	Table 'Activity': Encryption with PGP Tool	47
38	Table 'Activity': Outlook usage	47

39	Table 'Activity_PackageID'	48
40	Table 'Activity_PackageID'	48
41	Last-Visited MRU Artifact in Autopsy	48
42	Shortcut (LNK) FilesArtifact in Autopsy	49
43	LNK Files extracted from Autopsy in the investigator's system	49
44	Sent E-Mail Message by the suspect: Encrypted Data	50
45	Sent E-Mail Message by the suspect: Public and Private Keys	50
46	Sent E-Mail Message by the suspect: Passphrase	50
47	Tags in Autopsy	51
48	Exported Files from Autopsy	51
49	Import PGP Key	51
50	Imported PGP Keys	52
51	Decrypt Wizard in PGP Tool	52
52	Decrypt Wizard in PGP Tool	52
53	Decryption Completed	52
54	Decrypted and Original Files (comparison/match)	53
55	Report Generating Wizard in Autopsy	53
56	Autopsy Workflow	79
57	Timeline Analysis' First Interface. Picture downloaded from https://www.sleuthkit.org/autopsy/timeline.php	80
58	Timeline Analysis' Second Interface. Picture downloaded from https://www.sleuthkit.org/autopsy/timeline.php	80
59	Autopsy's User Interface	84
60	Tree Viewer example	84
61	Single File Extraction	85
62	Example of "Thumbnail Results Viewer"	86
63	Example of "Table Results Viewer"	86
64	Example of "Result Content Viewer"	87
65	Example of "Hex Content Viewer"	87
66	Example of "Media Content Viewer"	88
67	Example of "String Content Viewer"	88
68	Example of "Text Content Viewer"	88
69	Lists tab in the Keyword Search Configuration Dialog	89
70	String Extraction tab in the Keyword Search Configuration Dialog	90
71	General tab in the Keyword Search Configuration Dialog	90
72	Modules Pipelines	91
73	Ingest Modules Configuration	91
74	Ingest Box	92
75	Ingest Settings	92
76	Individual Keyword Search	92
77	Individual Keyword Search Results	93
78	Keyword List Search	93
79	Keyword List Search Results	94
80	Screenshot of options available in the File menu	105
81	Screenshot of options available in the View menu	106
82	Screenshot of options available in the Mode menu	106
83	Screenshot of options available in the Help menu	107
84	Features in the Toolbar	108

List of Tables

1	Sources of Digital Evidence Jhala (n.d.)	6
2	Comparison between Velociraptor models	28
3	ADALID Zeus Workstation Specifications	29
4	ADALID Hades Workstation Specifications	29
5	ADALID Poseidon Workstation Specifications	30
6	Cloud Services Forensic Tools and Techniques	59
7	Hardware Write Block Tools and Techniques	59
8	Data Analytics Forensic Tools and Techniques	60
9	Database Forensic Tools and Techniques	60
10	Memory Capture and Analysis Tools and Techniques	61
11	Image Analysis (Video & Graphics Files) Tools and Techniques	61
12	Deleted File Recovery Tools and Techniques	62
13	Password Recovery Tools and Techniques	62
14	Disk Imaging Tools and Techniques	63
15	Software Write Block Tools and Techniques	63
16	Email Parsing Tools and Techniques	64
17	Remote Capabilities/Remote Forensics Tools and Techniques	64
18	File Carving Tools and Techniques	65
19	Forensic File Copy Tools and Techniques	65
20	Incident Response Forensic Tracking & Reporting Tools and Techniques	66
21	Social Media Tools and Techniques	66
22	WiFi Forensics Tools and Techniques	66
23	Hash Analysis Tools and Techniques	67
24	Mobile Device Acquisition, Analysis and Triage Tools and Techniques	68
25	Steganalysis Tools and Techniques	69
26	String Search Tools and Techniques	70
27	Video Analytics Tools and Techniques	71
28	Video Format Conversion Tools and Techniques	71
29	Web Browser Forensics Tools and Techniques	71
30	Windows Registry Analysis Tools and Techniques	72
31	Operating Systems supported by PhotoRec	95
32	File Systems supported by PhotoRec	95
33	Archive file formats supported by PhotoRec	96
34	Multimedia file formats supported by PhotoRec. Part 1	96
35	Multimedia file formats supported by PhotoRec. Part 2	97
36	Multimedia file formats supported by PhotoRec. Part 3	98
37	Office file formats supported by PhotoRec	99
38	Other file formats supported by PhotoRec. Part 1	100
39	Other file formats supported by PhotoRec. Part 2	101
40	Other file formats supported by PhotoRec. Part 3	102

41	File Systems supported by FTK Imager	107
42	Whole Disk Encrypted supported by FTK Imager	109
43	Hard Disk Image Formats supported by FTK Imager	109
44	CD and DVD Image Formats supported by FTK Imager	109
45	Windows memory images supported by Volatility	110
46	Mac OS X memory images supported by Volatility	110
47	Linux memory images supported by Volatility	111
48	Memory Format Support for Volatility	111

CHAPTER 1

Introduction

Throughout history, communications users have evolved as well as their need to reach longer distances and wider audiences. To that end, computing was born and later the Internet, a technology capable of communicating to millions of people around the world instantly which has become a tool indispensable to carry out daily actions.

The Internet is one of the most powerful tools society possesses nowadays and being able to access this resource carries a great responsibility. Internet users must be aware of the dangers that can be found on the Web.

Cybercrime constitutes one of the most important threats regarding information technology. The use of the Internet has been extended to almost every aspect of society's lives, whether the subject is a professional matter or private life. This is the reason why it entails the biggest threat to every user.

Now, more than ever, it is possible to share every kind of data with any kind of device. Data include as files or media in any shape or form by using laptops, mobile phones, personal computers, and a long list of different devices. The information transmitted can be intercepted, manipulated, or deleted and the user must be aware of the nature of the information shared as well.

It is difficult, given these advances and continuous changes, to find updated bibliography that compiles: the latest versions of forensic software, the new legislative orders, recent standards and norms published, and other content disclosed by associations, schools, and agencies.

The theoretical framework of this thesis has been developed by consulting books written by specialists in the field of digital forensics, ISO/IEC standard documents, as well as models described by different government. The documentation for the practical framework was based on software user guides as well as training offered by the developers.

The purpose of this work is to offer an updated reference document, of a theoretical and practical nature, with the technical-legal aspects that the future forensic computer expert must know, and to provide an introductory look at the hardware and software technology used in the digital forensic investigation. The thesis focuses mainly on the technical aspects of the analysis. This includes the description of the investigation process as well as the tools and techniques. The reason behind this point of view is the jurisdiction of laws. Every country has different legislation regarding different crimes. Chapter 2 explains the basic concepts related to digital evidence. These include its definition, principles, characteristics as well as the importance of the chain of custody from the beginning to the end of the investigation.

Chapter 3 encompasses the broad concept of a "Digital evidence Investigation Process", where the recommended steps in each phase of the process are discussed in detail. The model explained is the NIJ 2004 model - which has been written and published by the United States Institute of National Justice. This is a globally accepted model. In addition,

internationally applicable methodologies have been cited and described, being mostly developed by ISO/IEC and IETF.

Chapter 4 describes the different tools used to carry out the analytical process. Software solutions are explained. The explanations detail the installation processes, the different features present the format options that users have. The description of these tools arises from the reading of the different documentation guides made available by the developers. When explaining certain tools in depth, it has been decided to describe open source tools, to guarantee easy access to them.

Moreover, it describes the hardware solutions, including among these the workstations used to carry out the investigation as well as certain tools used mainly in the evidence acquisition phase. These tools have been explained in less depth due to the lack of resources to be able to use them in the practical case. It has been chosen to introduce the products briefly and include the data sheet in the appendices to record their specifications.

In the last chapter, the theoretical concepts and knowledge discussed in previous chapters are put into practice by carrying out a complete practical case of digital forensic investigation and analysis. Each phase of the investigation is illustrated with images and screenshots, the programs and tools used are described, the results obtained based on the requirements of the judicial file are discussed, and finally, the conclusions are drawn up. Lastly, the author of the thesis was responsible for choosing the topic as well as the documentation and writing of the theoretical framework of this document. The practical case was personally carried through by the author as well as the description of the practical framework.

The choice of topic has been based on the interest of the author of the thesis, in addition to the need for an expansion of knowledge within the framework of cybersecurity. Furthermore, published works such as "*Digital forensics: an integrated approach for the investigation of cyber/computer related crimes*" by Moniphia Orlease Hewling, "*Role and Impact Of Digital Forensics in Cyber Crime Investigations*" by David Mugisha and "*Digital Forensics*" by Ajay Prasad and Jeetendra Pandey have been used to define a theoretical framework.

1.1 Cybercrime

According to the definition in [Panda Security \(2018\)](#) cybercrime is:

"Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense. A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device. It is also a cybercrime to sell or elicit the above information online."

It is also important to remark that there is a possibility for a computer to be a tool and a target at the same time, as it occurs in the case of hacking.

In the context of cybercrime there exist several subgroups like "*Cyber-terrorism*", "*information welfare*", "*phishing*", "*spams*", "*denial of service attacks*", "*hacktivism*", "*hate crime*", "*identity thefts*", "*online gambling*"¹ as well as the production and distribution of child pornography as it is noted in [Wall \(2009\)](#).

Also, besides the different subgroups mentioned above, there are three major categories where cybercrime falls into as is described in [Panda Security \(2018\)](#):

- **Property cybercrime:** refers to the possession of an individual's personal information such as credit card information or login credentials. Said information can be

¹Legal in many countries. It may end up in scams and it might be easily accessible by underage individuals

used with malicious intent for instance identity theft, making fraudulent online purchases, or gain access to online bank accounts.

- **Individual cybercrime:** refers to the distribution of malicious or illegal information. This can include cyberstalking, distribution of pornography, or trafficking.
- **Government cybercrime:** refers to what it is known as cyber terrorism and it comprises hacking of government sites, military websites, or distribution of propaganda.

1.2 Digital Forensics

According to information found in Sant & Hewling (2011) digital forensics refers to the acquisition, preservation, analysis, and representation of digital evidence produced from the investigation of digital-related crimes. This analysis digs deep into performing with certain specialized techniques, procedures, and tools that are going to be discussed later in the document. Digital forensics, which can also be referred to as "Computer Forensics", can be explained as "the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications and storage devices. A forensic specialist must collect data in such a way that is admissible as evidence in a court of law." Vacca & Rudolph (2010).

Digital Forensics will serve as a tool to pursue cybercrime in all categories mentioned in the section above. As cybercrime grows exponentially every day, evidence of such felonies grows as well. This is the reason why professionals that work in this field need to be aware of two important facets: technology and law. The experts, besides being proficient in the latest tools and methods for digital forensics analysis, need to be up to date with subjects like information security, cybercrime, and cybersecurity as well as the judicial system regarding forensics in this matter. Computer Forensics incorporates the experience of IT, forensics, and legislation which poses a fascinating and daunting range of problems surrounding cybersecurity to be addressed. Cybercrimes impose new challenges when it comes to their prevention, detection, investigation, and prosecution.

For an analysis to be perfectly done, there are several methods with different steps and characteristics that will guarantee the digital evidence to be preserved to ensure authenticity, traceability, and auditing in processes. "The traceability and preservation of processes is an important aspect to verify and guarantee the authenticity of all the digital objects used and produced by the process, and to allow an analysis whether the processes were executed as expected, or according to regulations" Mayer et al. (2014). Digital Forensics can be used in several settings such as Sammons (2012):

- **Criminal Investigations:** In the context of criminal investigation a vast number of crimes can be included such as child pornography, identity theft, homicide, sexual assault, robbery and burglary. The main reason behind this is that any of these crimes can still leave a digital evidence. In modern days, almost every device possessed by a citizen can provide such evidence.
- **Civil Litigations:** In civil cases, both parties require to examine evidence that are going to be used against them. This legal process is known as "discovery". Previously, this discovery involved the examination of each party exchanging reports,

letters, and memos; however, the introduction of digital forensics and eDiscovery² has greatly changed this practice.

- **Intelligence:** Terrorists and foreign governments have also joined the digital era. It is known that nowadays terrorists use digital technologies as a tool to communicate, recruit, and plan attacks.
- **Administrative Matters:** Digital evidence can also be profitable "incidents other than litigation and matters of national security. Violations of policy and procedure often involve some type of electronically stored information, for example, an employee operating a personal side business, using company computers while on company time."

²"As part of a process known as Electronic Discovery (eDiscovery), digital forensics has become a major component of much high dollar litigation. eDiscovery "refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case" Sammons (2012)"

CHAPTER 2

Digital Evidence

Digital evidence is defined as *any data stored or transmitted using a computer that supports or refutes a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi* (adapted from Chisum (1999)).

There are several other definitions such as the one proposed by the Standard Working Group on Digital Evidence (SWGDE), which states that any information of probative value that is either stored or transmitted in a digital form. Another definition proposed by the International Organization of Computer Evidence (IOCE) is information stored or transmitted in binary form that may be relied upon in court. Casey (2011)

As previously mentioned in Chapter 1, the data shared through networks can be in any shape or form. Different devices produce different types of data. As this occurs, it is normal to expect different sources of evidence, which can be seen in Table 1 Jhala (n.d.).

2.1 Locard's Principle

Locard's Principle states that any interaction between two items will create evidence. This will apply to any kind of interaction at a crime scene, "including between an offender and victim, between a person with a weapon, and between people and the crime scene itself." Casey (2011). This will apply to both physical, which is out of the scope of this document, and digital evidence. Figure 1 illustrates the Locard's principle.

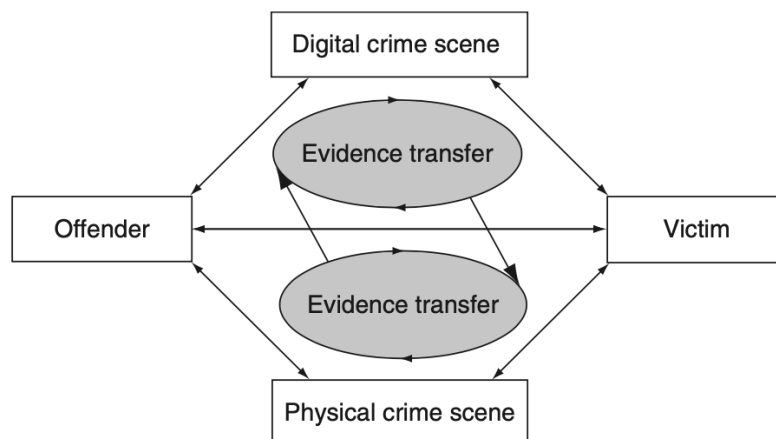


Figure 1: Graphical representation of the Locard's Principle Casey (2011)

Sources	Devices	Potential Evidence
Storage Devices	Hard Drives, External Hard Drives, Memory Cards, Removable Media, Thumb Drives	E-mail messages, Internet browsing history and chat logs, photographs, image files, databases, financial records and event logs.
Handheld Devices	Mobile Phones, Tablets.	Software applications, data, documents, Internet browsing history and chat logs, photographs, image files, databases, financial records
Peripheral Devices	Keyboard and mouse, Microphones, Web cameras, Memory card readers, VoIP devices, Printers	Incoming and outgoing phone and fax numbers; recently scanned, faxed, or printed documents; and information about the purpose for or use of the device.
Network Devices	Network hub, Laptop network card and ethernet cable, Internet modems, Network switch and power supply, Wireless access point, Wireless network server	The connected devices themselves. The device functions, capabilities, and any identifying information associated with the computer system; components and connections, including Internet protocol (IP) and local area network (LAN) addresses associated with the computers and devices; broadcast settings; and media access card (MAC) or network interface card (NIC) addresses
Other	Surveillance equipment, Digital Cameras, Video Cameras, Digital Audio Recorders, Video Game Consoles, GPS Systems	The device or item itself, its intended or actual use, its functions or capabilities, and any settings or other information it may contain is potential evidence.

Table 1: Sources of Digital Evidence [Jhala (n.d.)]

2.2 Best Evidence Rule

When evidence constitutes writing, recording or photographs, the court can usually demand for the original version of the evidence. The reason behind this rule was that the decisions made in the courtroom were the best possible based on the best available information. "The policy behind the Best Evidence Rule is to prevent un-necessary inaccuracy stemming from the fallibility of human memory or transcription" Ford (2014).

Thanks to the rapid development in digital technologies such as photocopiers, scanners and computers it is easy to forge or alter evidence, but it is also available the exact replication of evidence. Generally, copies are accepted in place of the original, thus, "a genuine question is raised as to the authenticity of the original or the accuracy of the copy or under the circumstances it would be unfair to admit the copy in lieu of the original" Casey (2011). An advantage of presenting exact copies as evidence is that the original is prevented from being altered or damaged.

2.3 Hearsay

A piece of evidence might not be admitted if it contains hearsay. Considering that, if the speaker or author of said evidence is not present in the courtroom to prove its truthfulness, it is possible to revoke it.

"Evidence is hearsay where a statement in court repeats a statement made out of court in order to prove the truth of the content of the out of court statement. Similarly, evidence contained in a document is hearsay if the document is produced to prove that statements made in court are true. The evidence is excluded because the crucial aspect of the evidence, the truth of the out of court statement (oral or documentary), cannot be tested by cross-examination." Hoey (1996)

This means that, for instance, some materials such as calls or e-mails can be used to prove the veracity of the evidence, but cannot be used to prove the full truth of the statements. Although, there are exceptions, which is the case for business records, this matter is out of the scope of this thesis.

2.4 Characteristics of Digital Evidence

Digital evidence must have certain characteristics along the process of forensics analysis:

- **Admissibility:** There must exist conformity with laws and legislative rules. A relationship between the digital evidence and the fact being proven must be established. Digital evidence must be obtained legally with authorization if necessary.
- **Integrity:** The source of the digital evidence must be trusted and remain unaltered from the time it was collected, by doing so the authentication process is supported. In order to verify the integrity of the evidence, digital fingerprints taken at the time of the collection and current state are compared.

Message digests and cryptographic hash values are used in the process. The reason behind this is that message digest algorithms always produce the same value for a given input. Any slight change produces a different value, which can determine if the evidence has been altered since the time of the first hash value generation. Figure 2 illustrates the difference in MD5 output with two files that differ only in one character.

Digital Input	MD5 Output
The suspect's name is John	c52f34e4a6ef3dce4a7a4c573122a039
The suspect's name is Joan	c1d99b2b4f67d5836120ba8a16bbd3c9

Figure 2: Two files on a Windows machine that differ by only one letter have significantly different MD5 values Casey (2011)

- **Completeness:** The digital evidence must help to lead the investigation to a conclusion. "When a forensic investigator states the evidence collected is a complete account it is implied that all the relevant evidence from the environment has been preserved (relevant to the subject of the investigation). We can interpret completeness as being the extent to which all the relevant evidence from the digital environment has been collected." Ahmad & Ruighaver (2004)
- **Authentication:** This concept refers to satisfying the court that the evidence has "remained unchanged, that the information in the record does in fact originate from its purported source, whether human or machine, and that extraneous information

such as the apparent date of the record is accurate" Sommer (1997). The expert must be able to prove to the authenticity of the evidence by explaining the reliability of the computer equipment, the manner in which the basic data was initially entered, the measures taken to ensure the accuracy of the data as entered, the method of storing the data and the precautions taken to prevent its loss of the reliability of the computer programs used to process the data, and the measures taken to verify the accuracy of the program.

Authentication is not a single-step process but, it is formed by two-step which are:

1. Initial examination of the evidence to determine if it provides what is claimed.
 2. Closer analysis to determine its probative value.
- **Objectivity:** There must therefore be no bias when evaluating and providing data, this is crucial to provide decision makers with the clearest possible view of the facts. The most effective method is to encourage the proof to talk for itself as much as possible. Through inference and all the relevant empirical facts should be provided. The objective evaluation method which evaluates the findings of a forensic analyst for distinctions or some other deficiency is another efficient approach.
 - **Repeatability:** A significant feature of the experimental process is that all tests or findings have to be replicated such that they can be confirmed independently. It is necessary to log in adequate detail the measures taken to identify and examine digital evidence to enable us to objectively validate the results in order to facilitate any analysis of forensic findings.

2.5 Chain of Custody

According to the definition found in Rios (2014), the chain of custody "refers to the chronological documentation and/or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic.". One the most important aspects of authentication is the maintenance and documentation of the chain of custody of evidence. Integrity and authenticity of a piece of digital evidence must be certified to a court of law. Benner (2009)

When evidence is presented as an exhibit, it is necessary to maintain and establish a record of the chain of evidence Jaffee et al. (2008). In case this record is not presented, the evidence may not have the characteristics needed even when its legitimate and unaltered. Tomlinson et al. (2006).

From the moment the evidence is collected and throughout the course of the investigation, the chain of custody keeps track of every individual that handles the evidence. This is performed in order to determine that the evidence was not manipulated or retained without authorization. Although there is no rule in regard to the amount of people that should intervene with the evidence, it is appropriate to keep this number as low as possible. Moreover, the people mentioned in the previous sentence must be qualified so evidence is handled properly to avoid tampering. Badiye et al. (2019)

CHAPTER 3

Digital Evidence Investigation Process

There are several models regarding the digital investigation process. These process models have their origins in the early theories of computer forensics which defined the field in terms of a linear process. For example, forensic computing was described in 1999 by McKemmish as: "The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable" [McKemmish \(1999\)](#). According to the citation above, the basis of a process will be constituted by the sequence of the following activities, *identification, preservation, analysis* and *reporting*. Variations will depend on the granularity and terminology of the different phases of said process. In the following subsections, the most common steps in the process are going to be discussed. Figure 3 illustrates the different phases that exist in various digital investigation process models.

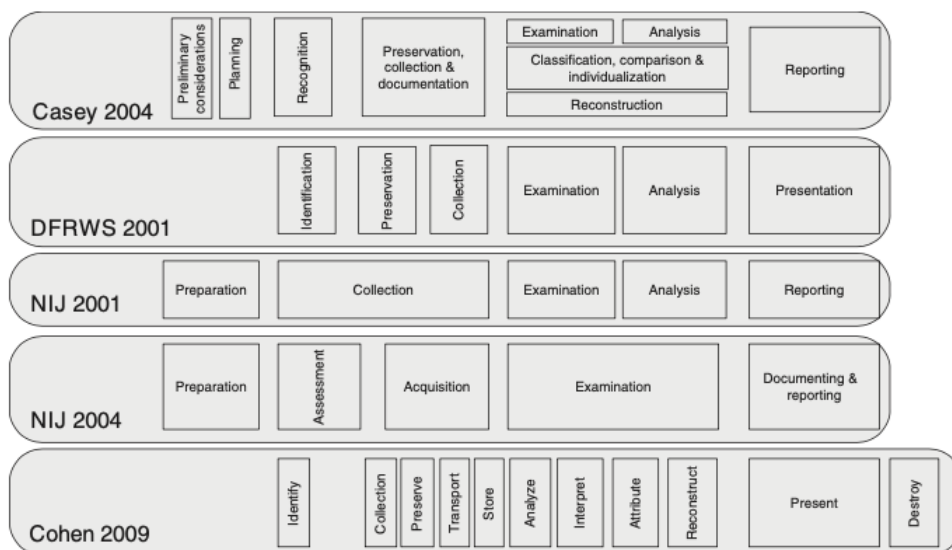


Figure 3: A comparison of terminology related to digital investigation process models [Casey \(2011\)](#).

Preparation.

This activity consists in the generation of a plan of action. The main purpose of the plan is to effectively conduct the digital investigation by obtaining supporting resources and materials.

Survey/Identification.

In this step of the digital investigation, the main goal is to find potential sources of digital evidence, which can be any of the ones previously described in Table 1.

Preservation.

The fundamental objective in this step is to prevent any changes in the *in-situ* evidence. This is the step where the isolation of the system on the network, securitization of relevant log files and collection of volatile data occurs.

Examination and Analysis.

In this step, the experts search for and interpret the evidence found.

3.1 Phases

In the following subsections, the different phases described by the NIJ 2004 model (United States Department of Justice (2004)). It is crucial to note that this is only a model that describes possible and general guidelines surrounding the phases of the investigation. Later in the document different standardised methods are going to be discussed and explained.

3.1.1. Evidence Preparation. Policy and Procedure Development

The objective is the development of policies and procedures to establish a plan of action with operations and functions to create the computer forensics unit. The plan of action must take into account several factors which are going to be discussed in the following sections:

Personnel

The digital forensics analysis must be carried out by competent experts, aware of the technologies to be in use, procedures and legislations. The subjects discussed by this segment include task requirements and required qualifications, working hours, on-call status, command structure and team arrangements.

Administrative considerations

Software licensing The tools used by the experts in the analysis must be acquired legally and properly licensed by the agency.

Resource commitment A digital evidence investigation requires certain resources, financial and personnel. Within these resources, the following items are included:

a facility where the analysis is going to take place, hardware equipment, software and hardware requirements, upgrades, experts' training and ongoing professional development and retention of examiners.

Training Throughout the investigation, expert examiners must stay skilled and up to date. This can be managed by improving the expertise of current workers or by hiring candidates from different disciplines. In the IT field, which is continuously evolving and changing, training is a crucial factor that must be considered in budget submissions.

Case management

The conditions for the prioritization and the scheduling of investigations will be determined and carried out once a proposal for forensic services is accepted. Criteria can include the complexity of the offense, court dates, deadlines, potential victims, legal factors, volatile nature of the evidence and resources available.

Evidence handling and retention

The guidelines for receiving, processing, documenting, and handling evidence and work products associated with the examination must be established according to the already existing departmental policy. Nevertheless, in the context of digital evidence handling and retention, the criteria could possibly exceed the policies mentioned before.

Developing technical procedures

There must be procedures to guide the process of evidence examination. This procedure must be put to test before applying it to ensure the potential results obtained are accurate, valid and reproducible. The procedures taken to carry out this part of the process begins with the identification of the problem. As it seems obvious, this step is mandatory to establish solution proposals to later test on samples. The results on the test can be positive or negative, this is rated after the evaluation. After all these tasks are performed, finalization of the procedure takes place.

3.1.2. Evidence Assessment

In order to decide the course of action, visual information will be cautiously examined concerning the complexity of the situation. The procedure of assessment will be executed by reviewing the search warrant or other legal authorization, the details of the case, the nature of the hardware and software, potential evidence and the circumstances surrounding the acquisition of the evidence. The assessment step is a key point in the investigation, without the potential collection and preservation of the evidence can be lost.

At this stage, the examiner evaluates the situation and considers many factors for analysis, such as whether the investigation should be conducted internally or involve an external agency; whether a search warrant should be issued. Any pre-search work may also be carried out such as the collection of details on the company's systems and assets; details on personnel participating in the situation, whether explicitly or indirectly; the collection of information on the protection incident team and its core skills, etc. In order to perform the inquiry the prosecutor must plan and test the forensic examination toolkit. The interviewer will also notify the testing team regarding the quest strategy and

the recommendations.

There are two defined points within the assessment process, which are:

The evolution of this step is based on two main points, being the review of the case the first one. In this sub-step, the first task will be the identification of the legal authority for the forensic examination request. It is mandatory to have insurance of a completed request for assistance. The subsequent tasks will be the completion of the documentation of the chain of custody. As was mentioned previously in the document, CoC is a crucial part of the investigation that must be kept updated overtime since the investigation is issued.

The second main point focus on the consideration of facts about the case. The first aspect an investigator should consider must be the processes that will be required to be performed on the evidence alongside the determination of the equipment needed. Inherently, this will lead to the possibility of the evidence. The evidence can issue from different sources. For instance, data obtained from an Internet service provider (ISP), remote locations or e-mail information. Peripheral devices (digital cameras, laminators, credit card blanks, check paper, scanners, and printers) can provide evidence to the case as well. After the investigator considers the sources of digital evidence, they should determine what can be considered actual evidence. Evidence can be found in media files, spreadsheets, document files, databases, financial records, aliases, e-mail accounts, e-mail addresses, ISP used, names, network configuration and users, system logs, passwords, usernames, etc. The skill levels of the users of these investigated devices need to be taken into account. This will determine if the user, being in possession of these skills, could have been able to conceal or destroy evidence with techniques such as encryption, booby traps, steganography. After all these aspects are evaluated, it is necessary to prioritize the order of evidence examination.

Onsite considerations

When investigators are onsite, there is a small window to consider the actions that need to be carried out. Onsite refers to the place where the system is physically located. First and foremost, the number and type of devices that will be included in the investigation must be identified as well as the documentation of the types and volume of media, including removable media and offsite storage areas and/or remote computing locations. Identification of the proprietary software and the operating system of the device is crucial to the investigation. There is a possibility that these devices are not connected to any kind of network at some point, so the determination of the existence of a network onsite is needed. With a view to being aware of the level of the system administrators and users, the investigator will interview them. On a general basis, the investigator will have to evaluate the general conditions of the site.

Processing location assessment

Assessment of the evidence must be put through with a view to determining the proper environment where the examination should take place. The examination will preferably occur in a controlled environment, such as a dedicated forensic work area or laboratory. Although, it is possible that circumstances can lead an examiner to fulfill an onsite examination. The investigator should consider the time they will need onsite to recover all the evidence previously mentioned in the document bordering on the suitability of equipment, resources, media, training, and experience they have to properly carry through the onsite evaluation. Long-term deployment and search should be also contemplated because of the impact on the business and logistics and staff concerns related.

Legal considerations are present in this phase as well in the identification of the reach of the search authority and possible concerns related to the application to different statutes.

Evidence assessment

As mentioned earlier in the document, there is a prioritization of the evidence in the analysis. This is based on the location where evidence is found and the stability of media to be examined. For instance, volatile data must be the first kind of evidence to be examined. One of the factors that require to be taken into consideration is the need for battery-operated devices to provide continuous electric power. In some cases, it is necessary to evaluate the storage locations for EMI 1 to ensure the evidence is not tarnished by this factor. Evidence could be possibly affected during packaging, transport or storage, hence the establishment of the condition of it is crucial when performing the analysis.

3.1.3. Evidence Acquisition

The main goal of this procedure is to acquire the original (or exact copy) digital evidence in such a way that protects and preserves it. This procedure is required as a result of the inherent properties of digital evidence, which is fragile. By the reason of its fragility, it can be easily forged, damaged or destroyed by cause of improper handling or examination. This step is where data is retrieved from where it is allocated originally. This can also include the request and reception communications data; it is not only referred to data allocated on a disk.

The steps performed in this phase will be decisive for the rest of the investigation because it entails the physical extraction of the digital evidence. Hence, security must be guaranteed at all costs. This security must be guaranteed in the examiner's systems as well, both hardware and software configurations and functioning are determining when the investigation is carried through. It is mandatory for the examiner's storage device to be forensically clean when the acquisition of the evidence.

It is possible that the storage devices require physical access by disassembling them to be protected from any external interference. The examiner will determine which devices need to be gathered. Such devices can either be internal, external, or both. All the specifications of the suspect's system need to be listed since it could affect the analysis. Among them, there are the condition of the drive (e.g., make, model, geometry, size, jumper settings, location, drive interface) and internal components (e.g., sound card; video card; network card, including media access control (MAC) address; personal computer memory card international association (PCMCIA) cards).

Despite in some cases, there is a need for battery-operated devices to be continuously provided with electric power, the disconnection of the storage devices to prevent plausible digital evidence to be destructed, damaged or altered is needed depending on the device and the nature of the evidence.

Retrieval of information about the configuration of the suspect's system through several controlled boots. The first one is needed in pursuance of capturing CMOS/BIOS information and test functionality. The second boot is required to test the computer's functionality and the forensic boot disk. And the third one is performed in order to capture the drive configuration information from the CMOS/BIOS.

After all these tasks are performed, the system must be powered down and proceed with the actual acquisition of the storage device using the examiner's system. It is important to configure the device, so it is recognized by the examiner's system.

There are exceptions to the removal of storage devices from certain devices. For RAID (Redundant Array of Inexpensive Disks) its removal may result in not usable results. In

laptop systems removal could be inaccessible and if possible, may result in unusable results. In the case of legacy devices there is a hardware dependency, older drives may not be readable in newer systems. There could be also a lack of access to equipment due to unavailability.

Additionally, there are some aspects to consider when treating the data during acquisition. It is advisable to perform an image of the suspected devices instead of working with the original exhibit in order to prevent altering it. When making a copy of the digital evidence, the bit-stream copy option will provide a bit-by-bit image of the original evidence. This will be helpful for the consideration of the copy evidence as to the original for the purpose of investigation. In order to guarantee evidence remains unaltered during the investigation process, the examiner can calculate the checksum or a hash value of both the original evidence and copy. This can also be applied to images.

3.1.4. Evidence Examination

In this step examination on data acquired occurs by the utilization of accepted forensics procedures. This examination will preferably not be conducted on the original evidence.

Preparation

Working directories with evidentiary files and data must be prepared. From these directories, the information should be recovered and/or extracted.

Extraction

There are two types of possible extractions, physical or logical. When the extraction is physical, the data is identified and recovered across the entire physical drive without regard to the file system. If the extraction is logical, files and data are identified and recovered based on the installed operating system, file system and/or applications.

Physical extraction In this stage, several methods can be applied such as keyword searching, file carving and extraction of the partition table and unused space on the physical drive.

Logical extraction In this stage, several methods can be applied such as the extraction of the file system information, data reduction to identify and eliminate known files, extraction of files pertinent to the examination, recovery of deleted files, extraction password-protected, encrypted and compressed data, extraction of file stack and extraction of the unallocated space.

Analysis of extracted data

Analysis refers to the process of interpreting the data that was previously extracted in views of establishing its significance to the case. The analysis may include these steps:

Timeframe analysis This step can help conclude when events occurred on a system, with this is possible to determine a relationship between usage of the computer and the user at the time the events befell. This analysis also incorporates time and date stamps in the file system metadata "(e.g., last modified, last accessed, created, change of status)" to connect files of interest to relevant time frames. Furthermore, a

review of the system and application logs should be considered. Among these logs, it is feasible to encounter error logs, in installation logs, connection logs, security logs, etc.

Data hiding analysis This step is vital considering data can be hidden in the system. This may help with the detection and recovery of data that might indicate knowledge, ownership, or intent. For example, there are methods to intentionally hide data on a system and purposely changing file extensions is one of them. If there are mismatches after performing a correlation between file headers to the corresponding file extensions, this may indicate intentionally hidden data.

Obtaining access to all the files, including password-protected, encrypted, and compressed files is key so as to know if there is an endeavor of concealing the data from unauthorized users.

Further to this, the usage of steganography is another way to hide data. According to the definition found in [Neijts et al. \(2018\)](#), steganography is a technique that hides secret data within an ordinary, non-secret, file or message in order to avoid detection. Later, at its destination, the secret data is extracted. There are no boundaries when it regards to the type of content that carries the secret data, this includes text, image, video or audio content and many more.

Ultimately, the obtention of access to the host-protected area (HPA) is relevant. An effort to conceal data may be suggested by the inclusion of user generated data in an HPA.

Application and file analysis Programs and files may contain information pertinent for the investigation and supply with awareness about the capability of the system and the knowledge of the user. Amid the methods that can be applied the examiner has to perform the review of file names in search of relevance and patterns, examine of the content of the files, identify of the number and type of operating system, establish a correlation between files and installed applications and relationships between different files, identify of unknown file types to determine their value to the investigation, examine of the file structure of the drive and the users' default storage location for applications¹, examine of the user's configuration settings and analyze of file metadata.

Ownership and possession Throughout the analysis, it is relevant to identify the user that created, modified or accessed a certain file. It may also be critical to determine ownership and knowledgeable possession of the questioned data.

Conclusion

Information derived from each of these steps itself cannot be enough to draw a conclusion. Nonetheless, when considered as a whole, comparisons between the different results may offer a bigger picture of the case. The examiner must consider the results of the extraction and analysis in their entirety.

3.1.5. Documenting and Reporting

This step must be done contemporaneously with the examination, as the actions taken during the digital evidence investigation must be correctly registered. Documentation is an ongoing process throughout the examination. The documentation executed by the examiner must be complete, accurate and comprehensive so interpreters of this information

¹This is performed to determine if files have been stored in their default or an alternate location.

can understand the case correctly. The report may include the identity of the reporting agency, case identifier or submission number, case investigator, identity of the submitter, date of receipt, date of report, descriptive list of items submitted for examination, (including serial number, make, and model), the identity and signature of the examiner, brief description of steps taken during the examination, such as string searches, graphics image searches, and recovering erased files and results/conclusions.

Summary of findings

This section of the report consists of a summary of the results of the examination executed on the system.

Details of findings

This section of the report consists in a deeper description about the results of the examination and it may include specific files related to the request, other files, including deleted files, that support the findings, string searches, keyword searches, and text string searches, internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity, graphic image analysis, indicators of ownership, which could include program registration data, data analysis, description of relevant programs on the examined items and techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies

Supporting materials

List of supporting materials used throughout the examination, such as printouts of particular items of evidence, digital copies of evidence, and chain of custody documentation.

Glossary

The document can include a glossary to help the reader understand technical terminology.

3.2 Methods

In the previous section on the document, the phases of the Digital Forensics Analysis are explained. It is important to note that within these phases, different standard methods can be applied in order to carry out said analysis:

3.2.1. RFC 3227

"*Guidelines for Evidence Collection and Archiving*": All the information included in this section is extracted from the RFC 3227 IETF's website [IETF \(2002\)](#). Description of the procedure taken in the analysis is described in the document of the RFC 3227 in the "Appendices" chapter.

3.2.2. ISO/IEC 27037:2012

Figure 4 illustrates the application of ISO/IEC documents to different phases of the investigation.

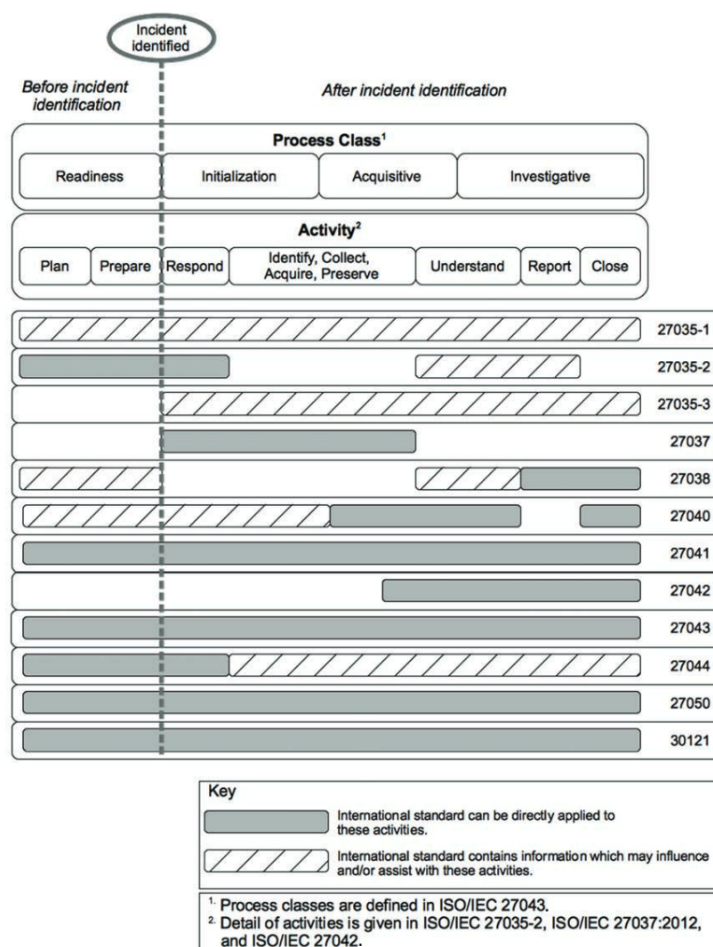


Figure 4: Application of different ISO/IEC standards in the phases of a digital forensics investigation

"Techniques of Digital Forensics Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence" ISO/IEC (2012)

This International Standard provides guidelines for specific activities in handling digital evidence, which are identification, collection, acquisition and preservation of digital evidence that may be of evidential value.

The examiner that is in charge of handling digital evidence should be able to be aware of the potential risks that they can encounter when working with the material. With this International Standard, there is an intention to provide guidance to carry out the investigation properly. This guidance is aimed at the following individuals:

- Digital Evidence First Responders (DEFRs)
- Digital Evidence Specialists (DESSs)
- Incident Response Specialists
- Forensic Laboratory Managers

The individuals mentioned above must follow certain principles in order to carry through the investigation correctly [Veber & Smutny \(2015\)](#):

- Minimal manipulation with digital devices or digital data.
- Documentation of actions and changes occurred to the digital evidence. Necessary to inform decision-makers who need to determine the reliability of digital evidence presented to them.
- Accordance between the laws of the country.
- DEFR should not act beyond their competence.

This International Standard guides individuals concerning common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions. This International Standard gives guidance for the following devices and/or functions that are used in various circumstances:

- Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto-optical disks, data devices with similar functions.
- Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards.
- Mobile navigation systems.
- Digital still and video cameras (including CCTV).
- Standard computer with network connections.
- Networks based on TCP/IP and other digital protocols.
- Devices with similar functions as above.

One of the most important points in an investigation is to ensure the integrity and authenticity of the potential digital evidence, because of this reason it will be necessary to carry out an acceptable methodology. However, the International Standard does not mandate the use of particular tools or methods. This will also apply for methodologies for the legal proceedings, disciplinary procedures and other related actions in handling potential digital evidence that are outside the scope of identification, collection, acquisition and preservation.

National laws, rules and regulations must work hand in hand with the International Standard, it will not replace specific legal requirements of any jurisdiction.

3.2.3. ISO/IEC 27041:2015

“Guidance on assuring suitability and adequacy of incident investigative method” [ISO/IEC \(2015a\)](#)

It offers guidelines on measures to ensure that the procedures and approaches used to evaluate cybersecurity incidents are sufficient. This takes into account whether third-party manufacturers and checks will aid with this assurance process. Its objectives are the following:

- Provide directions on the capture and subsequent analysis of both functional and non-functional requirements related to security in incident investigation.
- Using validation to ensure the adequacy of the investigative processes.
- Determine new validation rates and required tests from a validity exercise.
- Select specific evaluations and documentation in the validation process.

This International Standard may be useful to guarantee the validity of digital evidence in court proceedings. It defines part of a comprehensive analysis process that does not only include the following subject areas but also includes:

- Incident management.
- Digital evidence handling.
- IDS and IPS systems, including information that can be obtained from these systems.
- Storage security, including sanitization of storage.
- Ensure the analysis techniques are suitable for purposes.
- Analysis and interpretation of digital evidence.
- Understanding digital evidence forensic concepts and procedures.
- Security incident event management.
- Relationship between electronic discovery and other investigative methods, as well as the use of electronic discovery techniques in other investigations.
- Governance of investigations, including forensic investigations.

3.2.4. ISO/IEC 27042:2015

"Guidelines for the analysis and interpretation of digital evidence" [ISO/IEC \(2015b\)](#)

This International Standard offers a guide to digital evidence analysis and interpretation. It includes guidance about how the possible digital evidence of an event should be evaluated and viewed to decide and examine which can be needed to justify its comprehension.

It provides a standard context for assessing and evaluating security management incidents and can be used to incorporate new approaches. This also offers a variety of concepts that are relevant to modern digital forensic analysis taking into account that the usage of a certain method can influence the interpretation of the digital evidence used in the process.

It deals with the analytical models that can be used by digital forensics experts in static or active systems and the considerations to be taken into account in each case, especially attention to incidents in live or active systems such as mobile devices, encrypted systems, networks, etc.

There are two methods to approach live analysis. It is important to consider those systems that cannot be copied and extracted as an image. With this sort of system, there is a risk of losing digital evidence when copied so it will be crucial to try to minimize possible evidence garnishment and ensure there is a complete register of the processes carried

out. On the other hand, when there is a possibility to copy or image a system, it will be necessary to interact with it as well as observe its functioning. Other considerations include being careful to emulate the hardware or software of the original environment, using verified virtual machines, copies of the original hardware in order to allow analysis as close as possible to the real one.

Nevertheless, the content of the analysis results in the expert report and its legal considerations are detailed. Finally, it includes the competences of forensic experts: training, learning, skills, objectivity and professional ethics.

3.2.5. ISO/IEC 27043:2015

"Incident investigation principles and processes" [ISO/IEC \(2015c\)](#)

Provides guiding principles for incident investigation processes involving digital evidence. It includes the preparation processes prior to the incident through the closure of the investigation, as well as warnings about it. The International Standard describes the processes and principles applicable to the different types of criminal investigations, such as security breaches, system failures, unauthorized access, among many others. It does not offer specific details for each type of investigation, but an overview of the applicable research principles and processes.

3.2.6. ISO/IEC 27050

"Information technology— Electronic discovery"

ISO/IEC 27050-1:2019 Overview and concepts [ISO/IEC \(2019\)](#)

This International Standard is essential as it gives the expert an overview of the term *electronic discovery*, which "is the process of discovering pertinent Electronically Stored Information (ESI) or data by one or more parties involved in an investigation or litigation, or similar proceeding". In this overview terminology, concepts, and processes that are intended to be exploited by other parts of the 27050 series are included. Among the concepts, identification, preservation, collection, processing, review, analysis, and production of ESI are detailed. Electronic discovery turns out to be the unifying thread in investigations as well as in acquisition and management tasks of the evidence, which can have characteristics such as high sensitivity making special protections required.

ISO/IEC 27050-2:2018 Guidance for governance and management of electronic discovery [ISO/IEC \(2018\)](#)

Organizations, as well as stakeholders within and outside those organizations, at collective and individual risk, may be exposed by participating in electronic discoveries and processes at the legal, financial and ethical levels. This International Standard is intended to guide decision-makers and ensure that compliance and policy requirements continue to be met to enable effective and appropriate electronic discovery and processes.

This document is intended to address the concerns of electronic discovery by identifying risk and risk owners. The purpose of this document is to provide a guide for the governance and management of electronic discovery.

ISO/IEC 27050-3:2020 Code of practice for electronic discovery ISO/IEC (2020)

This International Standard provides requirements and recommendations addressed to both technical and non-technical personnel involved in activities related to electronic discovery. It is important to note that the user is expected to be aware of any applicable jurisdictional requirements. Moreover, additional material is included in order to help organizations have a better understanding of the goals that arise with electronic discovery processes. This document gathers aspects of both 27050-1: 2019 and 27050-2: 2018 to establish a broad framework to specify relevant measures for the reduction of the ESI life span.

CHAPTER 4

Tools for Digital Forensics Analysis

Nowadays, there are numerous tools for the digital forensics analysis that can be used for different types of data in a device. Depending on the analysis carried out and the evidence found the tools chosen by the examiner will differ. Among the target of these tools hard drives, storage devices, network topologies, software, mobile phones, laptops are found.

It is important to note that when evidence collection occurs it is better to use portable tools that can be run with USB devices and DVDs, which are executed externally, in order to avoid any kind of corruption in the digital evidence when installing these software applications in the suspect's system.

Subsequently, evidence that is collected and guarded is analyzed in what is called a "Forensics Laboratory". In this lab different hardware and software forensics tools can be used conducive to obtain and analyzed the extracted evidence.

When choosing a tool in the first place the examiner can encounter a huge difficulty due to the repeated problems of reliability, security and support, between the two existing currents: Tools with a commercial purpose which normally keep the procedures hidden for the users and must be paid in order to be used and tools created by a group or organization that are designed as open-source tools. Secondly, there is a problem surrounding the minimum requirements that must be met so that their use on the evidence does no more harm than good.

To guarantee the correct operation and reliability of forensic informatics tools, there are organizations that test and validate them, such as the National Institute of Standards and Technology (NIST) within their Computer Forensics Tool Testing Program (CFTT). The objective of this organization is to establish a methodology for the equipment, criteria and test procedures that allow the development of the tool specifications. The results provide the information necessary for manufacturers to improve their tools, and for users to have sufficient information to decide which software to purchase to obtain accurate and objective results.

In the following tables, from Table 6 to Table 30 (in "Appendices" chapter), software specified [The National Institute of Standards and Technology \(2019\)](#)'s website are listed. It is essential to note that the majority of these products are commercial solutions. Later in the document, software available in the market that are not included in NIST's catalog, mostly open-source and freeware, are listed and classified.

4.1 Autopsy

Autopsy [The Sleuth Kit \(n.d.a\)](#) is the software computer that represents the graphical interface to the command line digital investigation analysis tools in The Sleuth Kit and it was originally developed by Brian Carrier. These two can analyze Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3).

The software is maintained by Basis Technology Corp. with the assistance of programmers from the community. The company, as it shows on their website (<https://www.autopsy.com/support/training/>), offers different support services and training.

A very important trait about Sleuth Kit and Autopsy is that both are open-source and run on UNIX (Linux, Mac OS X, Open & FreeBSD, Solaris, Cygwin) and Windows platforms. Although, different versions are distributed under different licenses. While Autopsy 2 source code is distributed under a GPL 2 license, Autopsy 3 and 4 source code are distributed under a Apache 2 license. It is necessary to point out that the programming languages used for both source codes are different as well, while the version 2 is written in Perl, the version 3 is written in Java using the Netbeans platform.

Autopsy provides certain characteristics that help examiners carry through a more in-depth analysis [Wikipedia \(2020\)](#):

- **Extensible:** Through developing plugins, the user should be able to add new functionalities. These plugins can analyze all or part of the underlying data source. Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third-parties. (e.g. Timeline Analysis, Hash Filtering, Keyword Search, Web Artifacts, Data Carving, Multimedia, Indicators of Compromise.)
- **Centralized:** A standard process for accessing all functions and modules must be given by the tool.
- **Intuitive:** The browser must allow users to repeat steps taken previously without having to reconfigure excessively by offering wizards and historical tools. It should be noted that digital forensic tools could also be used by non-technical investigators. A proof of this is the Autopsy's default view, which is a simple interface where all the analysis results can always be found in a single tree.
- **Multiple Users:** The tool must hand over the possibility to be usable by a single examiner or a whole team of examiners.
- **Fast:** This is obtained thanks to the execution of several background tasks in parallel using multiple cores. Additionally, certain configurations can be applied in order to obtain a faster speed in analysis such as skipping searching for orphan FAT files and skip analysis of unallocated space and prioritization of user folders and files over system folders and files.
- **Cost Effective:** The software is completely free and at the same time offers the same core features as other digital forensics tools and offers other essential features, such as web artifact analysis and registry analysis, that other commercial tools do not provide.

Additionally, add-one modules [\[1\]](#) can be added to extend the original software package.

¹Found in <https://www.autopsy.com/add-on-modules/>

4.2 PhotoRec

PhotoRec is a free and open-source tool that is used for data recovery based on signatures, it recovers various data types including video, documents and archives from hard disks, CD-ROMs, memory cards (CompactFlash, Memory Stick, Secure Digital/SD, SmartMedia, Microdrive, MMC, etc.), USB memory drives, DD raw image, EnCase E01 image, etc. This tool is distributed under the GNU General Public License v2 or later. This means the user can run the program for any purpose, read and change the code in order to obtain a certain outcome, redistribute copies and distribute copies of the modified versions to others under the same license.

In order to understand how PhotoRec work, it is important to understand how file systems store files. FAT, NTFS, ext2/ext3/ext4 file systems store them in data blocks². The size of these block is a constant number of sectors. Generally, operating systems store data in a contiguous way with a view of minimizing fragmentation.

Once a file is deleted, metadata about it is lost. This metadata includes file name, date/-time, size, location of the first data block/cluster, etc. The first item PhotoRec is going to try to find is the data block size. When an examiner needs to recover deleted files and the file system is not corrupted, it is necessary to take into account how the file systems behave when it comes to deleted data. Although PhotoRec is file system agnostic, meaning it only goes after the underlying data, the software needs to be aware of where the data can be potentially found. In the case of ext2/ext3/ext4, the value for the data block can be read from the superblock. On the other hand, for FAT and NTFS systems, this value can be read from the volume boot record. Else ways, PhotoRec will require to read the media, sector by sector, directed towards finding the block size. Once the value is known by the software, the reading process will be performed block by block. After the blocks are read, these are checked against a signature database that comes with the program.

After the file is recovered, PhotoRec stops its recovery to later check the consistency of the file when feasible and starts to save the new file. The size of this new file will depend on fragmentation. If the data is not fragmented, the size of the new file will be identical or larger than the original. PhotoRec is able to know the original size by reading it from the file header and truncate it, if necessary, to the proper size. If the size of the new file is smaller than the one specified in the header, it ends up being discarded.

When the recovery process is finished, PhotoRec checks the previous data blocks to see if a file signature was found but the file was not able to be successfully recovered and tries it again. This is how fragmented files can be completely recovered.

Information regarding operating systems, file systems and file formats are included in tables in the "Appendices" chapter.

4.3 FTK Imager

FTK® Imager [AccessData Group, Inc. \(2016\)](#) is a data preview and imaging tool that is used in order to acquire digital evidence without altering it. These perfect copies are known as forensic images. In order to prevent any manipulation to the evidence, intentional or accidental, the software performs a bit-for-bit duplicate image of the media. By doing so, the forensic image is identical in every way to the original, including file slack and unallocated space or drive free space. After the acquisition is performed, further analysis can be carried through with other forensic tools, for instance, Access Data® Forensic Toolkit® (FTK). Needless to say, these two tools developed by the AccessData Group, Inc are complementary.

²called "cluster" in Windows environments

As mentioned previously in the document, the creation of the image should be one of the first steps taken by an Incident Responder. This is performed with the view of not losing any artifact or evidence about the potential attack. It is also important to note that the software calculates MD5 hash values and confirms the integrity of the data before closing the files.

There are two versions of the software. Installed or portable, the first one runs the full installation on the required system while the second one can be run through a USB stick. Information regarding operating systems and file systems are included in tables in the "Appendices" chapter.

4.4 The Volatility Framework

Volatility is a framework used to carry out digital forensics analysis designed by forensics, incident response, and malware experts. It allows a forensics investigator to analyze RAM dumps from 32/64-bit Windows, Linux, Mac and Android systems. It is written in Python, which an established forensic and reverse engineering language with loads of libraries that can easily be integrated with the framework. Volatility is packaged in various formats, including the source code in zip or tar file (for all platforms), a PyInstaller executable (Windows only), and a standalone executable (Windows only).

It is an open-source tool distributed under the GPLv2 license, meaning that the user has the possibility to read, learn from the code and extend it. The user also can immediately fix any issues instead of having to wait for any update from the vendors.

Furthermore, an extensible and scriptable API grants the user the freedom to go beyond and innovate. Analysts can add new address spaces, plugins, data structures, and overlays to truly weld the framework to their needs.

Volatility's modular design allows it to easily support new operating systems and architectures that do not yet exist. All devices are targets of possible attacks or misfortunes and thanks to Volatility's modularity it can be adapted to any operating system.

With this tool, it is possible to extract information from running processes, open network sockets, network connections, loaded DLLs from each process and cache log sections, process IDs and more. It also has support to extract information from Windows crash dump files and hibernation files among many other data.

Volatility operates fast and efficient algorithms without unnecessary overhead or memory consumption, this allows RAM dumps of large systems to be analyzed. For starters, in a few seconds volatility will list the kernel modules on an 80 GB system. Although improvements are still necessary, and time varies by command, other memory analysis frameworks can take much longer to perform the same tasks in much smaller memory dumps.

Information regarding operating systems, file systems and file formats are included in tables in the "Appendices" chapter.

4.5 Advanced Digital Forensics Workstations

The digital forensics workstations must be powerful and high-performance servers that would allow the investigator to conduct the analysis smoothly, this requires a large storage capacity for disk imaging, cloning and backup copies. Additionally, the processes in order to perform the analysis with certain technologies demand a considerable amount of resources.

4.5.1. Ondata

Ondata is a Spanish company that is in charge of design the Velociraptor forensic workstations. They are designed to solve the need for investigators to have the proper hardware in accordance with the analysis software. Ondata technicians have been able to design the right equipment so that researchers from both companies and the security forces can do their work smoothly and safely. These workstations are meant to cover efficiently all the steps in a digital forensics investigation, from data acquisition until reporting. [Ondata \(2020\)](#)

Velociraptor 3

It is equipped with SSD disks to give maximum speed to the Operating System and with RAM memory from 32GB to 256GB, which will allow the examiner to run multiple applications at the same time. In addition, they incorporate write-blocked ports FireWire, USB 3.0, SATA and eSATA, which facilitates connectivity with the different forensic devices that need to be investigated.

Velociraptor 3 incorporates a liquid cooling system, using refrigerant fluids to extract the heat generated by the equipment components, cooling it as a whole. This type of cooling, in addition to being less noisy than cooling with ventilation, increases the frequency of the processors' clocks, taking the equipment to its maximum performance.

They include software with forensic utilities that will be useful for the development of investigations. Also, to prevent possible data loss due to disk failures, it includes disk status monitoring software, which will issue an alert to the user if any of the forensic station's disks deviate from their operating range. Some of the utilities included in these devices are virtualization software, software to work ISO images, disk status monitoring software, hash calculation software, memory Analysis Tool Suite, timeline Analysis, hash filtered Keyword search, Hex editor and PCAP analysis.

Velociraptor 5

It is equipped with SSD disks to give maximum speed to the Operating System and with RAM memory from 128GB or 256GB, which will allow the examiner to run multiple applications at the same time. In addition, they incorporate write-blocked ports FireWire, USB 3.0, SATA and eSATA, which facilitates connectivity with the different forensic devices that need to be investigated.

As it occurs with the Velociraptor 3, Velociraptor 5 incorporates a liquid cooling system, using refrigerant fluids to extract the heat generated by the equipment components, cooling it as a whole. This type of cooling, in addition to being less noisy than cooling with ventilation, increases the frequency of the processors' clocks, taking the equipment to its maximum performance.

Ondata's Velociraptor devices are the only forensic station that incorporates monitoring software that monitors the status of all the disks connected to the station. The software sends notifications that alert the user if any of the disks installed in the equipment deviate from its range of operation, thus corrective and preventive measures can be taken to help prevent data loss. In addition, it includes software with forensic utilities that will be useful for the development of investigations.

The utilities included are the same as in the Velociraptor 3.

Velociraptor 7

It is equipped with 960GB SSD PCI disks to give maximum speed to the Operating System and with 256GB RAM memory, which will allow the researcher to run multiple applications at the same time. To give greater security to the stored data, it offers 32TB in Raid 5 for evidence storage; and to make the investigation quicker and more agile, it includes 2TB in Raid 0 for temporary and 8TB in Raid 0 for cases.

The station includes the DeepSpar Disk Imager 4 solution, which is a disk imaging device capable of recovering data from unstable hard disks with damaged sectors and can recover information that can be of great value for research. The solution brings the Forensics Add-on plug-in active, which allows using ATA commands to disable the automatic relocation of damaged sectors so that more data can be extracted, deleted or viewed master and user passwords from the disk, access to the hidden DCO area, Preparation of forensic reports at the file level including data such as path, name, size, creation date, number of sectors, corrupt sectors, MD5 hash, among others.

It comes equipped with FireWire, USB 3.0, SATA and eSATA write-locked ports, making it easy to connect to the various forensic devices that need investigation.

Following the same steps as Velociraptor 3 and 5, Velociraptor 7 incorporates a liquid cooling system, using refrigerant fluids to extract the heat generated by the equipment components, cooling it as a whole. This type of cooling, in addition to being less noisy than cooling with ventilation, increases the frequency of the processors' clocks, taking the equipment to its maximum performance.

The utilities included are the same as in the Velociraptor 3 and 5.




Velociraptor 3, 5 and 7 Specifications			
			
	Velociraptor 3	Velociraptor 5	Velociraptor 7
Processor	Dual Xennon 8C	2 x Dual Xennon 12C	2 x Dual Xennon 18C
RAM	64 GB	128 GB	256 GB
S.O. Disk	SSD 128 GB	SSD 256 GB	SSD PCi 960
Temp. Disk	2 TB	SSD 2 TB	2TB in Raid 0 SSD
Evidence Disk	6 TB	18 TB in Raid 5	32 TB in Raid 5
Cases Disk	6 TB	12 TB in Raid 0	8 TB in Raid 0
Operating System	Windows 10 Pro	Windows 10 Pro	Windows 10 Pro
Raid System	No	Yes	Yes
Write Blocker	Yes	Yes	Yes
Card Reader	Yes	Yes	Yes
DeepSpar	No	No	Yes
HotSwap Bay	Yes	Yes	Yes
Blu-Ray	27"	2 x 27"	3 x 27"
Screen	Yes	Yes	Yes
Keyboard	Yes	Yes	Yes
USB 3.0	Yes	Yes	Yes
HDMI	Yes	Yes	Yes
Gbe	Yes	Yes	Yes
FireWire	Yes	Yes	Yes

Table 2: Comparison between Velociraptor models

4.5.2. ADALID

ADALID is a Colombian company that is specialized in computers assembled specially for digital forensics purposes. These workstations are unique in the world and guarantee data processing speed and integrity in said processes. [ADALID \(2015\)](#)

Zeus

High-performance forensic workstation in terms of processing digital evidence, in accordance with the needs for a high volume of data analysis. It is specially made for forensics laboratories that require high availability of storage space through RAID 0, 1, or 5 arrangements, with an excellent high-temperature dissipation.


ADALID Zeus Workstation	
	<p>Board Dual Socket GA-7PESH3 LGA2011</p> <p>Processor: Intel® Xeon® E5-2600 V2 LGA 2011 (x2).</p> <p>Screen: 27-Inch Full-HD 2ms LED with Webcam and Sound.</p> <p>RAM: 64GB DDR3 2400Mhz HyperX Beast (Max 256GB).</p> <p>Connections: eSATA, SATA3, FireWire, USB 3.0.</p> <p>Solid State Hard Drive: 512GB CSSD-F512GBLX, Array x2 HDD 2TB.</p> <p>Burner: BluRay DL, DVD RW, CD RW.</p> <p>High-Performance Power Supply.</p> <p>Latest Generation Chassis.</p> <p>Dissipation: by Radiator All-In-One Liquid Cooling.</p> <p>GB GDDR5 DIGI+ VRM technology Graphic Card HD7770-2GD5 x3DVI x1 HDMI</p> <p>Write Blockers Kit: Tableau Ultra Kit II model.</p>
<p>Figure 5: Zeus workstation</p>	

Table 3: ADALID Zeus Workstation Specifications

Hades

Advanced forensic workstation in terms of processing digital evidence. Specially made for laboratories that demand high speed for acquisition and data analysis without losing probatory force in the evidence. It offers an excellent dissipation of high temperatures. Plus, interconnection capacity with various advanced data transfer technologies such as Thunderbolt, Wi-Fi 2ways, eSATA, SATA3, Bluetooth 4.0, NFC.


ADALID Hades Workstation	
	<p>Board 97-DELUXE (NFC & WLC) ATX DDR3 2600 LGA 1150</p> <p>Processor: Intel Core i7-4790K (8M Cache, up to 4.40 GHz) New 4th Generation.</p> <p>Screen: 27-Inch Full-HD 2ms LED with Webcam and Sound.</p> <p>RAM: 32GB DDR3 2400Mhz HyperX Beast.</p> <p>Connections: eSATA, SATA3, FireWire, USB 3.0, USB 2.0, Thunderbolt, WiFi 2ways, Bluetooth 4.0, NFC, Wireless Charger.</p> <p>Solid State Hard Drive: 512GB CSSD-F512GBLX, x1 HDD 2TB.</p> <p>Burner: BluRay DL, DVD RW, CD RW.</p> <p>High-Performance Power Supply.</p> <p>Latest Generation Chassis.</p> <p>Dissipation: by Radiator All-In-One Liquid Cooling System One Socket.</p> <p>GB GDDR5 DIGI+ VRM technology Graphic Card HD7770-2GD5 x3DVI x1 HDMI</p> <p>Write Blockers Kit: Tableau Ultra Kit II model.</p>
<p>Figure 6: Hades workstation</p>	

Table 4: ADALID Hades Workstation Specifications

Poseidon

Forensic workstation with the proper balance between power, performance, cost and energy consumption. Specially made for small or new forensic laboratories where the priority is based on the stability in processes with adequate hardware according to current technology. Useful for analysis of digital evidence and to provide training on applicable technical methodology, based on forensic computing principles.


ADALID Poseidon Workstation	
 <p>Figure 7: Poseidon workstation</p>	<p>Board Chipset: Intel Z87 Express x3 PCI-Express 3.0 ATX DDR3 2600 LGA 1150</p> <p>Processor: Intel Core i7-4790S (8M Cache, 3.2 GHz) New 4th Generation.</p> <p>Screen: 27-Inch Full-HD 2ms LED with Webcam and Sound.</p> <p>RAM: 32GB DDR3 1600Mhz</p> <p>Connections: eSATA, SATA3, FireWire, USB 3.0, USB 2.0.</p> <p>Solid State Hard Drive: 256GB CSSD-F512GBLX, x1 HDD 2TB.</p> <p>Burner: BluRay DL, DVD RW, CD RW.</p> <p>High-Performance Power Supply 1050W.</p> <p>Latest Generation Chassis.</p> <p>Dissipation: by multiple fans(Top, Front, GPU, Back, HDD).</p> <p>Write Blockers Kit: Tableau Ultra Kit II model.</p>

Table 5: ADALID Poseidon Workstation Specifications

4.6 Portable Hardware Devices for Digital Forensics

4.6.1. Logicube: Forensic Talon Ultimate

Designed for field or forensic lab use, the Talon® Ultimate delivers advanced, high-performance forensic imaging at a budget-friendly price. Featuring a compact footprint, user-friendly navigation and unbeatable imaging speed, the Talon Ultimate continues the proud legacy of previous generations of the Talon® forensic imaging solutions. Engineered specifically for digital forensic investigators, the Talon Ultimate meets all the forensic imaging, hashing and wiping requirements. [Logicube \(2020\)](#) Figure 8 provides a picture of the device described in this subsection, Talon Ultimate manufactured by Logicube.



Figure 8: Talon Ultimate Imaging Device

Features

Features to this product are included in the datasheet added as an appendix later in the document.

4.6.2. Tableau Forensic Imager TX1

The OpenText Tableau Forensic Imager (TX1) is an imaging solution that operates as a standalone device that can be used both in the lab and on the field. With this device, it is possible to acquire more data, faster from more media types without sacrificing ease-of-use or portability.

All the features found in this device, which are going to be described later in the document, can be accessed remotely through a web user interface. The web interface can be visited with the following web browsers: Google Chrome, Mozilla Firefox and Safari. Investigators will be able to manage administration/operation and participate in an investigation from any computer within the same network domain. [OpenText \(2020\)](#) Figure 9 provides a picture of the device described in this subsection, Forensic Imager TX1 manufactured by Tableau.



Figure 9: Tableau Forensic Imager TX1

Features

Features to this product are included in the datasheet added as an appendix later in the document.

4.6.3. Ditto Forensic FieldStation by CRU

Ditto Forensic FieldStation is a complete and portable toolkit for creating disk clones and images. Ditto FieldStation can be deployed by non-forensics experts and administered and operated remotely by forensics specialists. Via VPN, the Ditto FieldStation can be configured, administered, and managed via an intuitive web browser interface.

It allows the discovery, preview, and image files from hard drives and network file systems. Going further, physical imaging of complete hard drives it attained and logical imaging of specific file types from hard drives and network file systems.

A big advantage of this product is the fact that it is always completely free to keep the device updated as well as a free 3-year warranty and no annual fees. This is an important feature to take into account because of the already high prices of most of the tools

required in the Digital Forensics field. CRU (2020) Figure 10 provides a picture of the device described in this subsection, Ditto Forensic FieldStation manufactured by CRU.



Figure 10: Ditto Forensic FieldStation

Features

Features to this product are included in the datasheet added as an appendix later in the document.

CHAPTER 5

Case Study: Insider Threat - Data Leak

The practical framework will cover the case of a "*Business Data Leak*". The material used for the development of this practical case is made up of free samples/templates obtained through the Internet from various sites. The data sets used are documents with extensions .doc, .ppt and .xlsx. The analysis of the evidence will be carried out with the Autopsy software previously discussed in the document. The reason why the analysis is going to be conducted with this software it is because of its open-source nature and a vast range of utilities. It is the best choice if the election is based on price and quality. In order to be able to understand how to properly use the software in question, it was necessary to take the Training course available on the developer's website without damaging the data evidence.

The data evidence will be extracted from a .vdmk file. So as to create the case a virtual machine was required to perform the malicious actions. This virtual machine runs on Windows 10.

5.1 Description of the case

The development of the case begins with the contact by the CEO of the company *Bioerts*. The procedure is accepted by the company specialized in DFIR, *Cybersecua*. In this email, Morgan conveys his concern about a possible data leak from an accounting department employee to a competing company as shown in the following figure.

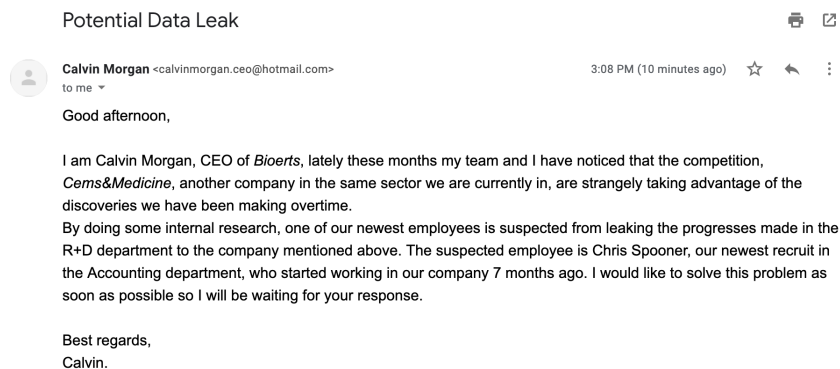


Figure 11: E-Mail received from Bioert's CEO Calvin Morgan

5.2 Assessment

5.2.1. Materials

The analysis is carried through in a MacBook Pro 13" Retina early with a 150GB Boot-Camp partition. In the following bullet list, specifications for the system are mentioned:

- Operating System: Microsoft Windows 10 Pro Education N
- Processor: Intel(R) Core(TM) i5-5257U CPU @ 2.70GHz
- RAM: 8GB
- System type: 64-bit Operating System, x64-based processor

As for the material to examine, it is extracted from a virtual machine created with VirtualBox. In the following bullet list, specifications for the system are mentioned:

- Name: Spooner_Accounting
- Operating System: Microsoft Windows 10 Pro for Workstations
- RAM: 4 GB
- System type: 64-bit Operating System, x64-based processor
- BaseBoard Product: VirtualBox 1.2

As for software, the forensics tools used in order to perform the investigation were FTK Imager (version 4.2.0) and Autopsy (version 4.14.0). FTK Imager was used to obtain a disk image to later analyze in Autopsy. The procedure carried through in the examination is explained later in the document.

5.2.2. Insider Threat: Definition and Indicators

The definition of Insider Threat includes the threats as anyone that has authorized and legitimate access to certain resources and uses this access to intentionally or unintentionally harm an organization and negatively impact the organization's critical information or systems. Insiders can be employees, vendors, partners, suppliers, etc. and according to [Verizon \(2019\)](#) there are 5 common types of dangerous insiders.

The first group comprises the disgruntled employees, these employees might be dissatisfied with several aspects in the work-field. The main reason can be the rejection in a petition for a promotion or a salary raise and poor relationships with colleagues and/or managers. The aim of this kind of insiders is to harm the organization utilizing the destruction of data or disruption of business activity.

The second group is composed of the malicious insiders, these are workers who exploit or abuse access for the theft, leakage or deletion of important company records. The contrast between these employees and the ones mentioned in the previous paragraph is their motivation. Disgruntled employees are moved by emotional response, while malicious insiders use existing privileges to access information for personal gain.

The third group comprehends the inside agents. Within the business are corporate or government agents that can be recruited, approached or persuaded by external parties to exfiltrate data. A new arriver or a trustworthy employee can be an inside agent. Their goal is to steal the intellectual secrets in return for a benefit for the competitors.

The fourth group contains regular and/or careless employees. These are employees or partners that end up misappropriating assets, breaking permissible usage measures, mismanaging information, installing unauthorized applications and utilizing unauthorized workarounds, are mistaking for malicious measures, most of which fall within the IT Shadow world. They normally possess limited access to sensitive data. They will also, either by accident or become the target of phishing, leak data or damage the business network unintentionally.

The fifth group involves third-party providers and contractors. These are business associates that risk protection through negligence, misuse or malicious access to or use of an asset. Security on sensitive data is not guaranteed in some cases due to little to no control over cybersecurity on the side of third-party providers.

The Potential Indicators of Insider Threat Activity may include:

- Aims or successful access without a valid "need-to-know" to systems and records.
- Requesting access to information apart from regular duties.
- Unusual or erratic behavior.
- Highly disgruntled attitude.
- Working at peculiar or late hours for little to no reason.
- Noticeable Unexplained economic growth or excessive indebtedness.
- Striving to disguise foreign contacts, travel, interests or suspicious activities.
- Unreported offers of financial assistance, gifts or favors by a foreign national.
- Exploitable behavior, such as criminal activity, sexual misconduct, excessive gambling, alcohol or drug abuse, or problems at work.

5.2.3. Interview with other employees

Victoria Davis - Accounting Department

The first employee interviewed by the digital forensic expert was Spooner's co-worker in the Accounting Department. Davis is a 28-year-old accountant that was employed by the company 3 years ago. Davis was the first employee that expressed concern for certain behaviors coming from Spooner. Davis stated the following:

"I never managed to establish a very close relationship with Chris. He was always a very reserved person with other employees. He was also not a very ostentatious person or that had strange behaviors. I started noticing changes two months ago. He started asking me many questions about possible projects in the company or even questions about my personal life. From that moment we established a more personal bond. Because of this, he told me that he would take a trip to the Maldives, in addition to this he acquired a really expensive car in a matter of two weeks. These last two things seemed really strange to me because in all the previous months I had not shown signs of such high purchasing power. Also, I began to notice that I was spending more time in the office than normal. When I confronted him about this, he told me that he was simply very busy with the accounting of the project that had been assigned to him, which was the most important that the company had at that time. For that reason, he was working overtime to finish his duties. I decided not to pay much attention to this because I was also involved in another very important project and sometimes, I had extra hours too, so I thought it was justified. The biggest red flag appeared at the time he commented by mistake that he had colleagues working on an important member of the competition, which is Bioerts, who just at that time had achieved exactly the same thing that

we obtained with the development of a technique that was going to get patented by Mediatrics and I started connecting the dots. The company's security department gave us instructions on how to detect possible insider threats. I detected certain patterns that were described in these briefings, so I expressed my concern to CEO Calvin Morgan." "

Ana Griffin - IT Department

the second employee interviewed by the expert was Ana Griffin, in charge of the IT department. Griffin is a 29-year-old SOC team member. Griffin stated the following:

"I have never had any type of relationship with this person, except for some meetings where the project in which he was involved was being discussed. According to things he has stated, he has never had many computer skills, except for the tools used in accounting. We have had quite short conversations, except for the one we had three months ago. We talked a little about PGP (Pretty Good Privacy), he asked me a few questions, but it was not noticeable that he didn't have much idea on the matter. I only explained to him the concepts of public and private key. Additionally, from the IT department, they informed me that they saw in the SIEM logs that there were abnormal downloads on the device he had assigned."

5.3 Acquisition: Disk Image creation with FTK Imager

This step in the investigation corresponds to the "Evidence Acquisition" phase. It is crucial because it entailed the obtaining of the evidence without altering it or tampering it. In order to create the disk in FTK the following steps are needed:

1. In the File Menu, select the "Create Disk Image" option.
2. A wizard guides the user through the process. The type of source is selected among the different options offered.

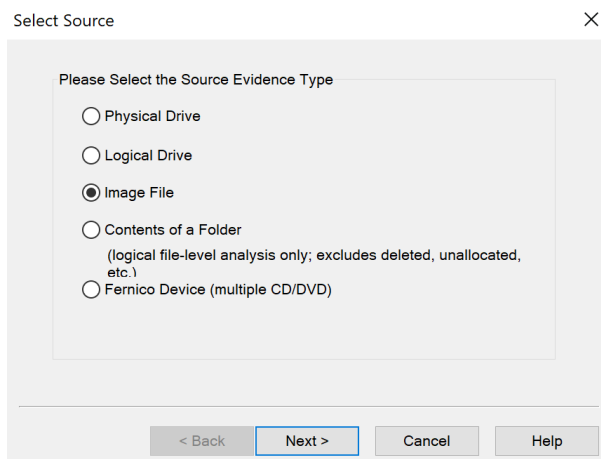


Figure 12: Select Source Wizard in FTK Imager

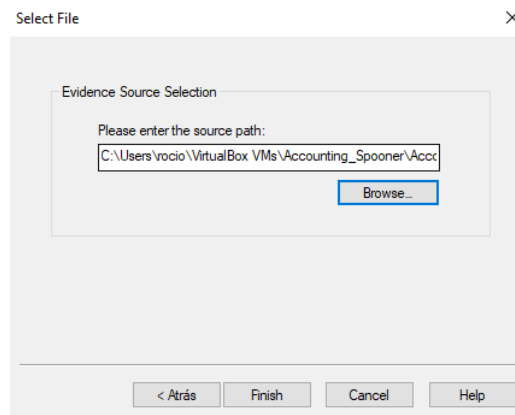


Figure 13: Select File Wizard in FTK Imager

3. After the image source is selected, the image destination type must be selected among the options offered in the wizard.

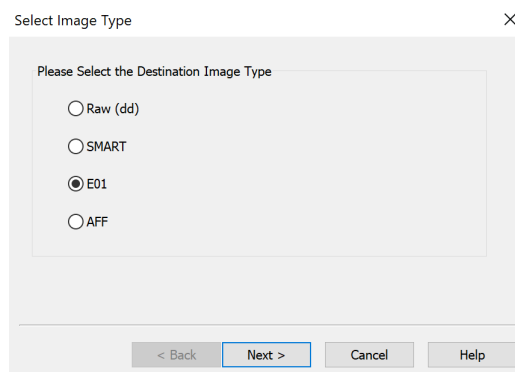


Figure 14: Select Image Type Wizard in FTK Imager

4. The investigator must fill the form with the Evidence Item Information in order to always keep track of the case.

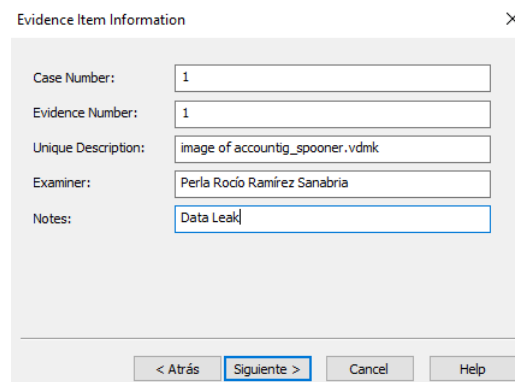


Figure 15: Evidence Item Information Wizard in FTK Imager

5. Finally, the image destination folder must be selected as well as the image filename. In this step is also possible to define the image fragment size, the compression and the use of AD encryption. It is important to keep in mind that source and destination require to be in separated storage units (i.e. different partitions)

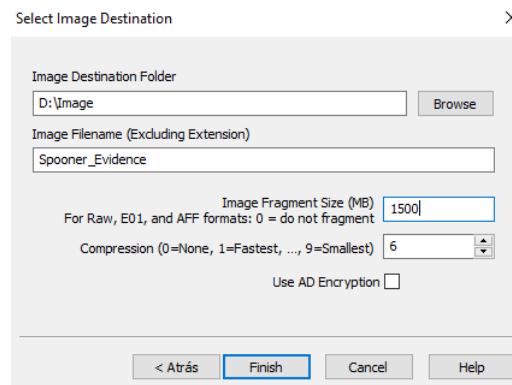


Figure 16: Select Image Destination Wizard in FTK Imager

6. After the configuration for the imaging process takes place, FTK Imager creates the image. This may take time depending on the configuration the examiner uses and the hardware capabilities of the examiner's system.

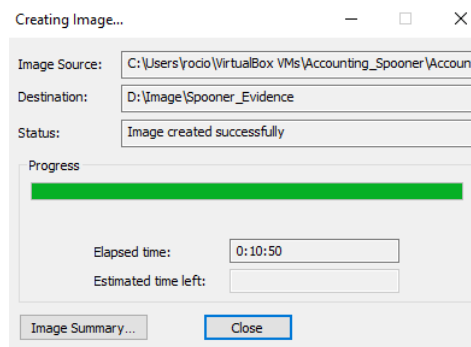


Figure 17: Creating Image process in FTK Imager

After the "Creating Image" process is performed, the application outputs the verification information to the user.

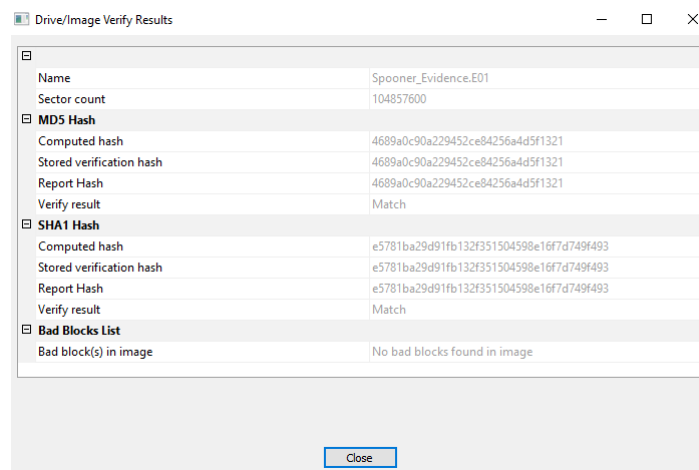


Figure 18: Drive/Image Verify Results in FTK Imager

Along with the .E01 file, a text document is generated in the destination folder. In this document, the information about the case and the image is included. It is included in the "Appendices" chapter.

5.4 Examination: Data analysis with Autopsy

The first step when conducting a digital forensics examination would be the creation of a new case as it shows in the following figure.

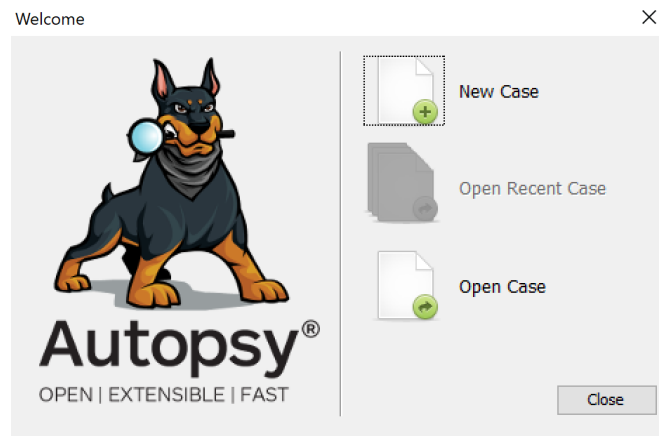


Figure 19: Initial Wizard to create a case in Autopsy

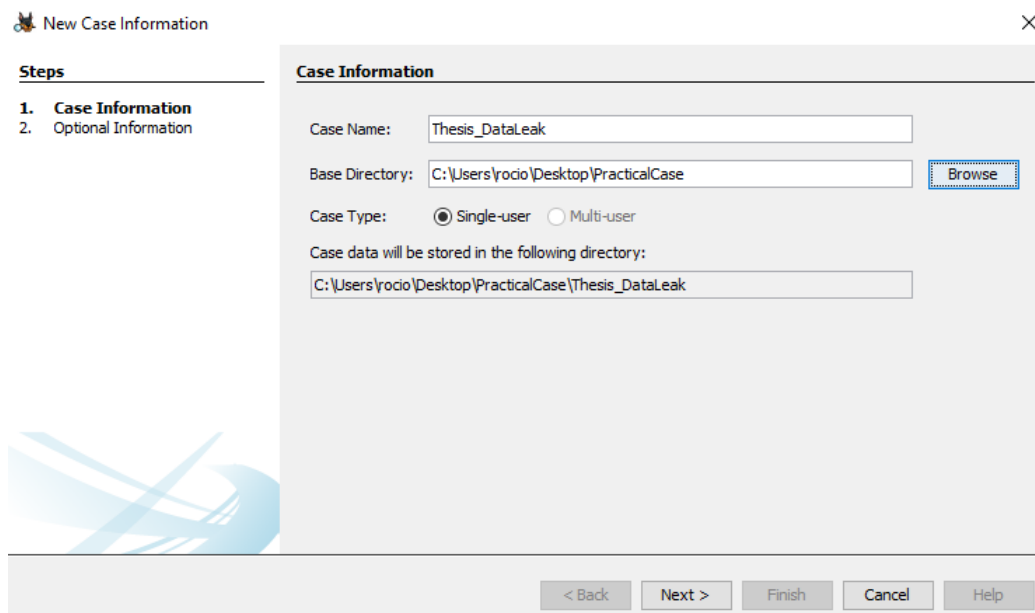


Figure 20: New Case Information Wizard in Autopsy

The next step is the addition of one or more data sources. In this case, the data source will be the image of the disk (format .E01) created with FTK Imager as previously mentioned in this document.

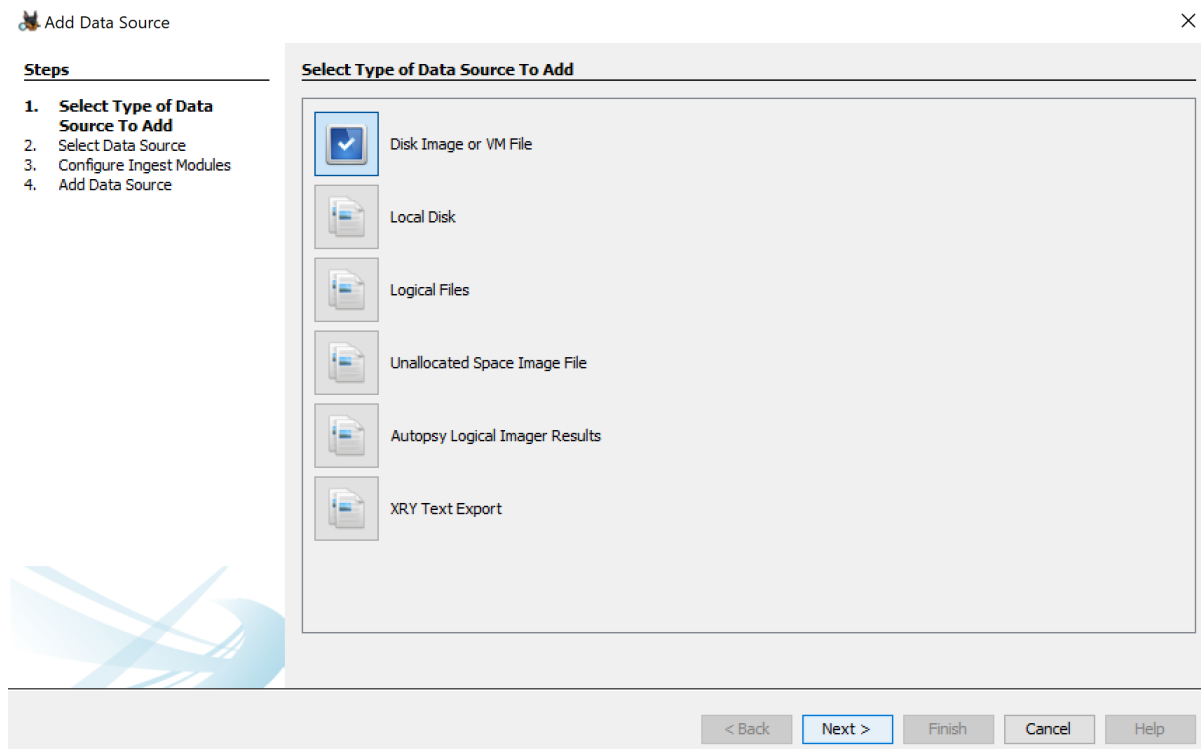


Figure 21: Add Data Source Wizard in Autopsy

In the next step, the examiner needs to select the data that will behave as the source by clicking on the "Browse" button.

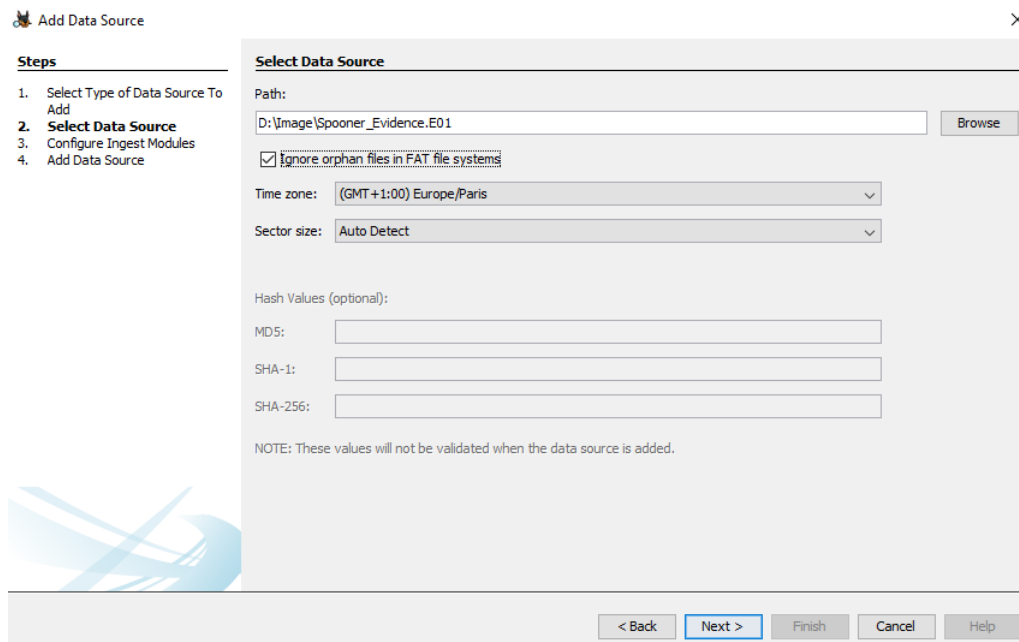


Figure 22: Select Data Source Wizard in Autopsy

As it was explained in the theoretical part of the thesis, the configuration of the Ingest Modules is necessary. These modules are the ones in charge of analyzing the data. This is the following step, depending on the demands of the examiner or the investigation per se, all of them are required or only specific ones.

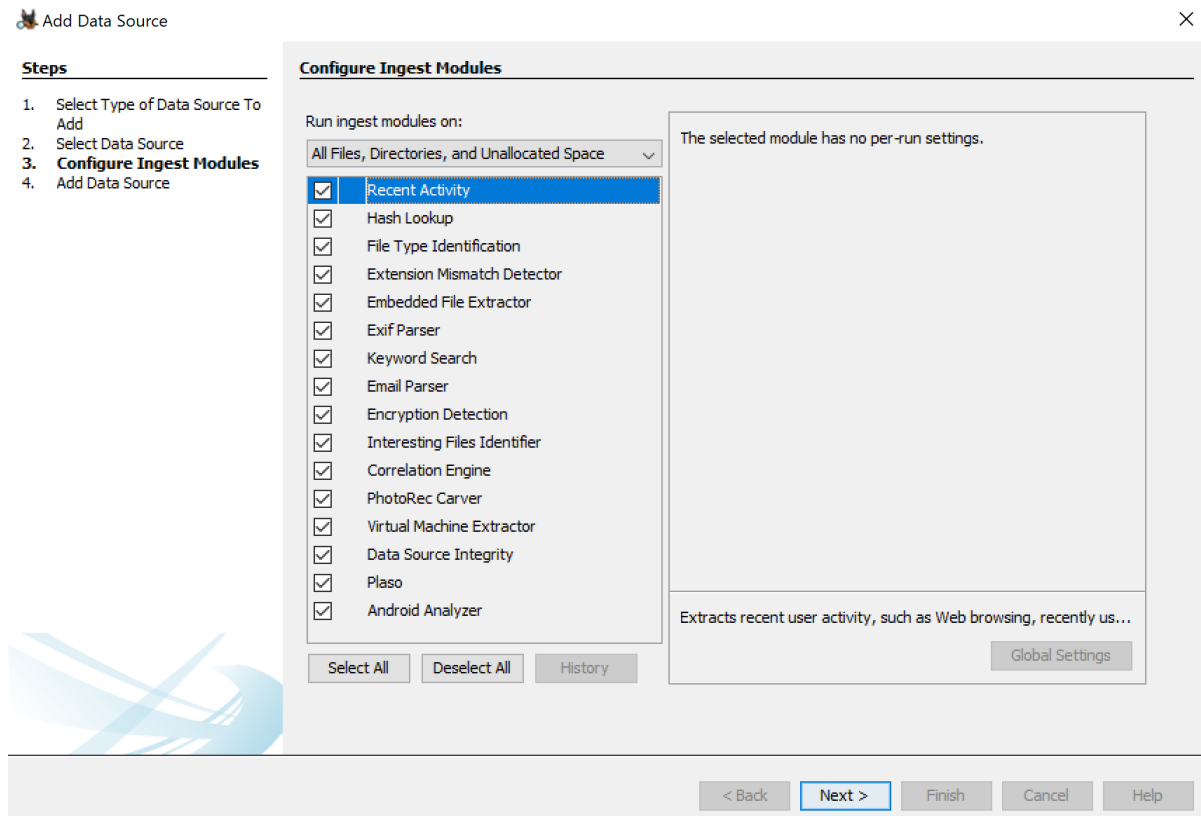


Figure 23: Ingest Modules Configuration Wizard in Autopsy

Once the data is added in the application, the analyzing process will begin as shown in the following figure.

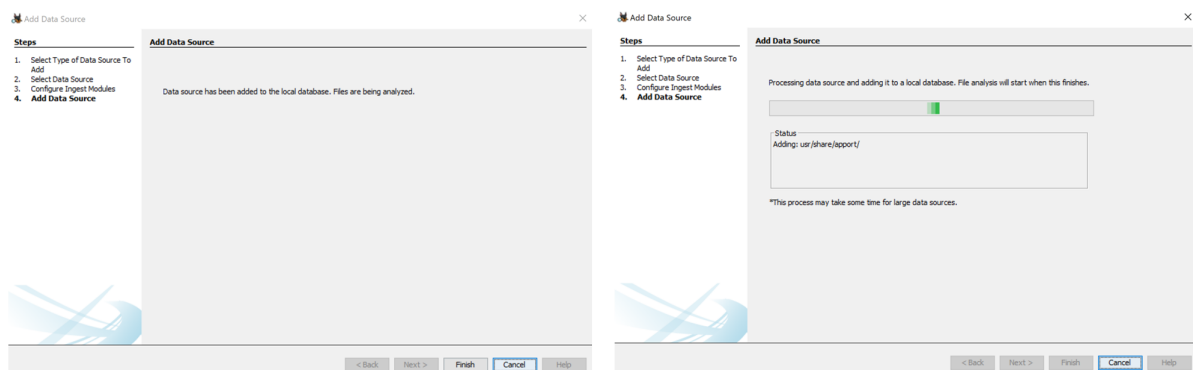


Figure 24: Adding Data Source in Autopsy

After Autopsy processes the data, the results start appearing in the Tree Viewer on the left side of the user interface. As ingest occurs, more results are available in the Tree.

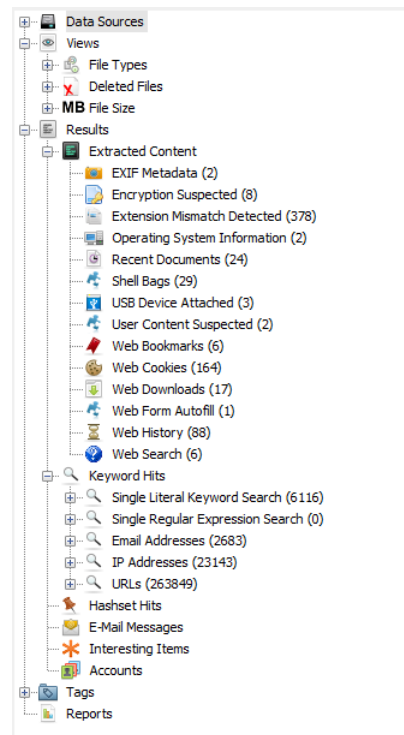


Figure 25: Tree Viewer of the case in Autopsy

The next step encompasses the examination of the different sources of evidence which can be the *Web Search*, *Web History*, *Web Downloads*, *E-mail Messages* and the *Windows Artifacts*.

5.4.1. Web Search

Source File	S	C	Domain	Text	Program Name	Date Accessed	Data Source
places.sqlite	✓		www.google.com	java jre	Firefox	2020-05-08 03:36:01 CEST	Spooner_Evidence.E01
places.sqlite	✓		www.google.com	pgp tool	Firefox	2020-05-08 03:40:53 CEST	Spooner_Evidence.E01
places.sqlite	✓		www.google.com	windows office mega	Firefox	2020-05-08 03:44:33 CEST	Spooner_Evidence.E01
places.sqlite	✓		www.google.com	winrar	Firefox	2020-05-08 03:45:51 CEST	Spooner_Evidence.E01
places.sqlite	✓		www.google.com	onedrive	Firefox	2020-05-08 03:55:32 CEST	Spooner_Evidence.E01
WebCacheV01.dat			www.bing.com	firefox	Microsoft Edge	0000-00-00 00:00:00	Spooner_Evidence.E01

Figure 26: Web Search in Autopsy

5.4.2. Web Downloads

The potentially leaked information was in the suspect's OneDrive shared folder. This information was shared with him by CEO Calvin Morgan. According to Morgan, the reason why the information was stored in that location is so that it was possible to keep a record of the changes made in the documents in addition to having them at any time. It is easy to edit given the Office Online option offered by the platform. Some guidelines required workers to modify these documents directly from the OneDrive's web application. Therefore, downloading and offline editing of these documents was strictly prohibited. This policy arises from the sensitivity of the information. Moreover, downloading additional software other than the ones installed on the device

at the time of assignment was prohibited. Systems were customized for each employee, so they already had all the necessary programs.

Source File	S	C	URL	Path	Date Accessed	Program Name	Domain
places.sqlite	✓		https://sdlc-esd.oracle.com/ESD6/35CDLJ9k98u...	C:/Users/Chris Spooner/Downloads/jre-9u251-windows-x6...	2020-05-08 03:36:35 CEST	Firefox	sdlc-esd.oracle.com
places.sqlite	✓		https://github-production-release-asset-2e65be...	C:/Users/Chris Spooner/Downloads/pgptoolgui-0.5.9.0.msi	2020-05-08 03:42:47 CEST	Firefox	github-production-release
places.sqlite	✓		http://d.winrar.es/d/103z1588870164/Vd9Nm...	C:/Users/Chris Spooner/Downloads/winrar-x64-590es.exe	2020-05-08 03:46:26 CEST	Firefox	d.winrar.es
places.sqlite	✓		https://0o5zza.dm.files.1drv.com/y4mjdPcJAw...	C:/Users/Chris Spooner/Downloads/Central_Superstore.xlsx	2020-05-08 04:07:08 CEST	Firefox	0o5zza.dm.files.1drv.com
places.sqlite	✓		https://public.dm.files.1drv.com/y4m6dX3BH5YT...	C:/Users/Chris Spooner/Downloads/confidential-projectnov...	2020-05-08 04:07:20 CEST	Firefox	public.dm.files.1drv.com
places.sqlite	✓		https://public.dm.files.1drv.com/y4mPG0jrmvfrA...	C:/Users/Chris Spooner/Downloads/R D project nov 2020.ppt	2020-05-08 04:07:44 CEST	Firefox	public.dm.files.1drv.com
places.sqlite	✓		https://public.dm.files.1drv.com/y4mGfNwzOwv3...	C:/Users/Chris Spooner/Downloads/project presentation 2...	2020-05-08 04:09:19 CEST	Firefox	public.dm.files.1drv.com
places.sqlite	✓		https://public.dm.files.1drv.com/y4mRfMqple7r...	C:/Users/Chris Spooner/Downloads/project2020.docx	2020-05-08 04:09:30 CEST	Firefox	public.dm.files.1drv.com
places.sqlite	✓		https://optima.turkuamk.fi/learning/ld19/bin/doc...	C:/Users/Chris Spooner/Downloads/Graduation_process.pptx	2020-05-08 05:35:01 CEST	Firefox	optima.turkuamk.fi
edb00001.log:Zone.Identifier							
schema.txt:Zone.Identifier							
spartan.edb:Zone.Identifier							
spartan.pat:Zone.Identifier							
MicrosoftEdgeCookiesBackup.dat:							
MicrosoftEdgeSettingsBackup.txt:							
Backup.dat:Zone.Identifier							
confidential-projectnovember 2020			https://public.dm.files.1drv.com/y4m6dX3BH5YT...				public.dm.files.1drv.com

Figure 27: Web Downloads in Autopsy

Besides downloading the files, it was noted that additionally the attacker illegally downloaded a copy of Microsoft Office 2019 as well as an installer for a PGP Tool. The illegal download could potentially infect the system due to the user's lack of skills in the field. By installing the PGP Tool, the not installing new software policy was violated as well.

5.4.3. Web History

There are relevant items in the browser's history such as the following visited pages:

Source File	S	C	URL	Date Accessed	Referrer URL
places.sqlite	✓		https://onedrive.live.com/	2020-05-08 04:05:47 CEST	https://go.microsoft.com/fwlink?LinkID=223554
places.sqlite	✓		https://onedrive.live.com/?id=root&cid=6FED9DE0BBA687...	2020-05-08 04:06:16 CEST	
places.sqlite	✓		https://onedrive.live.com/?id=%2D431191050857911992...	2020-05-08 04:06:16 CEST	https://onedrive.live.com/?id=root&cid=6FED9DE0BBA687...
places.sqlite	✓		https://0o5zza.dm.files.1drv.com/y4mjdPcJAwwtToUWg...	2020-05-08 04:07:08 CEST	https://onedrive.live.com/?id=%2D431191050857911992...
places.sqlite	✓		https://public.dm.files.1drv.com/y4m6dX3BH5TswshsBOL...	2020-05-08 04:07:20 CEST	https://onedrive.live.com/?id=%2D431191050857911992...
places.sqlite	✓		https://public.dm.files.1drv.com/y4mPG0jrmvfrARCON81hc...	2020-05-08 04:07:44 CEST	https://onedrive.live.com/?id=%2D431191050857911992...
places.sqlite	✓		https://public.dm.files.1drv.com/y4mGfNwzOwv37c0VJ_2LF...	2020-05-08 04:09:19 CEST	https://onedrive.live.com/?id=%2D431191050857911992...
places.sqlite	✓		https://public.dm.files.1drv.com/y4mRfMqple7rmdA7u5Dg...	2020-05-08 04:09:30 CEST	https://onedrive.live.com/?id=%2D431191050857911992...
places.sqlite	✓		https://outlook.live.com/mail/0/	2020-05-08 04:09:41 CEST	https://outlook.live.com/owa/0/
places.sqlite	✓		https://outlook.live.com/mail/0/inbox	2020-05-08 04:09:46 CEST	https://outlook.live.com/mail/0/
places.sqlite	✓		https://www.tuas.fi/en/	2020-05-08 05:29:34 CEST	https://www.tuas.fi/
places.sqlite	✓		https://sts.turkuamk.fi/adfs/ls?version=1.0&action=signi...	2020-05-08 05:29:47 CEST	https://messi.turkuamk.fi/
places.sqlite	✓		https://sts.turkuamk.fi/adfs/ls?wa=wsignin1.0&wtrealm=u...	2020-05-08 05:30:35 CEST	https://messi.turkuamk.fi/_trust/default.aspx?ReturnUrl=...
places.sqlite	✓		https://messi.turkuamk.fi/Sivut/messi_etusivu.aspx	2020-05-08 05:30:37 CEST	https://messi.turkuamk.fi/
places.sqlite	✓		https://messi.turkuamk.fi/english/Pages/frontpage.aspx	2020-05-08 05:32:09 CEST	https://messi.turkuamk.fi/english
places.sqlite	✓		https://optima.turkuamk.fi/	2020-05-08 05:33:14 CEST	http://optima.turkuamk.fi/
places.sqlite	✓		https://haka.funet.fi/shibboleth/WAYF?entityID=https%3...	2020-05-08 05:33:36 CEST	https://optima.turkuamk.fi/shibboleth/shiblogin
places.sqlite	✓		https://dp1.turkuamk.fi/ldp/profile/SAML2/Redirect/SSO?js...	2020-05-08 05:33:44 CEST	https://dp1.turkuamk.fi/ldp/profile/SAML2/Redirect/SSO?js...
places.sqlite	✓		https://dp1.turkuamk.fi/ldp/profile/SAML2/Redirect/SSO?js...	2020-05-08 05:33:57 CEST	https://dp1.turkuamk.fi/ldp/profile/SAML2/Redirect/SSO?js...
places.sqlite	✓		https://optima.turkuamk.fi/learning/ld19/bin/user?and=19...	2020-05-08 05:34:11 CEST	https://optima.turkuamk.fi/loginmenu
places.sqlite	✓		https://optima.turkuamk.fi/learning/ld19/bin/documents/24...	2020-05-08 05:35:01 CEST	https://optima.turkuamk.fi/learning/ld19/bin/user?rand=19...

Figure 28: Web History in Autopsy

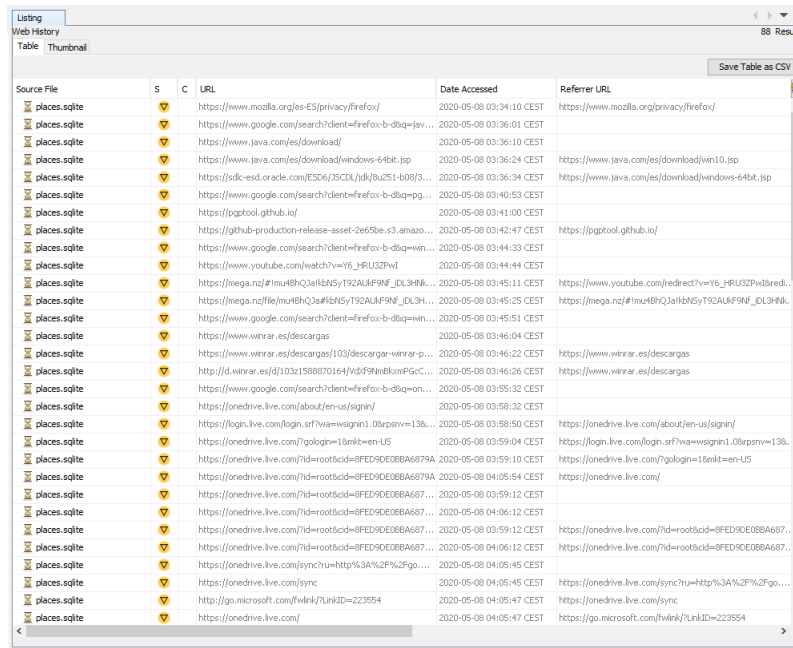


Figure 29: Web History in Autopsy

It is essential to note that for this case study the competitor’s website was represented with the URLs for <https://www.tuas.fi> and <https://www.optima.turkuamk.fi>. These two websites were used in order to pretend the attacker had access to the competitor’s site and other domains of it, such as Optima that required a sign-in. After signing in, the attacker also downloaded a file from the latter website.

5.4.4. Windows Artifacts

Open/Save MRU

This key keeps track of the list of recently opened or saved files via Windows Explorer-style dialog boxes (Open/Save dialog box). This includes web browsers like Internet Explorer or Firefox and also a majority of commonly used applications.

Location:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

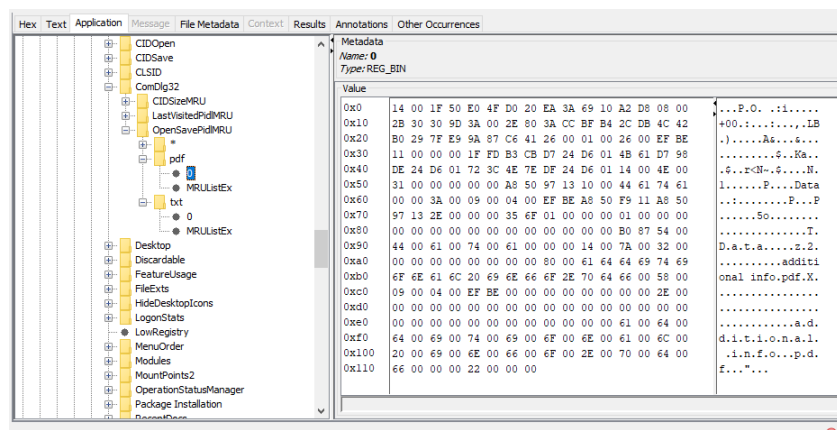


Figure 30: Open/Save MRU Artifact in Autopsy

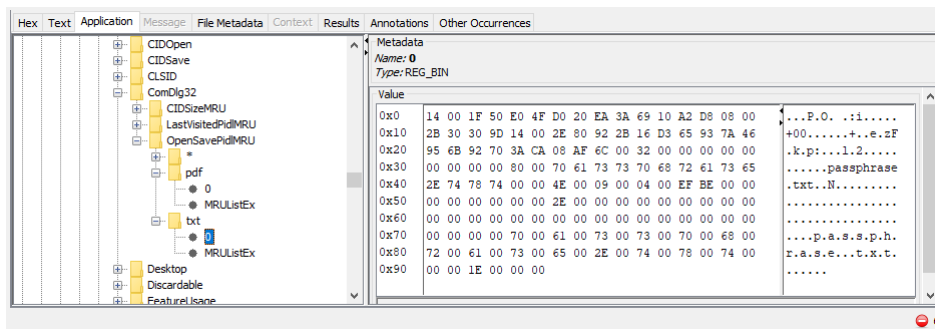


Figure 31: Open/Save MRU Artifact in Autopsy

Windows 10 Timeline

It is a feature that keeps a chronological record of the tasks performed in a PC. It includes the visited websites, edited Office documents and used multimedia files. This data is recorded in a SQLite database. It is very important not to confuse this with the "Timeline" created by different digital forensic tools.

Location:

C:\Users\<profile>\AppData\Local\ConnectedDevices Platform\L.<profile>\ActivitiesCache.db

This database is composed of the master table, along with seven tables. These tables are listed in the following figure:

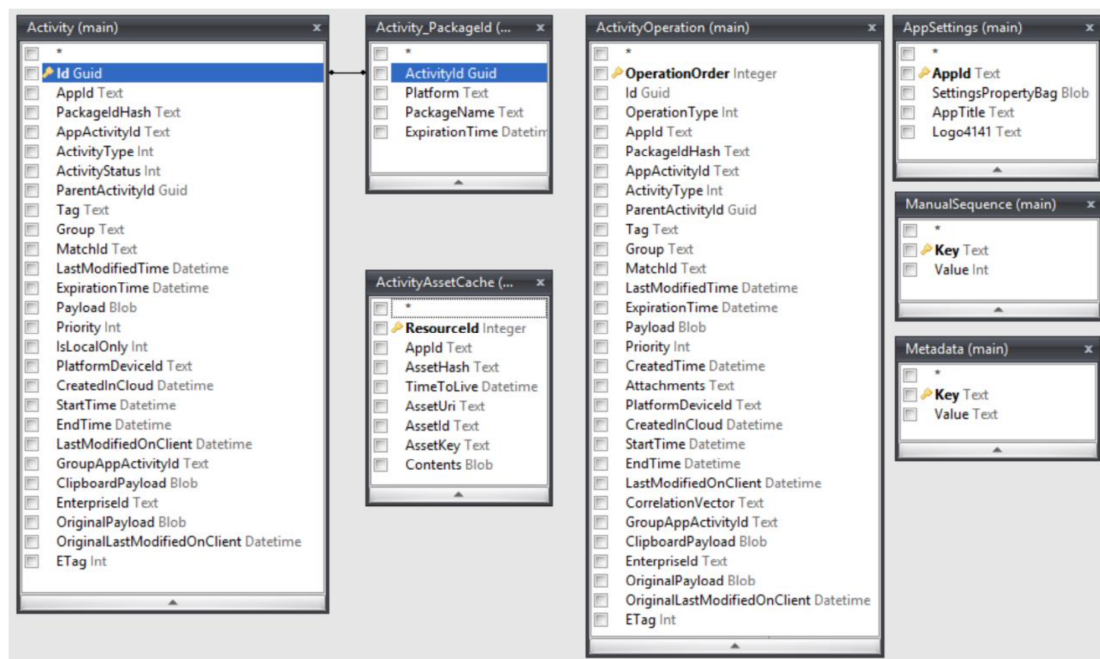


Figure 32: Database:ActivitiesCache.db schema

Each of these tables store information that is relevant to the system. There are three that store information regarding user activities: 'Activity', 'ActivityOperation' and 'Activity_PackageID'. When there is any new application execution, a new entry to the table 'Activity' is added and subsequently, it results in relevant entries in the 'Activity_PackageID' table.

In the following figures, it is possible to establish the relationship between these three tables along with the changes that happen when a new operation occurs in the system.

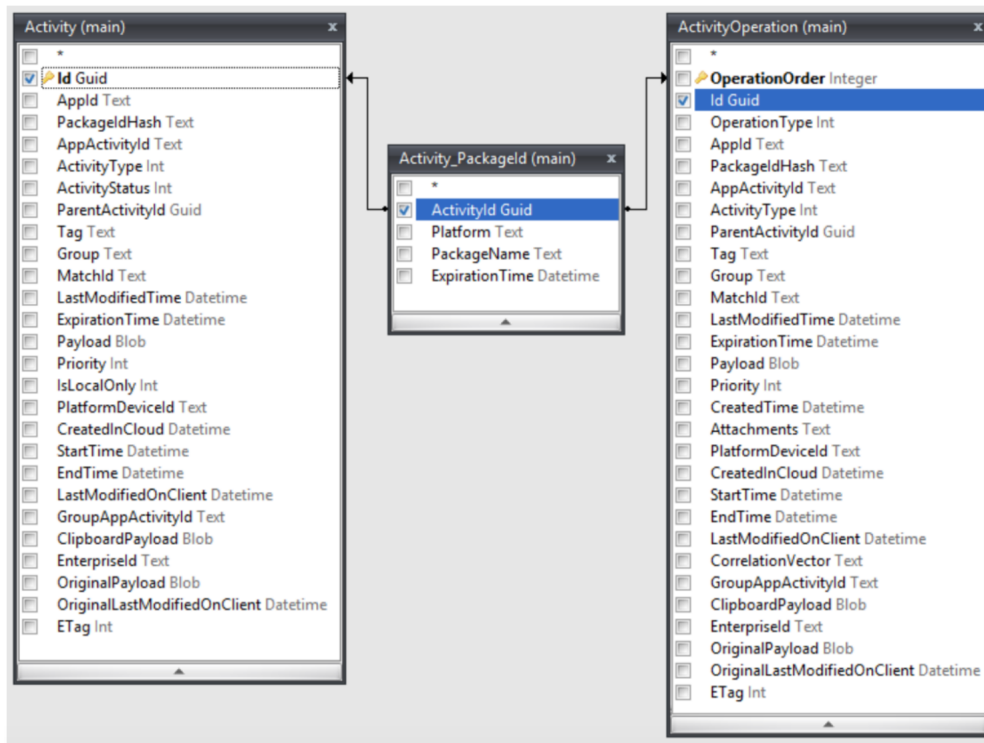


Figure 33: User information tables: 'Activity', 'ActivityOperation' and 'Activity_PackageID'

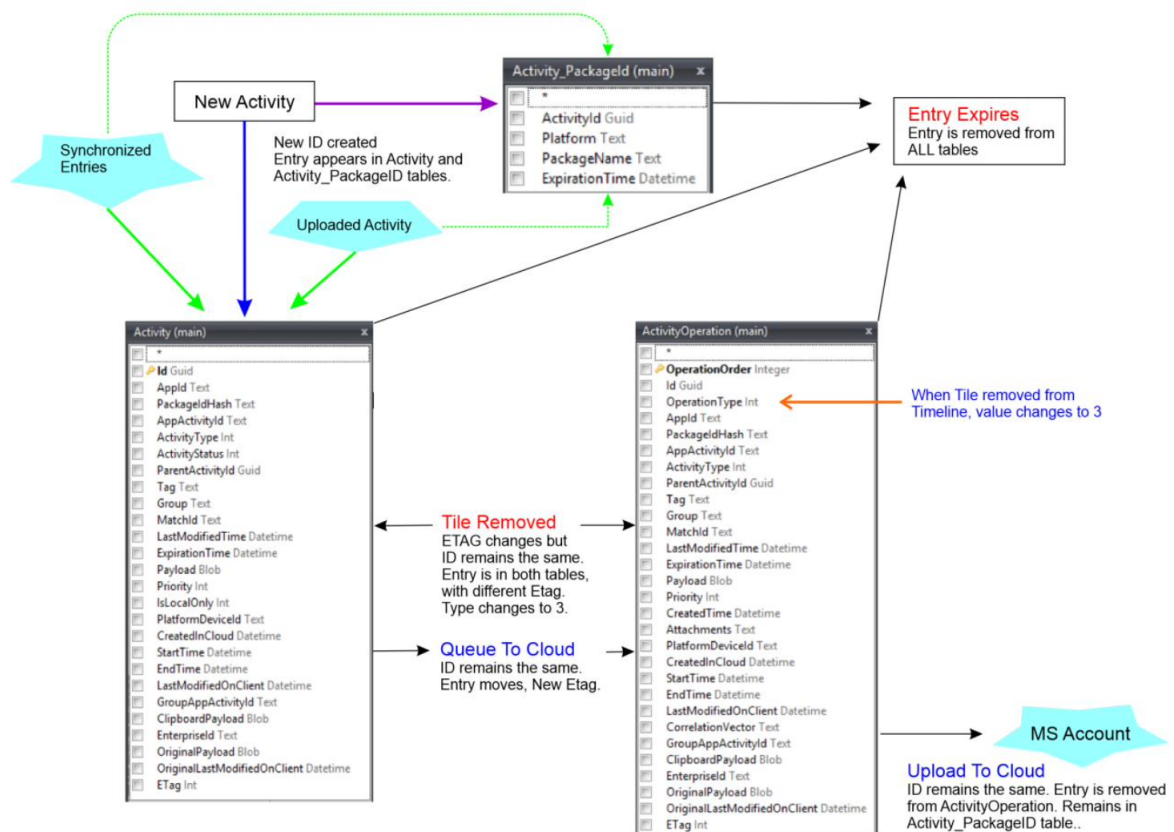


Figure 34: Windows Timeline Process

It is important to understand the data in these tables in order to know what the user executed in the system. The 'Activity' table has a unique ID for each entry/user activity, this value can be seen in the table 'Activity_PackageID' as well. The number of times the ID appears in the second table will depend on the 'Platform' field. These are the values the examiner needs to check to understand the user's actions. [Katsavounidis \(2018\)](#) Moreover, the 'Metadata' table includes the date/time the database was created by the system. While the 'ManualSequence' table shows the last Activity (ETAG) recorded in the database.

This artifact can be inspected with a browser for SQLite databases. For the sake of this case study, DB Browser (SQLite) was the tool chosen to perform this task. In order to take a better look at the data, the tables were exported as CSV files that could be visualized in Microsoft Excel. Relevant data was found in the tables 'Activity' and 'Activity_PackageID'. In both tables was able to determine that the attacker followed these steps:

1. Opened locally the original files downloaded from the OneDrive shared folder.
2. Renamed the files and modified one of the Word documents to add clarifying notes.
3. Encrypted the files with the PGP Tool, which requires Java Runtime Environment 1.8+ to function.
4. Used the Outlook application to send the encrypted files, the keys and the passphrase.

A	B	C	D
1	AppId	PackageIDHash	AppActivityId
2	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com"},{"j8HEKtCo07y04FdkYAYFQ52/YN8IECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)confidential-projectnovember2020.d		
3	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com"},{"j8HEKtCo07y04FdkYAYFQ52/YN8IECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)confidential-projectnovember2020.d		
4	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows.zHh/HcVcSbDVFNBfICT+ORMMdNIECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)project presentation 2020.ppt		
5	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows.zHh/HcVcSbDVFNBfICT+ORMMdNIECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)project presentation 2020.ppt		
6	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com"},{"j8HEKtCo07y04FdkYAYFQ52/YN8IECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)project2020.docx		
7	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com"},{"j8HEKtCo07y04FdkYAYFQ52/YN8IECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)project2020.docx		
8	[{"application":"Microsoft.Office.EXCEL.EXE.15","platform":"windows_win32"},{"application":"excel.activity.windows.com"},{"platf06wuk4HwX9P4BRFNtIWeMT17a/ECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)Central_Superstore.xlsx		
9	[{"application":"Microsoft.Office.EXCEL.EXE.15","platform":"windows_win32"},{"application":"excel.activity.windows.com"},{"platf06wuk4HwX9P4BRFNtIWeMT17a/ECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)Central_Superstore.xlsx		
10	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows.zHh/HcVcSbDVFNBfICT+ORMMdNIECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)R+D project nov 2020.ppt		
11	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows.zHh/HcVcSbDVFNBfICT+ORMMdNIECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)R+D project nov 2020.ppt		

Figure 35: Table 'Activity': Opening original downloaded files

A	B	C	D
1	AppId	PackageIDHash	AppActivityId
14	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com"},{"j8HEKtCo07y04FdkYAYFQ52/YN8IECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)confidential-projectnovember2020.d		
15	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com"},{"j8HEKtCo07y04FdkYAYFQ52/YN8IECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)random 2.docx		
16	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com"},{"j8HEKtCo07y04FdkYAYFQ52/YN8IECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)random 2.docx		
17	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com"},{"j8HEKtCo07y04FdkYAYFQ52/YN8IECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)random 2.docx		
18	[{"application":"C:\CSA40EF-ADF8-4BFC-874A-CDF2E0B9F8E1\Adobe\Acrobat DC\Acrobat\Acrobat.exe","platform":"window.NPP/igZwWmMfImlLols7ZF/ECB32AF3-1440-4086-94E3-5311F97F89C4}		
19	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows.zHh/HcVcSbDVFNBfICT+ORMMdNIECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)random 3.ppt		
20	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows.zHh/HcVcSbDVFNBfICT+ORMMdNIECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)random 3.ppt		
21	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows.zHh/HcVcSbDVFNBfICT+ORMMdNIECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)random 5.ppt		
22	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows.zHh/HcVcSbDVFNBfICT+ORMMdNIECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)random 5.ppt		
23	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com"},{"j8HEKtCo07y04FdkYAYFQ52/YN8IECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)random 4.docx		
24	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com"},{"j8HEKtCo07y04FdkYAYFQ52/YN8IECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)random 4.docx		
25	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com"},{"j8HEKtCo07y04FdkYAYFQ52/YN8IECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)random 2.docx		
26	[{"application":"C:\CSA40EF-ADF8-4BFC-874A-CDF2E0B9F8E1\Adobe\Acrobat DC\Acrobat\Acrobat.exe","platform":"window.NPP/igZwWmMfImlLols7ZF/ECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)additional info.pdf		
27	[{"application":"C:\CSA40EF-ADF8-4BFC-874A-CDF2E0B9F8E1\Adobe\Acrobat DC\Acrobat\Acrobat.exe","platform":"window.NPP/igZwWmMfImlLols7ZF/ECB32AF3-1440-4086-94E3-5311F97F89C4}(Local Downloads)additional info.pdf		

Figure 36: Table 'Activity': Opening renamed files and modifying 'random 2'

A	B	C	D
1	AppId	PackageIDHash	AppActivityId
34	[{"application":"[6D809377-6AFO-444B-8957-A377F02200E]\Java\jdk-11.0.6\bin\javaw.exe","platform":"x_exe_path"},{"apBUp+hoZPTHeW3RyOCofNlgN1h/w/ECB32AF3-1440-4086-94E3-5311F97F89C4}		
35	[{"application":"[6D809377-6AFO-444B-8957-A377F02200E]\Java\jdk-11.0.6\bin\javaw.exe","platform":"x_exe_path"},{"apBUp+hoZPTHeW3RyOCofNlgN1h/w/ECB32AF3-1440-4086-94E3-5311F97F89C4}		
36	[{"application":"[6D809377-6AFO-444B-8957-A377F02200E]\Java\jdk-11.0.6\bin\javaw.exe","platform":"x_exe_path"},{"apBUp+hoZPTHeW3RyOCofNlgN1h/w/ECB32AF3-1440-4086-94E3-5311F97F89C4}		
37	[{"application":"[6D809377-6AFO-444B-8957-A377F02200E]\Notepad++\notepad++.exe","platform":"windows_win32"},{"api5/SxQ6sRKNX7m8mIluYvWYh+NI/ECB32AF3-1440-4086-94E3-5311F97F89C4}		

Figure 37: Table 'Activity': Encryption with PGP Tool

A	B	C	D
1	AppId	PackageIDHash	AppActivityId
30	[{"application":"Microsoft.Office.OUTLOOK.EXE.15","platform":"windows_win32"},{"application":"Microsoft.Office.OUTLOOK.EXE1OCpK4J4YERQguAB/YhUymAfoC/ECB32AF3-1440-4086-94E3-5311F97F89C4}		
31	[{"application":"Microsoft.Office.OUTLOOK.EXE.15","platform":"windows_win32"},{"application":"Microsoft.Office.OUTLOOK.EXE1OCpK4J4YERQguAB/YhUymAfoC/ECB32AF3-1440-4086-94E3-5311F97F89C4}		

Figure 38: Table 'Activity': Outlook usage

The same information can be found in the second table mentioned previously.

#	A	B	C	D	E	F	G	H
5824	...	host		1592233987				
5825	...	x_exe_path	{6d809377-6afo-444b-8957-a3773f02200e}\java\jdk-11.0.6\bin\javaw.exe	1592233990				
5826	...	x_exe_path	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\java\jdk-11.0.6\bin\javaw.exe	1592233990				
5827	...	packageid	{6d809377-6afo-444b-8957-a3773f02200e}\java\jdk-11.0.6\bin\javaw.exe	1592233990				
5828	...	host		1592233990				
5829	...	x_exe_path	{6d809377-6afo-444b-8957-a3773f02200e}\java\jdk-11.0.6\bin\javaw.exe	1592234010				
5830	...	x_exe_path	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\java\jdk-11.0.6\bin\javaw.exe	1592234010				
5831	...	packageid	{6d809377-6afo-444b-8957-a3773f02200e}\java\jdk-11.0.6\bin\javaw.exe	1592234010				
5832	...	host		1592234010				
5833	...	windows_win32	{6d809377-6afo-444b-8957-a3773f02200e}\notepad++\notepad++.exe	1592234008				
5834	...	windows_win32	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\notepad++\notepad++.exe	1592234008				
5835	...	packageid	{6d809377-6afo-444b-8957-a3773f02200e}\notepad++\notepad++.exe	1592234008				
5836	...	host		1592234008				
5837	...	windows_win32	microsoft.windows.explorer	1592234198				
5838	...	packageid	microsoft.windows.explorer	1592234198				
5839	...	host		1592234198				
5840	...	windows_win32	microsoft.office.winword.exe.15	1592234190				
5841	...	host	word.activity.windows.com	1592234190				
5842	...	windows_win32	microsoft.office.winword.exe.15	1592234190				
5843	...	host	word.activity.windows.com	1592234190				
5844	...	packageid	microsoft.office.winword.exe.15	1592234190				
5845	...	windows_win32	microsoft.office.powerpnt.exe.15	1592234190				
5846	...	host	powerpoint.activity.windows.com	1592234190				
5847	...	windows_win32	microsoft.office.powerpnt.exe.15	1592234192				
5848	...	host	powerpoint.activity.windows.com	1592234192				
5849	...	packageid	microsoft.office.powerpnt.exe.15	1592234192				
5850	...	windows_win32	microsoft.office.powerpnt.exe.15	1592234192				
5851	...	host	powerpoint.activity.windows.com	1592234192				
5852	...	windows_win32	microsoft.office.powerpnt.exe.15	1592234192				

Figure 39: Table 'Activity_PackageID'

#	A	B	C	D	E	F	G	H
5953	...	host	word.activity.windows.com	1592235316				
5954	...	windows_win32	microsoft.office.winword.exe.15	1592235317				
5955	...	host	word.activity.windows.com	1592235317				
5956	...	packageid	microsoft.office.winword.exe.15	1592235317				
5957	...	windows_win32	microsoft.office.winword.exe.15	1592235337				
5958	...	host	word.activity.windows.com	1592235337				
5959	...	packageid	microsoft.office.winword.exe.15	1592235337				
5960	...	windows_win32	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\adobe\acrobat dc\acrobat\acrobat.exe	1592235340				
5961	...	windows_win32	{6d809377-6afo-444b-8957-a3773f02200e}\adobe\acrobat dc\acrobat\acrobat.exe	1592235340				
5962	...	host		1592235340				
5963	...	windows_win32	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\adobe\acrobat dc\acrobat\acrobat.exe	1592235342				
5964	...	windows_win32	{6d809377-6afo-444b-8957-a3773f02200e}\adobe\acrobat dc\acrobat\acrobat.exe	1592235342				
5965	...	packageid	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\adobe\acrobat dc\acrobat\acrobat.exe	1592235342				
5966	...	host		1592235342				
5967	...	windows_win32	microsoft.windows.explorer	1590248151				
5968	...	packageid	microsoft.windows.explorer	1590248151				
5969	...	host		1590248151				
5970	...	windows_win32	microsoft.windows.explorer	1590248175				
5971	...	packageid	microsoft.windows.explorer	1590248175				
5972	...	host		1590248175				
5973	...	windows_win32	microsoft.windows.explorer	1590248315				
5974	...	packageid	microsoft.windows.explorer	1590248315				
5975	...	host		1590248315				
5976	...	windows_win32	microsoft.office.outlook.exe.15	1592235573				
5977	...	host		1592235573				
5978	...	windows_win32	microsoft.office.outlook.exe.15	1592235587				
5979	...	packageid	microsoft.office.outlook.exe.15	1592235587				
5980	...	host		1592235587				
5981	...							

Figure 40: Table 'Activity_PackageID'

Last-Visited MRU

Works in tune with the OpenSaveMRU key by tracking the executable used to open the listed files in the previously mentioned key. Moreover, the directory that contains the last file that was accessed in tracked as well.

Location:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPID1MRU

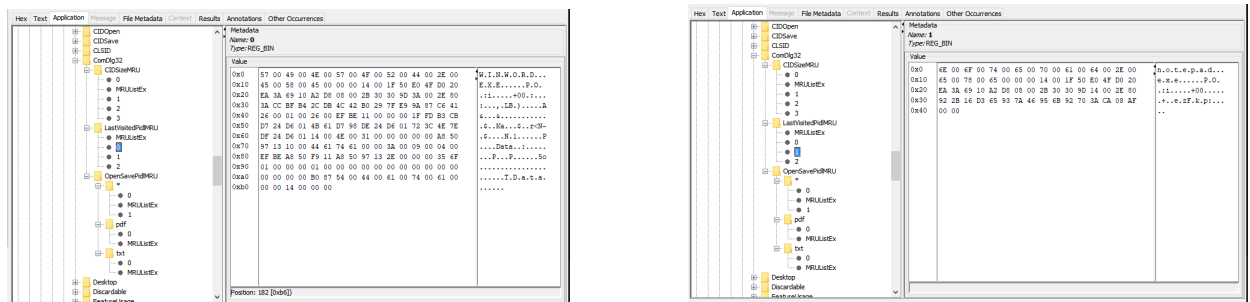


Figure 41: Last-Visited MRU Artifact in Autopsy

Shortcut (LNK) Files

These are shortcut files that are automatically created by Windows. It works as a pointing reference to a file, application or directory. They are generated when opening local or remote files and documents.

Primary Locations:

C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\
 C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\

Name	S	C	Modified Time	Change Time	Access Time	Created Time
[current folder]			2020-05-08 05:37:43 CEST	2020-05-08 05:37:43 CEST	2020-05-08 05:37:43 CEST	2020-05-08 03:2
[parent folder]			2020-05-08 03:29:19 CEST	2020-05-08 03:29:19 CEST	2020-05-08 05:06:55 CEST	2020-05-08 03:2
AutomaticDestinations			2020-05-08 05:09:51 CEST	2020-05-08 05:09:51 CEST	2020-05-08 05:11:05 CEST	2020-05-08 03:2
CustomDestinations			2020-05-08 05:37:28 CEST	2020-05-08 05:37:28 CEST	2020-05-08 05:37:28 CEST	2020-05-08 03:2
additional.info.lnk			2020-05-08 04:29:23 CEST	2020-05-08 04:29:23 CEST	2020-05-08 04:29:23 CEST	2020-05-08 04:2
Central_Superstore.lnk			2020-05-08 04:17:07 CEST	2020-05-08 04:17:07 CEST	2020-05-08 04:17:07 CEST	2020-05-08 04:0
confidential-projectnovember2020.lnk			2020-05-08 04:37:50 CEST	2020-05-08 04:37:50 CEST	2020-05-08 04:37:50 CEST	2020-05-08 04:0
Data.lnk			2020-05-08 04:37:51 CEST	2020-05-08 04:37:51 CEST	2020-05-08 04:37:51 CEST	2020-05-08 04:1
desktop.ini			2020-05-08 03:28:58 CEST	2020-05-08 03:28:58 CEST	2020-05-08 04:37:48 CEST	2020-05-08 03:2
Downloads.lnk			2020-05-08 05:37:42 CEST	2020-05-08 05:37:42 CEST	2020-05-08 05:37:42 CEST	2020-05-08 03:4
Graduation_process.lnk			2020-05-08 05:35:02 CEST	2020-05-08 05:35:02 CEST	2020-05-08 05:35:02 CEST	2020-05-08 05:3
https--onedrive.live.com-syncru=http%3A%2F%2Fgo.microsoft.c...			2020-05-08 04:05:37 CEST	2020-05-08 04:05:37 CEST	2020-05-08 04:05:37 CEST	2020-05-08 04:0
Microsoft Office 2019.rar.lnk			2020-05-08 03:46:51 CEST	2020-05-08 03:46:51 CEST	2020-05-08 04:52:50 CEST	2020-05-08 03:4
ms-gamingoverlay--kgjcheck-.lnk			2020-05-08 03:48:43 CEST	2020-05-08 03:48:43 CEST	2020-05-08 04:52:50 CEST	2020-05-08 03:4
Normal.lnk			2020-05-08 05:37:42 CEST	2020-05-08 05:37:42 CEST	2020-05-08 05:37:42 CEST	2020-05-08 04:3
odopen--unlockVault-accounttype=personal.lnk			2020-05-08 05:09:51 CEST	2020-05-08 05:09:51 CEST	2020-05-08 05:09:51 CEST	2020-05-08 04:3
passphrase.lnk			2020-05-08 04:44:03 CEST	2020-05-08 04:44:03 CEST	2020-05-08 04:44:03 CEST	2020-05-08 04:4
project presentation 2020.lnk			2020-05-08 04:20:35 CEST	2020-05-08 04:20:35 CEST	2020-05-08 04:20:35 CEST	2020-05-08 04:0
project2020.lnk			2020-05-08 05:37:42 CEST	2020-05-08 05:37:42 CEST	2020-05-08 05:37:42 CEST	2020-05-08 04:0
R+D project nov 2020.lnk			2020-05-08 04:20:50 CEST	2020-05-08 04:20:50 CEST	2020-05-08 04:20:50 CEST	2020-05-08 04:0
Templates.lnk			2020-05-08 05:37:43 CEST	2020-05-08 05:37:43 CEST	2020-05-08 05:37:43 CEST	2020-05-08 04:3
The Internet.lnk			2020-05-08 05:09:52 CEST	2020-05-08 05:09:52 CEST	2020-05-08 05:09:52 CEST	2020-05-08 03:4

Figure 42: Shortcut (LNK) FilesArtifact in Autopsy

Name	Date modified	Type	Size
AutomaticDestinations	5/14/2020 12:48 PM	File folder	
CustomDestinations	5/14/2020 12:48 PM	File folder	
additional.info	5/14/2020 12:48 PM	Shortcut	1 KB
additional.info.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
Central_Superstore	5/14/2020 12:48 PM	Shortcut	1 KB
Central_Superstore.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
confidential-projectnovember2020	5/14/2020 12:48 PM	Shortcut	1 KB
confidential-projectnovember2020.lnk-sl...	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
Data	5/14/2020 12:48 PM	Shortcut	1 KB
desktop	5/14/2020 12:48 PM	Configuration sett...	1 KB
Downloads	5/14/2020 12:48 PM	Shortcut	1 KB
Graduation_process	5/14/2020 12:48 PM	Shortcut	1 KB
Graduation_process.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
https--onedrive.live.com-syncru=http%3...	5/14/2020 12:48 PM	Shortcut	2 KB
https--onedrive.live.com-syncru=http%3...	5/14/2020 12:48 PM	LNK-SLACK File	3 KB
Microsoft Office 2019.rar	5/14/2020 12:48 PM	Shortcut	1 KB
Microsoft Office 2019.rar.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
ms-gamingoverlay--kgjcheck-	5/14/2020 12:48 PM	Shortcut	1 KB
Normal	5/14/2020 12:48 PM	Shortcut	2 KB
Normal.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	3 KB
odopen--unlockVault-accounttype=pers...	5/14/2020 12:48 PM	Shortcut	1 KB
passphrase	5/14/2020 12:48 PM	Shortcut	1 KB
passphrase.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
project presentation 2020	5/14/2020 12:48 PM	Shortcut	1 KB
project presentation 2020.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
project2020	5/14/2020 12:48 PM	Shortcut	1 KB
project2020.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
R+D project nov 2020	5/14/2020 12:48 PM	Shortcut	1 KB
R+D project nov 2020.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
Templates	5/14/2020 12:48 PM	Shortcut	1 KB
Templates.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
The Internet	5/14/2020 12:48 PM	Shortcut	1 KB

Figure 43: LNK Files extracted from Autopsy in the investigator's system

5.4.5. E-Mail Messages

Unfortunately, Autopsy was not able to obtain the messages sent by the attacker, but since the account belongs to the company, the CEO authorized the investigator to access the account with its credentials. The messages were sent to another Gmail account, under the name of the `randomuserthesis@gmail.com`. In these e-mails, the leaked content was found as well.

Figure 44 illustrates the e-mail sent by the attacker with the encrypted data.

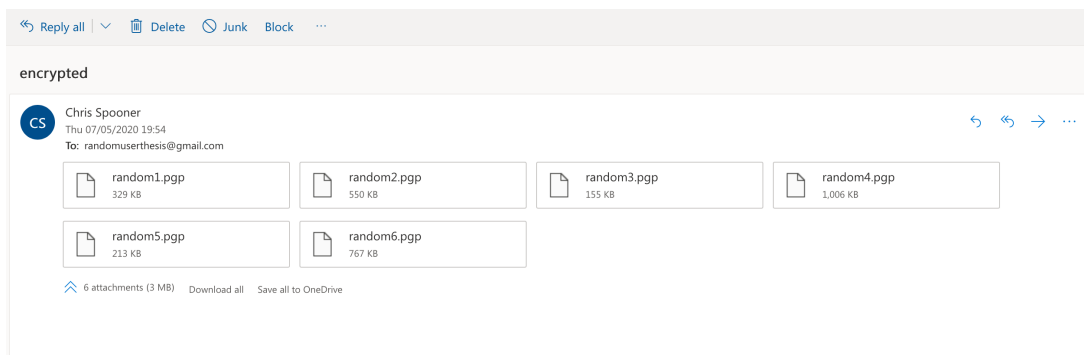


Figure 44: Sent E-Mail Message by the suspect: Encrypted Data

Figure 45 illustrates the e-mail sent by the attacker with the public and private keys for encryption.

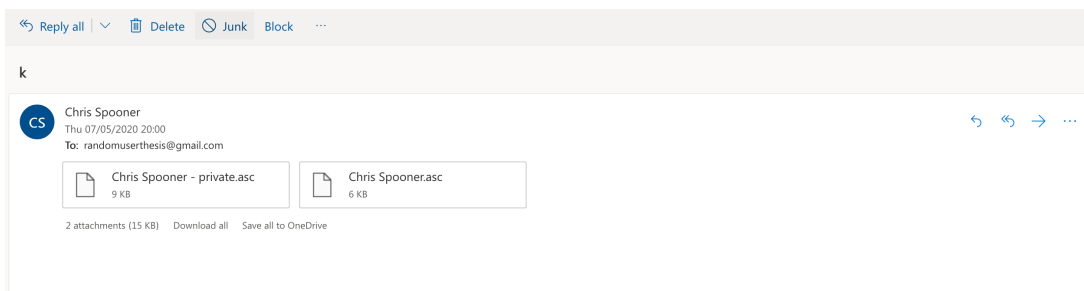


Figure 45: Sent E-Mail Message by the suspect: Public and Private Keys

Figure 46 illustrates the e-mail sent by the attacker with the passphrase for the creation of the keys sent in previous figure.

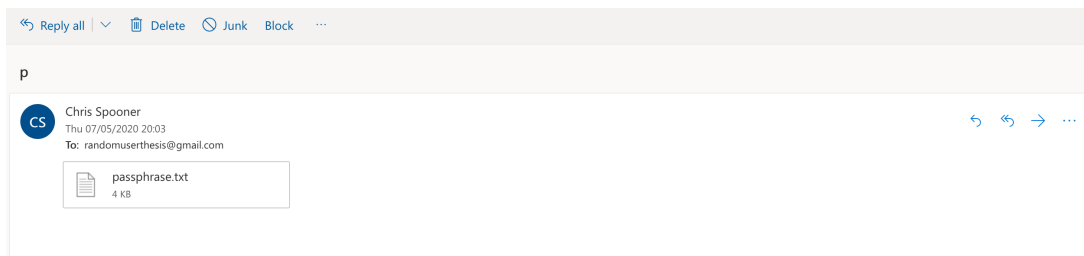


Figure 46: Sent E-Mail Message by the suspect: Passphrase

5.4.6. Tags

When searching for files downloaded by the suspect, the last basic step is where tagging occurs. This is useful to keep track of the different pieces of evidence throughout the in-

investigation and include them in the report that is generated by the software itself. Figure 47 illustrates the tags added in the case in the software Autopsy.

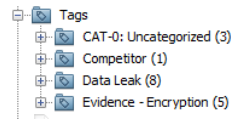


Figure 47: Tags in Autopsy

After digging into all the possible sources of evidence in the system, it was possible to export pictures and videos to the system where Autopsy is locally running.

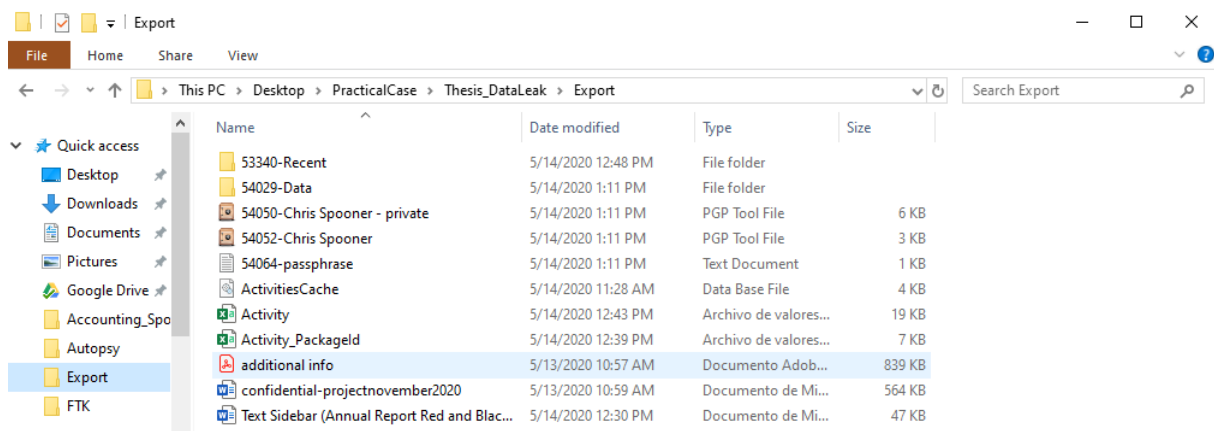


Figure 48: Exported Files from Autopsy

It was possible to export the encrypted data the attacker sent on the message previously included. Along with the information, the private key, the public key and the passphrase were obtained. By using the PGP Tool, the investigator is able to obtain the decrypted files going through the following steps:

1. Import the suspect's keys into the PGP Tool.

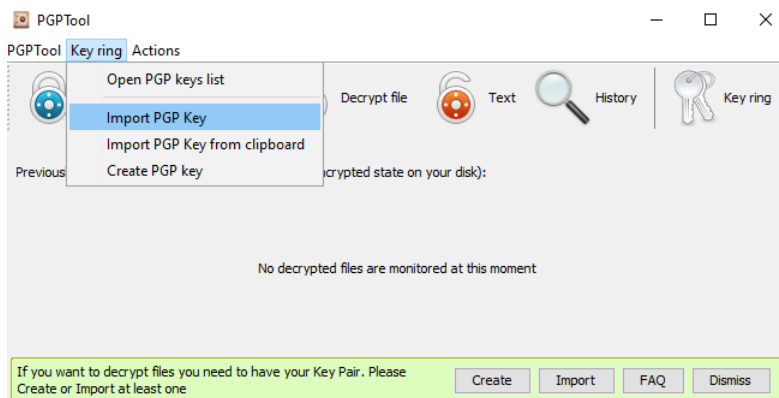
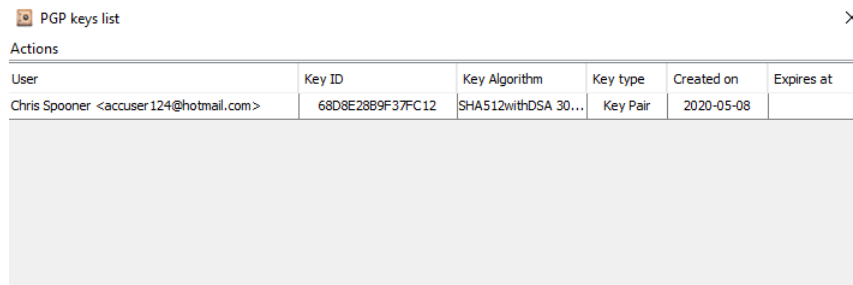


Figure 49: Import PGP Key



PGP keys list					
Actions					
User	Key ID	Key Algorithm	Key type	Created on	Expires at
Chris Spooner <accuser124@hotmail.com>	68D8E28B9F37FC12	SHA512withDSA 30...	Key Pair	2020-05-08	

Figure 50: Imported PGP Keys

2. Select the file to decrypt.
3. Specify the passphrase included in the file `passphrase.txt`.

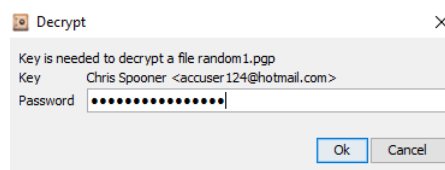


Figure 51: Decrypt Wizard in PGP Tool

4. Select the decrypted file destination.

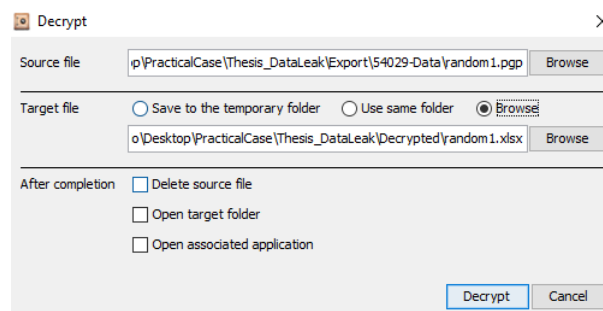


Figure 52: Decrypt Wizard in PGP Tool

5. Repeat step 2 according to the number of files to decrypt. Step 4 required if a new destination is desired only.
6. File decrypted.

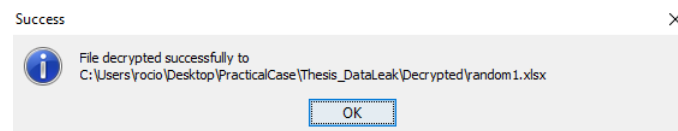


Figure 53: Decryption Completed

After decrypting the files, they are collated with the material that is located in the OneDrive shared folder. The original files were provided by Bioerts. There is a change in one file by adding some clarifying notes, which resulted in the file `additionalinfo.pdf`

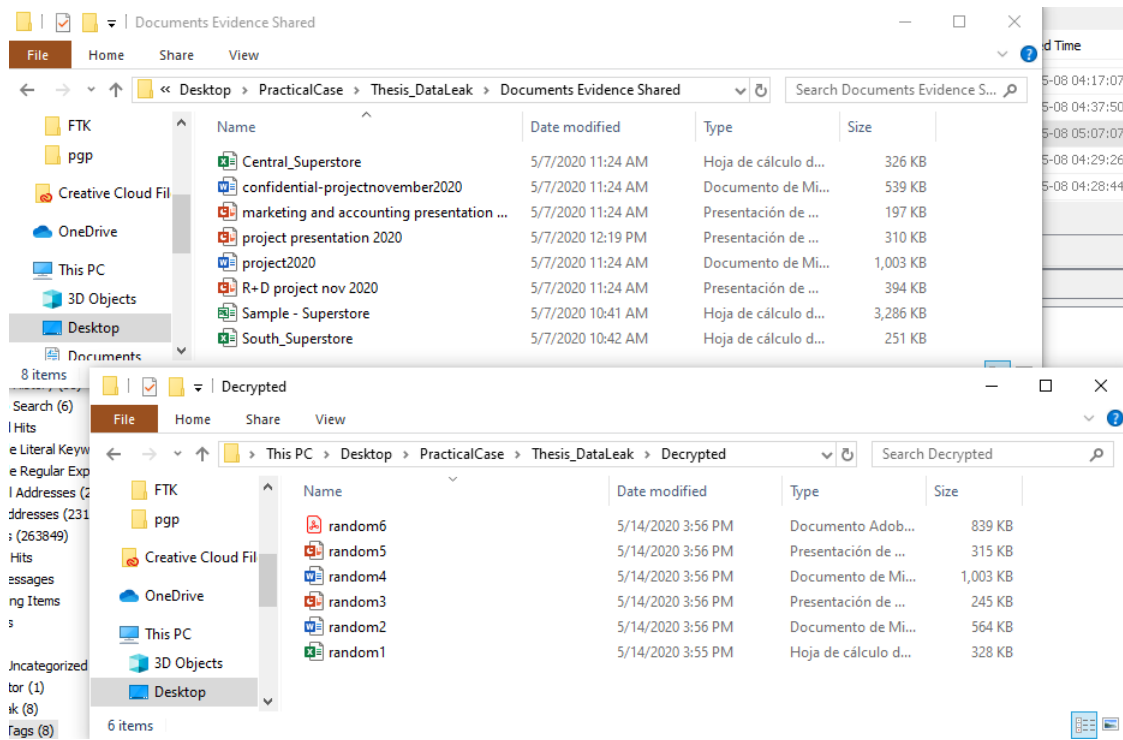


Figure 54: Decrypted and Original Files (comparison/match)

After the analysis of the data is completed, a report can be generated automatically. Different output formats can be selected as shown in the following figure. This report is going to be included later in the document. Figure 55 illustrates the wizard in software Autopsy to generate a report automatically.

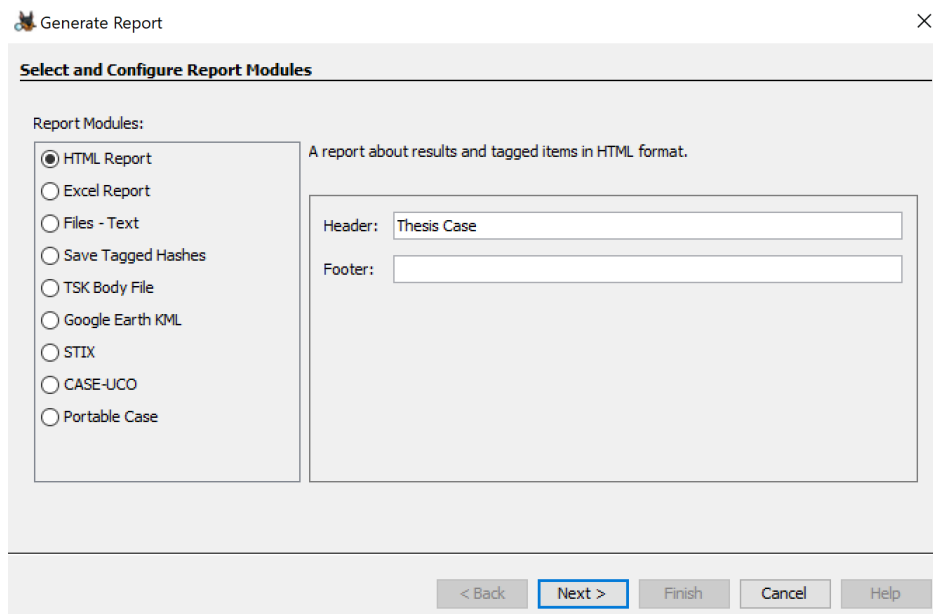


Figure 55: Report Generating Wizard in Autopsy

5.5 Reporting

Report generated by Autopsy included in the "Appendices" chapter.

CHAPTER 6

Discussion

With the evolution of communications, starting from the switching systems to the high-tech services present in society nowadays, attempts to break the privacy and security to access unauthorized or confidential content have always accompanied. The evolution of technology has had to go hand in hand with the evolution of laws protecting communications. Thus, emerging new categories of crime in the legal framework. Those in charge of helping in the resolution of this new criminal category, which is cybercrime, are, as previously mentioned, the forensic computer experts.

As stated before in the introduction of this document, the world is digitally connected and the flow of information in technological media defines a challenge for regular users of the Internet. Accordingly, the forensic experts must go a step further and expand their skills to analyze and understand its complexity.

It is important to rule out that the fact of introducing more advanced technologies will make it more difficult to guarantee the veracity of the digital evidence in the commission of a crime. In part, this is due to the lack of perception and ignorance that users have of ICT and the interconnected systems that make it possible to interrelate.

For a computer expert, it would be crucial at all times to determine the existence of a crime and who has been responsible. This task becomes more arduous due to the convergence between the real and the virtual world, added to the absence of geographic borders. This gives users *carte blanche* to access content anywhere on the globe.

The problem aggravates the moment in which it damages progress that could benefit scientific research, as is the case in this case study. There is an urgent need to be able to solve such cases. Digital Forensics plays an essential role in bringing attackers to the court and presenting solid, valid, and admissible digital evidence that enables these crimes to be prosecuted. To obtain a conviction, this evidence must have some characteristics. These have been described in this document and are a requirement.

In this thesis, an analysis process has been described that follows the standards and complies with the model described in the third chapter. Having this, admissibility of the evidence that is qualified as accurate and reliable is guaranteed. It is noted that despite the suspect's attempt to erase the evidence after formatting the disk, it has been possible to obtain evidence traces.

After an exhaustive study of the analytical procedure, the requirements of the digital evidence and the management of the tools to carry out the investigation it has been possible to demonstrate that the crime has taken place, so it can be said that the objectives of this thesis have been achieved.

CHAPTER 7

Conclusion

The thesis has dealt with the supposed obstacles of the constantly changing technology to provide an updated, suitable and admissible analytical framework for a digital forensic analysis carried out by an investigator. It is necessary to consider the possibility of corruption of a case due to mismanagement of the investigation phases. The examination of the digital evidence in the case study was decisive to determine that the offense took place.

The cybercrime chosen for the case study was a “Data Leak/Data Breach” case. The reason behind this choice resides in the importance of this kind of attack entails for almost any company or individual all over the world. It is no news that sensitive data has a price nowadays, and no data category is at no risk of being stolen. This thesis has been able to demonstrate the effectiveness of forensic analysis tools to prove the existence of a computer crime carried out by an attacker. During the course of the investigation, standard documents were also taken into account to assure the digital evidence has the characteristics listed in Chapter 2.

The importance of the results obtained after a digital forensic analysis leads to a decisive point when it comes to proving the innocence or guilt of the suspect. As remarked before, an analysis that does not follow established rules and regulations could stop the prosecution of a truly guilty defendant.

The limitations that may arise may be related to the impossibility of obtaining comprehensive evidence, either due to software limitations or the corruption of the evidence. The greatest advantage is that, along with the advance of information technologies, there is also a leap forward in tools that allow digital forensics experts to carry out more efficient investigations.

The results can be contrasted and analogous to real cases where this type of crime has taken place. Also, the place where this crime has been committed is relevant when undertaking an investigation. One way to continue and extend this work would be taking into account the jurisdiction of the crimes committed since this thesis does not delve deeply into this aspect.

Bibliography

- AccessData Group, Inc. (2016), *Imager User Guide*.
- ADALID (2015), 'Soluciones en informática forense'. Accessed on: 29/04/2020.
URL: <https://www.adalid.com/productos/soluciones-en-informatica-forense/>
- Ahmad, A. & Ruighaver, A. (2004), Towards Identifying Criteria for the Evidential Weight of System Event Logs., in 'Australian Computer, Network & Information Forensics Conference 2004: Perth, Western Australia', p. 5.
- Badiye, A., Kapoor, N. & Menezes, R. G. (2019), Chain of Custody (Chain of Evidence), in 'StatPearls [Internet]', StatPearls Publishing.
- Benner, J. (2009), 'Establish a transparent chain-of-custody to mitigate risk and ensure quality of specialized samples', *Biopreservation and biobanking* 7(3), 151–153.
- Casey, E. (2011), *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd edn, Academic Press, chapter Digital Forensics Foundations of Digital Forensics, pp. 7, 17, 23, 189.
- Chisum, W. J. (1999), Crime reconstruction and evidence dynamics, in 'Presented at the Academy of Behavioral Profiling Annual Meeting', Monterey, CA.
- Conexión Inversa (2013), 'Forensic Powertools (Listado de herramientas forenses)'. Accessed on: 15/04/2020.
URL: <http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html>
- CRU (2020), 'Ditto'. Accessed on: 30/04/2020.
URL: <https://www.cru-inc.com/ditto/>
- Digital Formats (n.d.), 'Mbox Email Format'. Accessed on: 19/04/2020.
URL: <https://www.loc.gov/preservation/digital/formats/fdd/fdd000383.shtml>
- Ford, C. (2014), 'What the Best Evidence Rule is - and what it isn't', *Mont. Law.* 40(2), 22. Accessed on: 31/03/2020.
URL: http://scholarship.law.umt.edu/faculty_barjournals/115
- Hoey, A. (1996), 'Analysis of the Police and Criminal Evidence act, s.69 - Computer Generated Evidence'.
- IETF (2002), 'RFC 3227. Guidelines for Evidence Collection and Archiving'. Accessed on: 06/04/2020.
URL: <https://tools.ietf.org/html/rfc3227>
- ISO/IEC (2012), 27037:2012 *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*.
URL: <https://www.iso.org/standard/44381.html>

- ISO/IEC (2015a), 27041:2015 *Guidance on assuring suitability and adequacy of incident investigative method*.
URL: <https://www.iso.org/standard/44405.html>
- ISO/IEC (2015b), 27042:2015 *Guidelines for the analysis and interpretation of digital evidence*.
URL: <https://www.iso.org/standard/44406.html>
- ISO/IEC (2015c), 27043:2015 *Incident investigation principles and processes*.
URL: <https://www.iso.org/standard/44407.html>
- ISO/IEC (2018), 27050-2:2018 *Guidance for governance and management of electronic discovery*.
URL: <https://www.iso.org/standard/66230.html>
- ISO/IEC (2019), 27050-1:2019 *Overview and concepts*.
URL: <https://www.iso.org/standard/78647.html>
- ISO/IEC (2020), 27050-3:2020 *Code of practice for electronic discovery*.
URL: <https://www.iso.org/standard/78648.html>
- Jaffee, W. B., Trucco, E., Teter, C., Levy, S. & Weiss, R. D. (2008), 'Focus on alcohol & drug abuse: ensuring validity in urine drug testing', *Psychiatric Services* 59(2), 140–142.
- Jhala, A. P. (n.d.), 'Digital Evidence - Technical Issues'. Accessed on: 25/03/2020.
URL: <http://www.aitd.net.in/pdf/13/12.%20Digital%20%20Evidence-%20Technical%20Issues.pdf>
- Katsavounidis, C. (2018), 'Github - kacos2000/windowstimeline'. Accessed on: 13/05/2020.
URL: <https://kacos2000.github.io/WindowsTimeline/WindowsTimeline.pdf>
- Logicube (2020), 'Talon® ultimate'. Accessed on: 30/04/2020.
URL: <https://www.logicube.com/shop/talon-ultimate/>
- Magnet Forensics (2014), 'Forensic Analysis of LNK files'. Accessed on: 19/04/2020.
URL: <https://www.magnetforensics.com/blog/forensic-analysis-of-lnk-files/>
- Mayer, R., Rauber, A. & Antunes, G. (2014), A context model for digital preservation of processes and its application to a digital library system, in 'IEEE/ACM Joint Conference on Digital Libraries', pp. 459–460.
- McKemmish, R. (1999), *What is forensic computing? Trends and issues in crime and criminal justice*, Vol. 118, Australian Institute of Criminology Canberra.
- Neijts, R., Semilof, M. & Clark, C. (2018), 'Definition. steganography'. Accessed on: 04/04/2020.
URL: <https://searchsecurity.techtarget.com/definition/steganography>
- Ondata (2020), 'Soluciones en informática forense'. Accessed on: 29/04/2020.
URL: <https://www.ondata.es/recuperar/computer-forensics.htm>
- OpenText (2020), 'Tableau forensic imager tx1'. Accessed on: 30/04/2020.
URL: <https://www.guidancesoftware.com/tableau/hardware/tx1>
- Panda Security (2018), 'Types of Cybercrime'. Accessed on: 23/03/2020.
URL: <https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/>
- Rios, D. J. (2014), *Security Officer Study Guide*, 1st edn, Lulu.com, chapter Crime and Accident Scene Protection, p. 67.

- Sammons, J. (2012), *The basics of digital forensics: the primer for getting started in digital forensics*, Elsevier.
- Sant, P. & Hewling, M. O. (2011), Digital forensics: the need for integration, in 'Proceedings of the Sixth International Workshop on Digital Forensics & Incident Analysis (WDFIA 2011)', University of Plymouth, p. 1.
- Sommer, P. (1997), 'Downloads, Logs and Captures: Evidence from Cyberspace', *Journal of Financial Crime* 5, 138–151.
- The National Institute of Standards and Technology (2019), 'Computer Forensics Tools and Techniques Catalog'. Accessed on: 14/04/2020.
URL: <https://toolcatalog.nist.gov/search/index.php>
- The Sleuth Kit (2016), 'Autopsy User Documentation - UI Layout'.
URL: https://sleuthkit.org/autopsy/docs/user-docs/4.0/uilayout_page.html
- The Sleuth Kit (n.d.a), 'Autopsy'. Accessed on: 19/04/2020.
URL: <https://www.sleuthkit.org/autopsy/>
- The Sleuth Kit (n.d.b), 'Autopsy - Features'. Accessed on: 19/04/2020.
URL: <https://www.sleuthkit.org/autopsy/desc.php>
- Tomlinson, J., Elliott-Smith, W. & Radosta, T. (2006), 'Laboratory information management system chain of custody: Reliability and security', *Journal of Analytical Methods in Chemistry* 2006.
- United States Department of Commerce (2019), 'Software Quality Group. The National Software Reference library (NSRL)'. Accessed on: 19/04/2020.
URL: <https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl>
- United States Department of Justice (2004), *National Institute of Justice Annual Report 04*, Office of Justice Programs.
- Vacca, J. & Rudolph, K. (2010), *System Forensics, Investigation and Response (Information Systems Security & Assurance)*, 1st edn, Jones & Bartlett Learning, chapter Forensics Methods and Labs, p. 58.
- Veber, J. & Smutny, Z. (2015), Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic, in 'European Conference on Cyber Warfare and Security', Vol. 2015, pp. 294–295.
- Verizon (2019), 'Insider threat report - executive summary'. Accessed on: 10/05/2020.
URL: <https://enterprise.verizon.com/resources/executivebriefs/2019/insider-threat-report-executive-summary.pdf>
- Wall, D. S. (2009), What are cybercrimes?, in 'Crime and Deviance in Cyberspace', Ashgate Publishing, p. 16.
- Wikipedia (2020), 'Autopsy (software)'. Accessed on: 19/04/2020.
URL: [https://en.wikipedia.org/wiki/Autopsy_\(software\)](https://en.wikipedia.org/wiki/Autopsy_(software))