



INTERNATIONAL
HELLENIC
UNIVERSITY

Forensic analysis in the cloud: current state, tech- nical obstacles & chal- lenges

Patsarikas Andreas

SID: 3307150010

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Communications and Cybersecurity

DECEMBER 2016

THESSALONIKI – GREECE



INTERNATIONAL
HELLENIC
UNIVERSITY

Forensic analysis in the cloud: current state, tech- nical obstacles & chal- lenges

Patsarikas Andreas

SID: 3307150010

Supervisor:

Assist. Prof. Eirini Kotsia

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Communications and Cybersecurity

DECEMBER 2016

THESSALONIKI – GREECE

Abstract

Cloud is a new challenge which must be faced by forensic investigators. There are various types of cloud services, with each type having a different potential use in criminal activity. The difficulty lies in identifying and acquiring (or retaining) potential data when disparate services are used. The communication and cooperation with the service providers, for retrieving the stored files, is a time consuming process. For this reason, investigators must know where are the application data locally stored.

There is a need for a framework of digital forensic investigations that is adapted to the requirements and special features of these services. In this thesis, we are proposing a framework based on existing methodologies.

By using popular cloud services like Box, we will apply the proposed framework of forensic investigation on a computer with Windows 7. We will examine a variety of scenarios, including a number of file handling methods and access to this service. This research contributes to a better understanding of the artifacts that are likely to be encountered by investigators at the identification stage, by defining the data remnants in the computer system. Such possible sources of information are the application files, the browser history and RAM.

Despite the fact that the use and sharing of software, hosted on the Internet, is the next step in exploitation of World Wide Web, it could be a challenge for the researchers of digital forensics. The dependency of individuals and businesses from various providers of cloud services (SaaS, PaaS, IaaS), may hinder the procedure of forensic investigations.

Contents

ABSTRACT.....	III
CONTENTS.....	V
1 INTRODUCTION.....	9
1.1 RESEARCH OBJECTIVES	10
1.2 THESIS STRUCTURE.....	10
2 DIGITAL FORENSICS	12
2.1 DEFINITION	12
2.2 DIGITAL EVIDENCE AND DATA	12
2.3 RESEARCH EVIDENCE.....	14
2.4 FORENSIC INVESTIGATION PROCEDURE	16
2.4.1 <i>Collection</i>	16
2.4.2 <i>Preservation</i>	16
2.4.3 <i>Analysis</i>	19
2.4.4 <i>Presentation</i>	21
2.5 DIGITAL FORENSICS' CATEGORIES.....	21
3 INTRODUCTION TO CLOUD COMPUTING AND CLOUD STORAGE	23
3.1 KEY AND SIGNATURE FEATURES OF CLOUD COMPUTING.....	24
3.2 SERVICE DELIVERY MODELS (SPI MODELS) OF CLOUD COMPUTING	26
3.3 DEPLOYMENT MODELS OF CLOUD COMPUTING	29
3.4 CLOUD STORAGE.....	33
3.5 DIGITAL FORENSICS AND CLOUD STORAGE.....	34
4 EXAMINATION OF RAM.....	36
4.1 THE ROLE OF RAM ANALYSIS IN MODERN DIGITAL ENVIRONMENT	36
4.2 FORENSIC ANALYSIS OF RAM.....	36
4.3 TYPES OF EVIDENCE THAT CAN BE FOUND IN RAM	37
4.4 LEGAL IMPLICATIONS OF RAM RECOVERY	37

4.5	LIMITATIONS OF RAM ANALYSIS	37
4.6	TOOLS AND TECHNIQUES.....	38
4.7	DATA PRESERVATION IN RAM	38
4.8	CONCLUSIONS.....	39
5	METHODOLOGY.....	41
5.1	REQUIREMENTS	41
5.2	PROPOSED METHODOLOGY	42
5.2.1	<i>Purpose</i>	43
5.2.2	<i>Preparation</i>	43
5.2.3	<i>Identification and Collection</i>	44
5.2.4	<i>Preservation (Forensic copy)</i>	44
5.2.5	<i>Analysis</i>	44
5.2.6	<i>Presentation</i>	44
5.2.7	<i>Feedback / Completion</i>	44
6	INVESTIGATION METHODOLOGY	45
6.1	INVESTIGATION PROBLEM.....	45
6.2	INVESTIGATION PURPOSE	45
6.3	INVESTIGATION QUESTIONS.....	45
6.3.1	<i>Investigation Question 1</i>	45
6.3.2	<i>Investigation Question 2</i>	46
6.4	EXPERIMENTAL PROCEDURE.....	46
6.4.1	<i>Experimental Procedure for Answering the First Question</i>	47
6.4.2	<i>Experimental Procedure for Answering the Second Question</i> ...	48
6.5	HARDWARE	49
6.6	SOFTWARE	50
6.7	CREATION OF VIRTUAL MACHINES	53
6.8	FILES	54
6.9	CREATION OF FORENSIC IMAGES	55
6.10	ANALYSIS OF FORENSIC IMAGES	60
6.11	ANALYSIS OF BROWSERS	64
6.11.1	<i>Analysis of Mozilla Firefox (FFX)</i>	64
6.11.2	<i>Analysis of Google Chrome (GC)</i>	67

6.12 SIGNATURE COMPARISON METHODOLOGY.....	69
6.13 LIMITATIONS OF THE INVESTIGATION.....	70
6.14 CONCLUSIONS.....	71
7 DIGITAL FORENSIC INVESTIGATION OF BOX CLOUD STORAGE	
SERVICE.....	72
7.1 INTRODUCTION.....	72
7.2 PURPOSE/OBJECTIVE.....	73
7.3 BOX SERVICE ANALYSIS IN WINDOWS 7 ENVIRONMENT.....	73
7.3.1 <i>Preparation</i>	73
7.3.2 <i>Identification and Collection</i>	74
7.3.3 <i>Preservation</i>	74
7.3.4 <i>Analysis</i>	74
7.4 USE OF THE APPLICATION SOFTWARE FOR UPLOADING FILES.....	77
7.4.1 <i>Event Logs Examination</i>	77
7.4.2 <i>Examination of RAM</i>	80
7.5 USE OF THE APPLICATION SOFTWARE FOR RETRIEVING FILES.....	84
7.5.1 <i>Event Logs Examination</i>	85
7.5.2 <i>Examination of RAM</i>	87
7.6 RESULTS OF BOX'S APPLICATION SOFTWARE ANALYSIS.....	89
7.7 ACCESS THROUGH BROWSER.....	90
7.7.1 <i>Use of Mozilla Firefox</i>	90
7.7.2 <i>Use of Google Chrome</i>	98
7.7.3 <i>Conclusions</i>	101
7.8 METADATA.....	102
7.8.1 <i>Use of Box's Application Software</i>	102
7.8.2 <i>Use of Browser</i>	103
7.9 DELETION.....	105
7.9.1 <i>First Scenario of File Deletion</i>	105
7.9.2 <i>Second Scenario of File Deletion</i>	106
7.9.3 <i>File Deletion through Browser</i>	107
7.10 BOX'S APPLICATION SOFTWARE UNINSTALLATION.....	108
7.11 PRESENTATION.....	109
8 INVESTIGATION CONCLUSIONS.....	112

8.1	INVESTIGATION OBJECTIVES.....	112
8.2	INVESTIGATION FINDINGS	113
8.2.1	<i>Investigation Question 1</i>	113
8.2.2	<i>Investigation Question 2</i>	114
8.2.3	<i>Special Mentions and Further Research</i>	114
	TABLE OF FIGURES.....	119
	TABLE OF TABLES	122

1 Introduction

The purpose of this chapter is to provide an introduction and to present the overall structure of the thesis. This chapter also outlines the main research objectives within the framework of the forensic analysis of cloud storage services. Lastly, there is a brief description of the thesis structure.

Digital computer forensics is defined as the process of identifying, preserving, analyzing and presenting digital evidence in a way that is legally acceptable [23].

There are also clearly defined principles governing the conduct of digital forensic investigation. These are:

- No action is able to change data held on a computer or storage media, which may be presented at court.
- Use of archetypal (original) data by a third party, after authorization.
- In case an individual considers that access to archetypal data is necessary, that individual must be capable to do so and be able to explain the importance and the consequences of his actions.
- The person in charge of the investigation, is entrusted with the overall responsibility to ensure compliance with the forthcoming legislation and these principles [17].

Lastly, the US National Institute of Justice has published a guide for the forensic analysis of computers. In this guide, the principles that need to be respected by the investigators, are defined, some of which are:

- no action should affect the integrity of the data
- the individuals in charge of the data analysis need to be properly trained
- each activity need to be documented

[28]

Despite that the scope and procedures of digital forensics are well defined, the technology used by the cloud and its legal implications, may complicate and in many cases hinder the investigation procedure.

Cloud, because of its infrastructure, facilitates criminal activities. It offers to criminals, easy access to encryption technologies, like SpiderOak. Moreover, a criminal can quickly erase all data from his account, which increases the possibility not to leave evidence for the forensic analysis. Lastly, an unclear legal framework that criminals can exploit is created, because the storage of data is happening on servers located abroad, and cause of the policy of the companies that provide cloud services.

1.1 Research Objectives

The focus of this research is to determine whether there are any remnants of data from the use of cloud storage services in a computer system running Windows 7. First, we developed a framework that will guide our research. This framework is built based on the principles of digital forensics of computers, and it is having as a standard the methodology of the Law Enforcement Process Model. The methodology, which we developed, may as well be used by investigators to investigate real crimes.

Objective 1: Determine the theoretical background of digital forensics and cloud storage technology.

Objective 2: Develop a framework of digital forensic analysis, that will help the investigators to follow a standard procedure, when undertaking forensic analysis of cloud storage services.

Objective 3: Examine popular cloud storage services, like Box, and check if there are any data remnants to contribute to forensic research and analysis.

Objective 4: Examine the effects, from a forensic standpoint, that the data traffic of these applications have (metadata, date of access, hash value modification).

With the completion of our investigation, we will have gained a better understanding of digital data, generated by the use of these applications. Finally, we will have defined the points where the investigators should draw their attention, like the phases of identification, preservation, analysis and presentation of research.

1.2 Thesis Structure

Chapters 2,3,4,5 are the theoretical background of our research. Specifically, in chapter 2, we will define the term Digital Forensics, what constitutes digital evidence and the process that we follow in a forensic investigation. In chapter 3 we will examine cloud

technology, cloud storage services and how this technology affects digital forensics. In chapter 4 we will analyze the forensic examination of RAM, the data that can be found, and the factors that affect the duration of their storage in memory. In chapter 5 we will determine the methodology that we are going to follow in our research. In chapter 6 we will determine the questions to be answered, that came up by the research which we will do, the tools and how to use them. In chapter 7 we will analyze Box Cloud service. Lastly, in chapter 8 we will summarize our findings, and some future extensions that our research can have.

2 Digital Forensics

In this chapter we will present, in detail, digital forensics, its objectives and the principles that should be followed. Finally, we will analyze the phases and the categories in which it is divided.

2.1 Definition

Digital era has produced many new professions, but one of the most unusual is digital forensics. Digital forensics deals with the implementation of the law on computer science. A definition of this term is the following: As digital forensics, we defined the digital investigation and analysis techniques that include the identification, preservation, collection, documentation and report of digital data, in order to define exploitable and legal evidence.

Even though digital forensics is similar to other forms of forensics, the process of digital forensics requires excellent knowledge of computer hardware and software, in order to prevent unintentional cancellation or destruction of evidence and their preservation for further analysis. Also, the digital investigator must know in detail the national and international laws that are relative to the collection of evidence. Digital forensics has become a popular topic in the society of computer security. Although it is an exciting field, the size of the information that is available is far bigger than the size of the information that is possible to get analyzed, and the digital investigator needs to be experienced in order to know when to stop analyzing.

The main idea behind digital forensics is in the recovery of data. To do this, you must:

- *Identify the evidence.*
- *Determine how to preserve the evidence from getting changed.*
- *Collect, process and analyze evidence.*
- *Ensure that the evidence will be accepted by the court.*

2.2 Digital Evidence and Data

Digital evidence is the most important means of proof when examining a cybercrime case and any element that has a digital format. The Scientific Working Group on Digital

Evidence (SWGDE) [29], a consortium of international organizations that operates at the field of digital evidence, in October of 1999 standardized the evidence that have digital format and categorized them into:

- *Digital Evidence*: Information which have evidential value in a criminal case and can be stored or transmitted in digital form.
- *Data Objects*: Objects or information which have evidential value in a criminal case and are related to physical objects.
- *Physical Items*: The physical media where the information and data objects are stored, or through which are transmitted.
- *Original Digital Evidence*: Items and data objects at the time that are collected from the crime scene.
- *Duplicate Digital Evidence*: A replica digital copy of all the data objects that are included in an original digital object.
- *Copy*: An exact reproduction of the information that are contained in a genuine physical object, regardless of this object.

Digital evidence can be stored on any device, such as an electronic computer, tablet, mobile phone etc., and in any storage medium, such as CDs, DVDs, USB sticks, memory cards etc.

A “key” feature of digital evidence is the large degree of their alterability. They can easily be modified or destroyed by using various tools and methods. Therefore, the investigator should seek and treat this information with great care.

Digital evidence are consisted of Digital data. Digital data are distinguished in Volatile data and Persistent data. Volatile data are stored in system memory (registry¹, cache memory, RAM), and they disappear if the computer shuts down or restart. Persistent data are stored in the hard disk drives of the system or in other storage devices, such as USB sticks, CDs / DVDs, memory cards and external hard disks. These kind of data will not be lost when you shut down or restart the computer.

¹ On disk, the Windows Registry isn't simply one large file but a set of discrete files called hives. Some hives are volatile and don't have associated files. The system creates and manages these hives entirely in memory; the hives are therefore temporary in nature. The system creates volatile hives every time the system boots. These files are database files, and only RegEdit, Regedit32 and the Kernel32 can read them.[30]

2.3 Research Evidence

The primary goal in a digital forensic investigation is to define the type of evidence to be sought in the case. Knowing the type of the evidence being sought; is an indispensable part of a successful investigation.

It is necessary to examine each one of these objects, to discover evidence that we can use in our investigation.

Hardware

While it is expected that in the beginning of an investigation we will focus on the hardware parts, that is not always true. Numerous times it is possible to collect evidence, by examining the peripherals devices (Keyboard, mouse, CD / DVD player, scanner, etc.) for fingerprints. In several investigations it is of primary importance, whether the suspect used a device or not. Before analyzing the hardware, we need to be sure that we are authorized to do so. After ensuring that we have the proper permission, we need to create a list of all the evidence that we found. We record all the computer parts and anything that is connected to the computer over wired or wireless connection.

Computer System

A computer system is consisted of hardware and software, that process the data, and it may include:

- A case that contains the circuits, motherboard, processor (CPU), hard drives, RAM and interfaces / connectors.
- Peripherals like a screen, a keyboard and a mouse.
- External connected drives, devices and accessories.
- The operating system and a wide variety of programs.

Computer systems can take many forms, such as desktops, laptops, net-books, servers, etc. The additional peripherals include routers, switches, printers, scanners, etc.

Removable Storage Media

Removable storage media are used for many purposes and are a source of information for evidence. They are usually used for:

- Back up of data
- Data transfer
- Installing software

The first two uses are those that have more interest for the investigator. Although we may not find evidence in a hard drive, we should always seek for secondary backups or copies. Generally, there are two types of files that exist in the removable storage media. The files that are stored intentionally and the temporary ones. The intentionally ones are stored files, which are saved as copies of files that may have been erased.

While the investigation is in progress, if the system seems to have been “cleaned”, we must look for backups. In fact, the existence of software that “cleans” the system of evidence, like Evidence Eliminator, usually indicates that the user is hiding something. The user is quite likely to have made backup copies before “cleaning” the system. Temporary files, the second type of files that can be found in removable storage media, are files or remnants of files which have been temporarily stored, in order to get transferred from one computer to another. It is quite likely that the files will still exist after the transfer, since there are quite few people who “clean” the removable storage media in a right way.

Documents

The last common type of evidence are the non-digital documents. We can define as a document anything that is written, can be touched and held. Evidence that are consisted of documents are documentary evidence. Printed reports, handwritten notes, and tables, are few examples of documentary evidence. The most important characteristic of the documentary evidence is that they need to get authenticated. It must be proven that the evidence derived from suspect’s computer and have not been changed since their collection.

The investigator should take pictures of the documents and tables, and carefully examine the crime scene for any document which may be used as evidence. Many people write their credentials on sticker notes and keep them on their computer’s screen. Furthermore, evidence may exist above, beneath or behind the hardware parts.

2.4 Forensic Investigation Procedure

The forensic investigation, as we can see in the figure below (Figure 1), has four phases:

- *Collection*
- *Preservation*
- *Analysis*
- *Presentation*

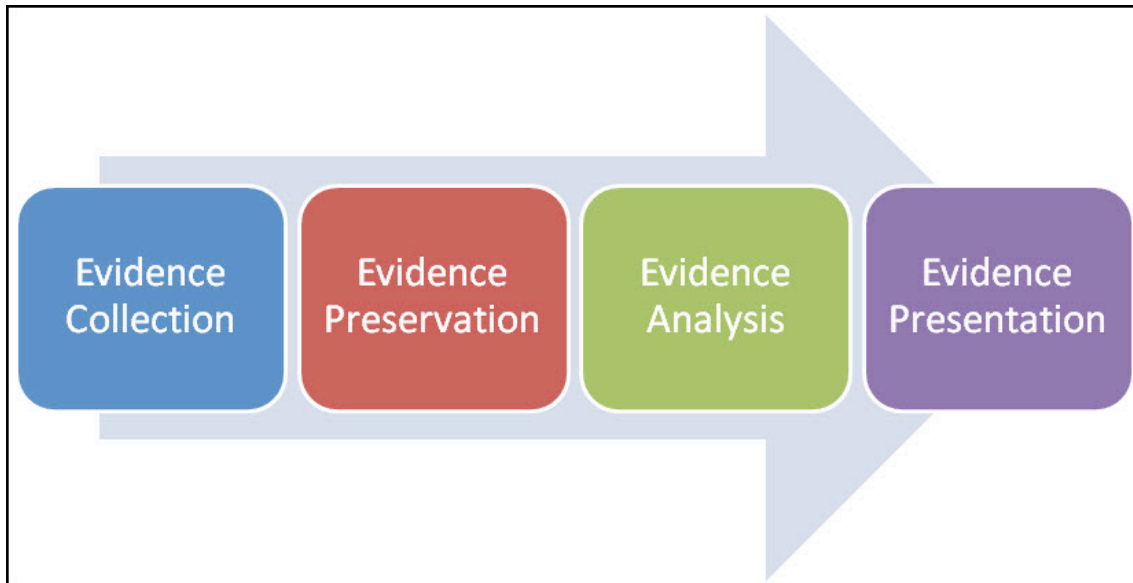


Figure 1: Phases of forensic investigation

2.4.1 Collection

It includes the procedures and methods of recording the physical scene of the crime. The documentation of the crime scene creates a registry for the investigation. It is important to record accurately the scene itself, the state of the computers, the storage media, the wireless network devices, the mobile phones and tablets, the internet and local network accesses and other electronic devices.

2.4.2 Preservation

A key issue, in the procedure of digital forensics, is the preservation of data. The phase of preservation corresponds to the pausing of any activities in the crime scene. It focuses on stopping or preventing any activity that may damage the digital information being collected. The phase of preservation includes actions such as the isolation of computers, the cancelation of ongoing deletion procedures, and the selection of the most secure method to collect the information.

A computer has essentially two sources of data that are of interest to the investigator. The volatile and the non-volatile memory. The volatile memory is mainly related to the RAM memory of the computer, but it also includes the cache memory and registry memory. The non-volatile memory is associated with all the other types of media that do not lose their data when the power source is removed. Hard drives are the most common type of non-volatile memory, with storage capacities that now reach terabytes. This category also includes the various removable storage media (e.g. USB drives and SD cards).

The first problem that an investigator will face, is what to do with the suspicious computer. If the system is off, the decision is a bit simpler, since it is most likely all the volatile data are lost. If the system is still powered on, the investigator must decide whether to terminate its operation immediately, or whether to proceed with the recovery of system's volatile data (RAM, cache memory). In chapter 4 we will examine in more detail the RAM memory.

Once the volatile data are copied, a number of other tools can then be used to extract useful information about the computer system. There is also a wide variety of available tools that could be used, during the live analysis, for the collection of relevant data.

To ensure the integrity of the information that are obtained during the live analysis, it is important to ensure that the investigator will use version of tools which belong to him (i.e. trusted) and not the tools that are installed on the system to be analyzed. Therefore, it is common for forensic investigators to create their own suite of tools, for use during live collection and analysis.

After the completion of live analysis, follows the system's shut down and its transport to the laboratory, for the forensic collection of non-volatile data. The acquisition of the hard drive can be achieved in various ways:

- Removing the drive from the suspicious computer and connect it to a reliable machine. The connection method with the reliable system would depend on the hard drive's interface (e.g. PATA, SCSI, SATA). The insertion of a write blocker, between the hard drive and the computer, ensures the data integrity of the hard drive to be tested.
- Establishing a connection with the suspicious machine through network connection. The secure boot of the suspicious computer, using the appropriate programs

(stored either in a CD / DVD or in a USB drive), allows us to recover the hard drive.

From the organizations' / companies' standpoint, is not always possible to follow the previous steps for the collection of non-volatile data. Many organizations are equipped with systems that is not simple task to terminate their operation. Because of this, the use of other methods, for the recovery of non-volatile data, is required.

Here are the four levels of data collection, sorted by increasing precision:

- *Individual files*
- *Back up repositories*
- *Bit-to bit recovery of the individual disk partitions.*
- *Bit-to-bit recovery of the entire disk.*

If the data are stored or still remain within existing files, then the first two approaches will be successful in identifying data. The advantage of the latter two approaches, is the wealth of information that can be collected from memory's and operating system's un-allocated clusters.

There is a variety of tools that facilitate the copying process. The original method of the forensic disk copy was the creation of an exact bit-to-bit (raw) disk image. Unix's (Operating system) "dd" command is used widely for this purpose. This means that if the investigator wants to copy a disk of 250GB, he will need at least a 250GB drive to store the copy.

This subchapter began with a reference to the fact that data preservation is imperative at this stage. The procedure of securing the preservation of data, derived from the need to guarantee the data integrity. The universal tool that is used for this purpose are the hash functions (or else digest functions). A hash function is able to receive an input of variable length and produce an output of fixed length that defines the input uniquely, and is often mentioned as a data fingerprint.

Two algorithms are used:

- The *Message Digest 5 (MD5)*, with a 128-bit output, which was created by Ronald Rivest.
- The *Secure Hashing Algorithm (SHA-1)*, with a 160-bit output, which was published by NIST.

By obtaining a fingerprint of the suspicious hard drive before its replication, and then by comparing the initial result with the copy's hash output, an investigator is able to confirm if a precise bit-to-bit duplicate disk has been produced.

Although there are plenty of tools that can undertake this procedure, a careful examination of the hardware, software and procedures is required in order to be used. The incompatibilities among hardware, the access to the BIOS to modify the devices' boot order, and different driver versions are factors that can affect the recovery process. However, once the fingerprint is successfully acquired, the hard drive can then be analyzed.

Once a copy of a disk or a partition is created, and its integrity is verified, the investigator does not need to operate with the original drive. In fact, it is common practice for the original evidence to be stored in guarded facilities, and to be paid special attention to environmental factors that may affect the integrity of the evidence (e.g. positioning hard drives near magnetic sources).

2.4.3 Analysis

In the analysis phase, the investigator examines the acquired data to identify the evidence. There are three major categories of evidence:

- *Aggravating / Incriminating evidence*: Those which support a specific theory.
- *Exculpatory evidence*: Those that are contrary to a specific theory.
- *Evidence of Tampering*: Those that cannot be associated with any theory, but they indicate that the system status has been tampered with.

The analysis of digital data may not be as exciting as the identification and collection, but this is the most crucial component of digital forensics. In this phase, we extract and interpret the data, to create a report that will organize and interpret the mystery world of digital evidence, so that it can be used to prove or drop civil, administrative or criminal charges.

The analysis of digital devices and storage media, for the purpose of locating and exporting data, has evolved into an advanced methodology, which is driven by the development of increasingly powerful and advanced digital forensic tools.

These are automated toolboxes that incorporate a plethora of functions, and offer a graphical user interface (GUI) that facilitates the user's interaction with the application.

So instead of using several specialized programs for data analysis, we can use a program to achieve most of these common tasks:

- Identification of the file type, by checking the file's header.
- Recovering deleted files.
- Search for files in distributed / unallocated space.
- Email Mining and Processing.
- Analysis of log files and registry files.
- Analysis of metadata.
- Creation of reports.

Moreover, some processes, such as email processing and the recovery of deleted files, are performed automatically in the background.

Automated forensic toolboxes have dramatically increased productivity and have become the norm for the analysis of various storage media. However, there are various command line tools and independent programs that perform specific processes. Regardless of the tools' type that will be used, if the user of the digital devices (which will be investigated) have not used any data masking process (e.g. cryptography), we will be able to recover all data.

In fact, if we do not apply restrictions on our search (e.g. keywords, time constraints), we will end up with too much information that will burden our investigation.

Operating system's artifacts is a term that describes the data, metadata, log files, inodes, plists, restore points and temporary files that all operating systems create, as they perform their myriad functions. The identification, extraction / recovery, and most importantly the interpretation of artifacts, permits us recreating the operations and status of the media that we examine. The challenge, which a forensic investigator faces when he detects such artifacts, is multiplied. First and foremost, he must correctly interpret the information carried by this artifact, considering that different operating systems handle differently the same artifacts.

The second challenge is probably more difficult. We need to explain, to a computer systems unfamiliar audience, that these data were created by the internal functions of an operating system, and what is their importance.

2.4.4 Presentation

The investigator will be presenting his findings in a clear, comprehensive, well-structured and precise report, in which he will explain all the conclusions he has reached. Regardless of the investigation's nature (corporate, legal), the steps which are performed at the stages of collection and analysis are similar, because they are dominated by technical, rather than legal, issues. The stage of presentation, however, depends entirely on corporate policy and legal law, which may vary for each case. At this stage, we present the findings together with the corresponding data from a survey. In a corporate investigation, the audience is usually consisted by the directors' board, the general manager and the executives. In a court, the audience is usually just a judge. So the corporate policy and the legal framework determine the manner, the purpose and the content of the presentation.

2.5 Digital Forensics' Categories

Digital forensics are divided into the following subcategories:

- *Computer Forensics*
- *Network Forensics*
- *Database Forensics*
- *Mobile Device Forensics*
- *Cloud Forensics*

Computer forensics is defined as “the implementation of the forensic science techniques on hardware”. In other words, computer forensics is the procedure of identifying, preserving, analyzing and presenting digital evidence in a legally acceptable manner.

On the other hand, network forensics is the capture, recording and analysis of network events, in order to discover the source of the security attacks. Network forensics generally have two purposes. The first purpose which concerns security, involves the monitoring of a network in order to detect ineligible actions. An attacker could delete all the log files on a computer, so the network data constitute the only available evidence for forensic analysis. The second purpose of network forensics associates with the law enforcement. In this case, the analysis of the recorded network traffic can include actions such as the reconstruction of transferred files, keyword search, and analysis of human communication, such as e-mails or chat sessions.

Database forensics is a branch of digital forensics that focus on forensic analysis of databases and their associated metadata. The steps which are performed are similar to the ones of computer forensics, following the normal procedure of forensic research and its application on the content of the database and metadata. A forensic investigation of a database can be associated with the timestamps of the various actions that were performed, in order to examine the operations of a database user. Alternatively, the forensic investigation may focus on identifying the transactions in a database system or an application, which suggest illegal acts, such as fraud.

Mobile device forensics is a branch of digital forensics, concerned with the recovery of digital documents or data, from a portable device. The term portable device does not include only mobile phones, but also any digital device that has both internal memory and the ability to communicate. The spread of smartphones created the need for forensic investigation of the devices. This need could not be covered by the existing digital forensic techniques. The memory type; the different methods of operation and communication between the user and mobile device, require a different forensic procedure compared to computer forensics. There are required specialized data extraction techniques that are tailored to the respective device. Portable devices can be used for the storage of several kinds of personal information, such as photos, contacts, calendars and notes.

Cloud forensics is the combination of cloud computing and digital forensics. Cloud computing is a joint collection of regulated network resources (e.g. networks, servers, storage systems, applications and services) that can be quickly readjusted with minimal effort. Digital forensics is the application of the computer science principles, for the purpose of retrieving digital evidence and their presentation. Cloud forensics is a subset of network forensics. Therefore, cloud forensics follow the main phases of network forensics, while having the techniques adapted to cloud computing. Cloud computing is an evolving technology with complex aspects, which we will examine below.

3 Introduction to Cloud Computing and Cloud Storage

There are many discussions nowadays about Cloud Computing, and there is a plethora of references for this vague notion. In the traditional computing infrastructure, Operating Systems (OSs), applications or data are typically stored in user's personal computer. In the working environment, data are stored on servers, which are usually in the same building, and they are well accessible from the rest of the company.

According to the US National Institute for Standards and Technology (NIST) [26], "Cloud Computing is a model for enabling ubiquitous, convenient, on demand network access to a share pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing is a different form of Information Technology infrastructure. It is a service where data and services are provided by data centers, which are accessible from practically anywhere through the Internet and the use of desktops, laptops, tablets and smartphones. Someone can say that cloud computing is the next stage in the evolution of the World Wide Web.

Cloud computing is mostly a framework for a "new" business model of providing services, and not a technology, which seems has already started to monopolize the attention of scientists, engaged in IT, for the years to come. It is the evolution of the widespread, nowadays, virtualization technology and the model of utility computing. One of its "key" features is that allows users to interact with devices or data, in such a way that minimizes the necessary interaction with the underlying layers of the technology stack.

Cloud is a huge change in the way of which computing resources are provided, since it allows storage and processing of data via the Internet wherever we are and the use of operating systems and applications. Furthermore, the user does not need to purchase and install them on their computer. Instead, he can now use these resources as services. The provision of such services is similar to electricity supply, which you can use as much as you need, whenever you need it and pay only for what you consumed. Consumer is only concerned with the location of the plug and not with the production or the supply of electricity.

The most important applications that refer to cloud-based computing are Office, Business, Storage and Media applications. There are several companies that already offer such services and others that are planning to do it in the near future. Some of these companies and their respective cloud platform services are: a) Amazon and Elastic Compute Cloud (EC2), b) Google and App Engine, c) Microsoft OneDrive and Azure Services Platform, d) Dropbox and Dropbox storage services, e) Salesforce and Force.com, g) Facebook.

However, there is a confusion about what these “Cloud” services are, which are the benefits they offer, which are the possible drawbacks, and especially how safe are these services and how well protected are the privacy and personal data of users.

3.1 Key and Signature features of Cloud Computing

Regarding the cloud-based systems, as we can also see in Figure 2, the key features that compose them are:

- *Client Computers* (Mobile, Thin, Thick)
- *Data Centers* (Virtualizing Servers)
- *Distributed Servers*

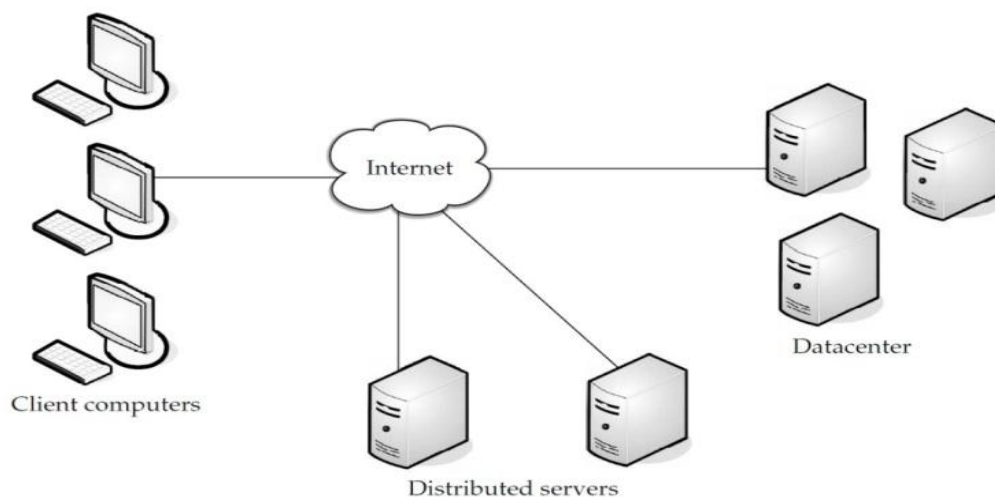


Figure 2: Key features that compose Cloud-based systems

There are five signature features of cloud-based Systems which make the difference against the traditional computational methods. These are:

- *On Demand Self-Service*: Consumers are able to use the computational resources that they need (such as the time they will use the server and the amount of storage that they will use through the network) without having to mediate with the provider of the service.
- *Broad Network Access*: These capabilities are available through the network and can be accessed through mechanisms and disparate platforms of users (e.g. mobile phones, laptops, tablets).
- *Multitenancy (Resource Pooling)*: Provider's computing resources are used to serve multiple consumers by using multiple tenants model, and with having physical and virtual resources dynamically re-assigned, depending on consumers' demand. Consumers have no control or knowledge of the specific positioning of the supplied resource, but they may be able to identify the location at a more abstract level, such as country, city or specific datacenter. Examples of such resources are storage, processing, memory, network bandwidth, and virtual machines. For the consumers – end users, the features that are available for them to attend, often appear to be unlimited and can be purchased – obtained in any quantity at any time.
- *Rapid Elasticity*: These resources can be bound directly, resiliently and many times automatically, and as a result they exhibit immediately a mark as unavailable and quickly to be released and reappear as available.
- *Measured Service*: Cloud systems automatically control and optimize the use of computing resources, by using measuring systems in one of the levels of abstraction that import, which is suitable for the particular provided service (storage, processing power, bandwidth, active number of users, etc.). The use of resources can be monitored, controlled and it is needs to be mentioned that provides transparency on both sides, the consumer – end user and the provider of the used service.

These are the features that make cloud-based systems an attractive option for businesses and even for government organizations.

3.2 Service Delivery Models (SPI Models) of Cloud Computing

There are three basic service delivery models in cloud computing (Figure 3). These three models are also called as “SPI Models” from their initials, which are Software, Platform and Infrastructure as a Service.

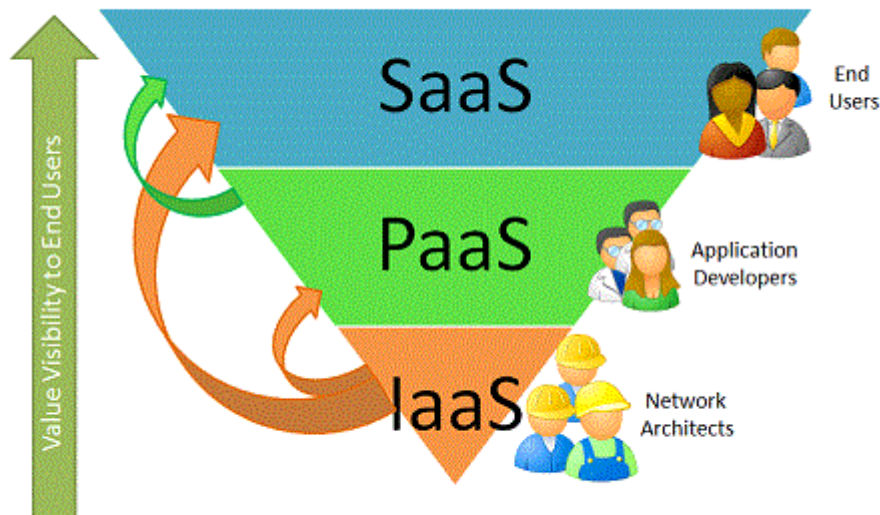


Figure 3: Service delivery models of a Cloud-based system

These three basic models can be defined, by analyzing them, as follows:

- *Software as a Service SaaS:* Consumers are provided with the ability to use on demand the provider’s applications that “run” in a cloud infrastructure. The applications can be accessed through multiple customer devices, such as a “thin” client or a web browser. Consumers are not able to manage or control the underlying infrastructure, that is comprised of the network, the servers, the operating systems and the memory, with the possible exception of the configuration settings of limited applications for specific users. For the suppliers the SaaS model is attractive, for the reason that provides effective protection of intellectual property, while it creates a continuous flow of income. Also this platform produces benefits for customers who do not tend to develop their own software, but are in need of applications with high demands on computing resources. Examples of SaaS are online word processing and spreadsheet tools, customer man-

agement services on the web, like Salesforce CRM, Google Docs. Figure 4 shows an example of a Software as a Service model.



Figure 4: SaaS Infrastructure

- *Platform as a Service PaaS:* Consumers are provided with the capability to develop on the infrastructure of the “Cloud” applications or acquired applications, by using programming languages and tools, which are supported by the provider, and the relevant API (Application Programming Interface). Consumers, as in SaaS, are not able to manage or control the underlying infrastructure. Though they have control over the applications that are being developed, and the ability to modify the environment and the performance of its applications. Examples of PaaS are Microsoft Azure, Force and Google App Engine. Figure 5 shows an example of a Platform as a Service model.

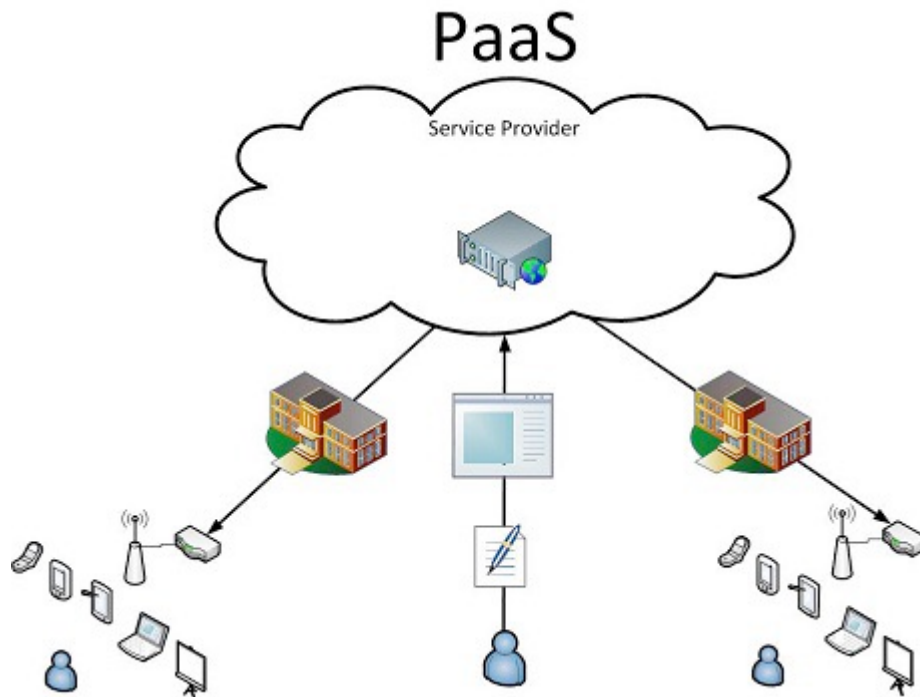


Figure 5: PaaS Infrastructure

- Infrastructure as a Service IaaS*: It is the management platform, through which is done the entire management of IaaS. Consumers are provided with the ability to develop and “run” any desired software, which can include operating systems and applications by using basic computer resources, such as processing power, memory and networks. Essentially, virtual machines and materials are provided, in abstract form, which the consumers have the ability to control through the supplied API. Consumers do not manage or control the underlying infrastructure, but they have control over operating systems, memory, developing applications and possibly limited control over selected parts of the network, such as firewalls (example, Host firewalls). Examples of IaaS are Amazon’s Simple Storage Service (S3), OneDrive, Dropbox and Rackspace Cloud. Figure 6 shows an example of an Infrastructure as a Service model.

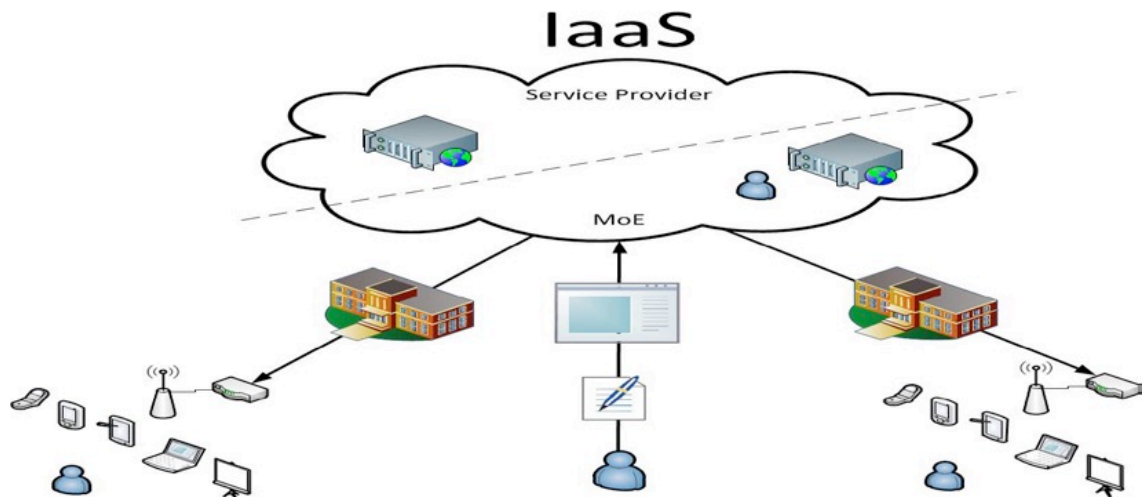


Figure 6: IaaS Infrastructure

3.3 Deployment Models of Cloud Computing

In addition to the Service Delivery models (SaaS, PaaS, IaaS), we can distinguish four Service Deployment models. These four models are:

- *Public Cloud:* By public cloud we mean a set of computer and computer networks resources, which are based on the cloud computing model and are available online, and in most cases supplied by a provider. As a model, public cloud is characterized by plenty advantages, some of which are: services are offered to users with safety, resiliency and continuous availability, and it is characterized by great flexibility due to the immediate supply of services and it charges only for the services that will be used. We can see an example of a public cloud at Figure 7.

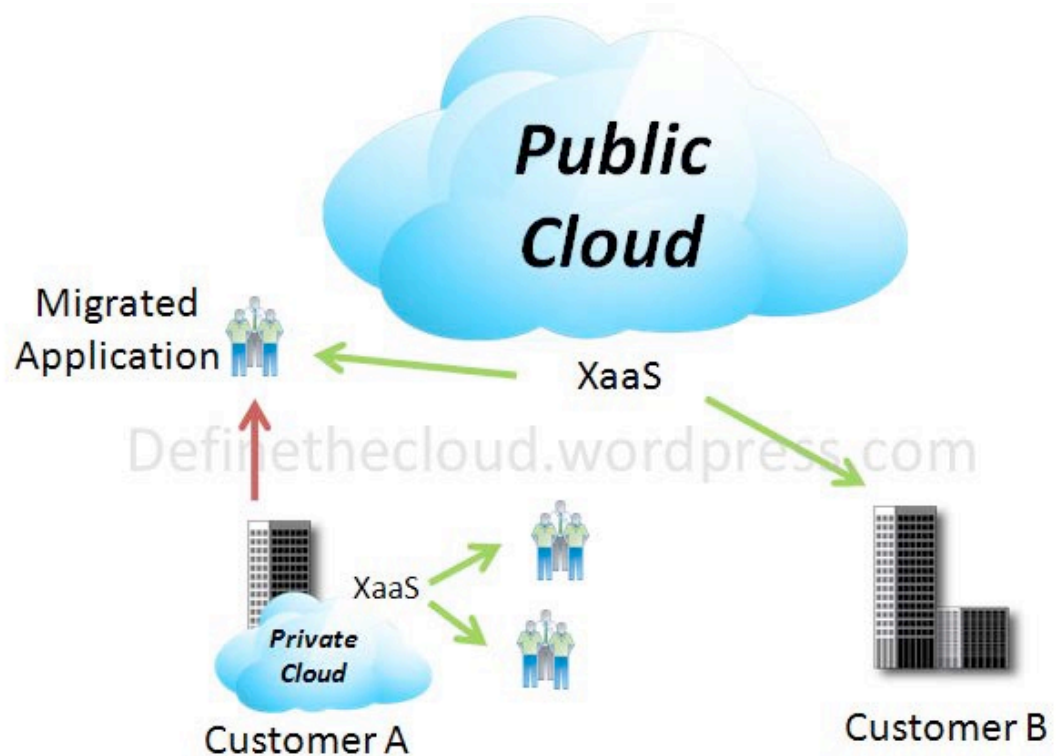


Figure 7: Public Cloud

- *Private Cloud:* It is a set of computing resources offered in a way to be designed, defined and controlled by a particular organization (Figure 8). A major disadvantage of private cloud is the high acquisition and operating costs. Frequently, it is confused with Virtualization, which however is only a small portion of it. Private cloud subjects to the security restrictions of the organization, due to the implementation of the framework of an existing data center of an organization, thus providing greater security to sensitive data. Finally, private cloud stabilizes and optimizes the performance of existing hardware, in a particular data center, through the Virtualization technologies that they use, thus reducing operating costs and improving the efficiency of the data center. [31]

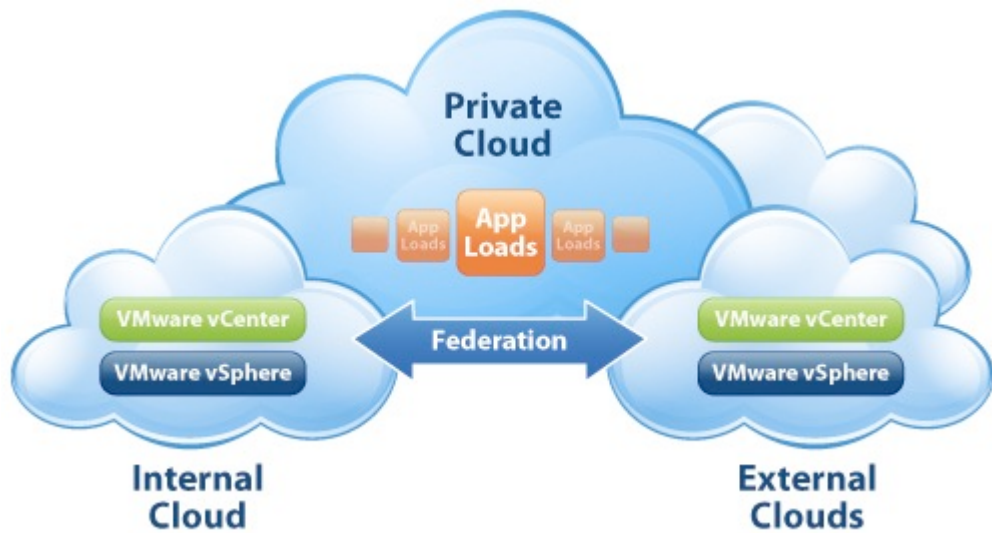


Figure 8: Private Cloud

- *Community Cloud:* This model has a structure which is divided by many organizations and serves a specific community. This community has as a common ground a particular goal or interest. This model has a feature that can be managed by an agency or letting a third party organization or company have authority over it. Figure 9 shows an example of a community cloud model. [32]

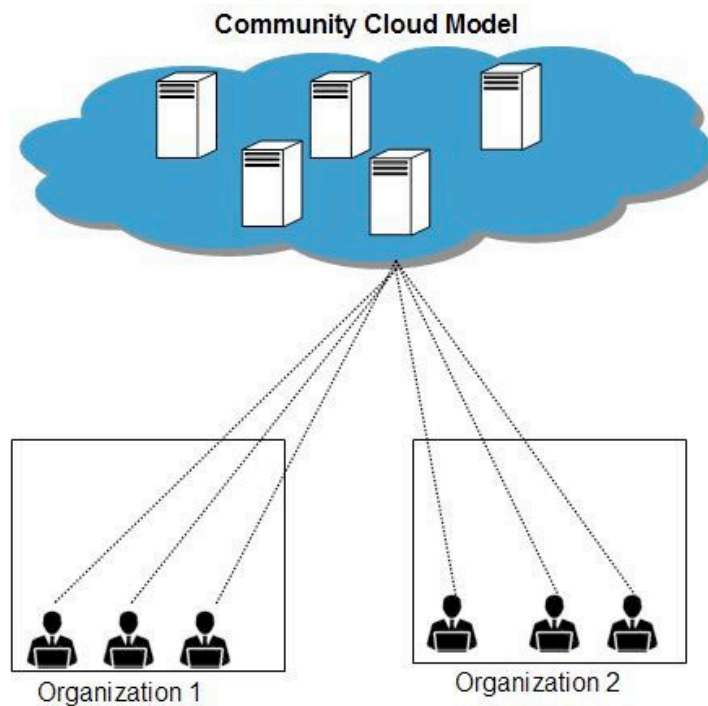


Figure 9: Community Cloud

- *Hybrid Cloud*: This model combines resources from public cloud, or resources from one or more private cloud, and even a combination of both. Figure 10 shows an example of Hybrid Cloud model.

A hybrid cloud can provide users with the following[33]:

- *Scalability*: While private clouds offer a certain level of scalability, depending on their settings (for example, either hosted internally or hosted externally), public clouds offer scalability with fewer limitations, because resources are diverted from the larger cloud infrastructure.
- *Cost Saving*: public clouds are likely to offer more significant scaling economies (such as centralized management), and thus more cost-effective than private clouds. Therefore, hybrid clouds are making possible for organizations to save money, while maintaining sensitive secure operations.
- *Security*: private cloud as an element of hybrid cloud does not only provide security, where this is necessary for the sensitive functions, but it may also fulfill the regulatory requirements for handling and storage, when it is possible to be applied.
- *Flexibility*: Availability of resources can provide organizations with more opportunities to explore various business directions.

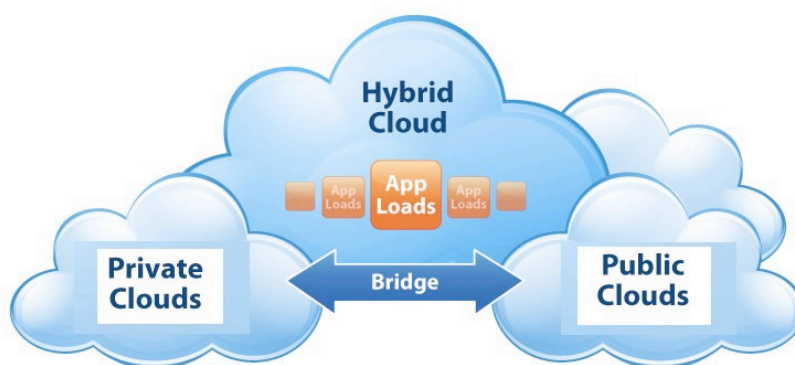


Figure 10: Hybrid Cloud

An organization can implement a model or many different deployment models, depending on the cloud model that provides the best solution. For example, a critical applica-

tion that has as a purpose to maintain or any other specification of security, may require a hybrid or a private cloud model. In contrast, a generic application that can be required for a temporary work, may be ideal for a public cloud. We can see a table with all the attributes of the Deployment models at Figure 11.

	Private Cloud	Community Cloud	Hybrid Cloud	Public Cloud
Infrastructure Ownership Model (Ownership of Physical Infrastructure such as facilities, network, compute and storage)				
Service provider owned	X	X	X	X
Government owned	X	X	X	X
Third Party Vendor owned		X	X	
Infrastructure Location				
On-Premise (Internal or behind the firewall)	X	X	X	
Off-Premise (external or outside the firewall)	X	X	X	X
Operations Model (responsible party for applying the security controls, patching, etc)				
Service Provider Operated	X	X	X	X
Government Operated	X	X	X	
Third Party Vendor Operated	X	X	X	
Governance Model (Responsible party for ensuring compliance to policies and standards, etc)				
Service Provider			X	X
Government	X	X	X	
Third Party Vendor			X	X
Data Security Level				
Low	X	X	X	X
Moderate	X	X	X	
High	X	X	X	
Cost Model				
Upfront Capital expenditure	X	X	X	
Ongoing support cost	X	X	X	
Demand based Service fee			X	X
Time to deploy				
Immediate				X
Mid term		X	X	
Long term	X			
Accessible and Consumed By				
Admin Users	X	X	X	X
Trusted Consumers(Employees, Contractors)	X	X	X	X
Public Consumers (Authorized to consume services but not legally a part of the organization/Government)			X	X
Service Types				
Citizen Engagement Services			X	X
Software-as-a-Service (SaaS)	X	X	X	X
Platform-as-a-Service (PaaS)	X	X	X	X
Infrastructure-as-a-Service (IaaS)	X	X	X	X
Traditional hosting Services	X	X	X	

Figure 11: Deployment model matrix

3.4 Cloud Storage

Saving in cloud (Cloud Storage) or else file hosting, is the storage of computer data in remote infrastructure, and not to local storage devices that are connected to the computer.

There is a large number of providers of cloud storage services, many of which offer free storage services, such as Dropbox, SpiderOak, Box etc. Access to these various services

can be accomplished in various ways. The user can install the application software on a computer or use a browser.

Cloud storage can be used by criminals to store illegal data and provide a distribution point that does not connect the owner or users with the illegal data. In other words, it provides a difficulty in accountability of ownership or correlation with illegal data. The data stored in the cloud can also be targeted by cybercriminals, who may be able to gain access to the victim's account and the data contained therein. [22].

The security of cloud services is handled properly, but from a forensic standpoint, cloud storage does not ensure the forensic readiness or the facilitation of forensic analysis.

Law enforcement agencies and investigators need to have access to the data stored in the cloud storage accounts. The difficulties arise from the attempt to apply traditional forensic investigation methods in a cloud environment. In a typical investigation of a computer, the physical material is seized, a copy is created, and the analysis is performed at this duplicate. In a cloud storage environment, the hardware is housed in a large data center, which may be located in another country, and the can be distributed over many such data centers around the world. Therefore, physical analysis is the least challenging [21].

3.5 Digital Forensics and Cloud Storage

Crimes related to cloud storage can be classified according to the definitions of cyber-crime. Cybercrime can include crimes where a computer is used as a tool, target, or as a storage device. The data stored in the cloud may be the target of criminals, while cloud Storage can be used to store illegal data or data related to a crime. Cloud services can also be used as a tool for committing a crime. It has been reported that a virtual server of Amazon's EC2 cloud service has been used in the attack that led to the disruption of Sony's PlayStation Network service [25].

The difficulty of accessing the hardware to detect evidence, is a challenge for researchers. The "key" evidence may be distributed across multiple data centers in different countries. Given this, there may be legal and jurisdictional issues that must be addressed by researchers.

The identification of the actual suspects in the cloud environment is also an issue. By confiscating a computer or a device, there may be evidence of ownership or correlation to an individual. Instead, in the operating environment of a cloud application, this corre-

lation may not be possible. The use of anonymous networks, like TOR (The Onion Router), for accessing a cloud storage account, may hinder the investigations [11].

Finally, another issue faced by forensic experts is the identification of the service providers and their accounts, such as user names and passwords. The analysis of user devices, such as hard drives, network traffic, or mobile devices, can provide this information.

4 Examination of RAM

A large portion of our research will focus on the analysis of RAM. For this reason, it is necessary to specify the type of evidence that we can find in RAM. Finally, since this is a type of volatile memory, we will try to clarify the lifetime of data and the factors on which it is connected.

While traditional computer forensics involve the study of non-volatile storage media, such as hard drives and USB devices, memory forensics involve the conception and analysis of volatile memory, such as the RAM.

Data are considered volatile, when they are likely to be lost after a restart of a system or be replaced during its normal operation. Such data are often not structured in the same way as file systems, and it can be more difficult to be identified and analyzed in meaningful conclusions. However, the information that can be retrieved from the volatile data are often valuable in facilitating research, while many types of data can only be recovered from RAM [29].

4.1 The role of RAM analysis in modern digital environment

The forensic examination of memory has the potential to contribute significantly to any investigation. It is extremely valuable since it overcomes several limitations of traditional forensic analysis, and even helps to address the problems posed by new technologies, such as encryption. Since technologies continue to evolve, the forensic examination of RAM will become increasingly critical to effectively collect the requisite evidence.

4.2 Forensic Analysis of RAM

The analysis of the volatile memory is a less precise and defined process than the analysis of a hard disk drive. Hard drives have a strictly predetermined structure, and analysts know where to look for certain structures and data types in a specific file system. (for example FAT 32). As far as the volatile memory is concerned, it is impossible to predict what will be found or where it will be saved. This is due to the fact that the volatile

memory is partitioned into different areas depending on which part of the memory is used.

4.3 Types of Evidence that can be found in RAM

Various types of evidence are available in the computer's memory. The volatile and transient forms of evidence include (Amari, 2009):

- The “active” processes and services.
- The decrypted versions of programs.
- System information (e.g. time elapsed since the last reboot).
- Information for the online users.
- Registry
- Active network connections.
- “Artifacts” of conversations and communications in social media and MMORPG games.
- Recent communications over Webmail systems.
- Information from Cloud services.
- The decryption keys for the encrypted disks at the time of memory recovery.
- Recent images seen by the user.
- Malware

4.4 Legal Implications of RAM Recovery

It is important to realize that the process of retrieving the volatile memory will inevitably leave its footprint to the system. While this may be acceptable to the analyst, it should be taken into account the laws governing this process. A proper and step by step documentation of memory's retrieval is necessary for the collection of evidence that correspond to the applicable legal framework.

4.5 Limitations of RAM Analysis

The analysis of RAM has its limitations. Many types of data that are stored in computer memory are ephemeral. The information about the running processes will not disappear until you stop their execution. The situation is however not the same with the other con-

tents of RAM. The residues of the recent discussions, communications and other user activities can be replaced by other data, whenever the operating system requires another memory block [13].

4.6 Tools and Techniques

There is a series of tools and methods available for retrieving the volatile memory. From a forensic standpoint, there are certain conditions that any such a tool should fulfill. These conditions are:

- Operation at kernel level
- Portability
- Only reading permissions for the data
- Leaving as small digital footprint as it is possible

Operation at kernel level is a prerequisite for such a tool. Many applications have safety precautions against RAM acquisition methods. At best there will be a series of zeroes instead of the data, and in the worst case scenario the application will take immediate measures for the destruction of the protected information and the system's restart. For this reason, it is required that the tool is running at kernel level.

These tools should be portable and ready to "run" from a device which is provided by the investigator (e.g. an external USB device). Moreover, no forensic tool should ever alter or modify the data that are analyzed.

Lastly, the smaller footprint left by a memory acquisition tool, the better. The use of a tool that leaves footprints, may eventually lead to the destruction of certain evidence [19].

4.7 Data Preservation in RAM

The purpose of this thesis is not to identify and examine how the volatile memory behaves and operates. However, in the framework of our investigation we should clarify the lifetime of data in volatile memory and the factors that are influencing them.

So in this section we will try to gain some insight into the lifetime of the data that are stored in RAM (e.g. For how long will a program remain loaded in memory, when it had been loaded into memory while running? - While a program is still running, will it continue to reside in memory?).

After the program's termination, will follow the reallocation of the memory that have been used. This action cannot be fully and precisely defined. There are a number of factors that can affect the distribution, redistribution and replacing of volatile memory [27].

Figure 12 below informs us about the preservation of memory data in a Solaris OS [19].

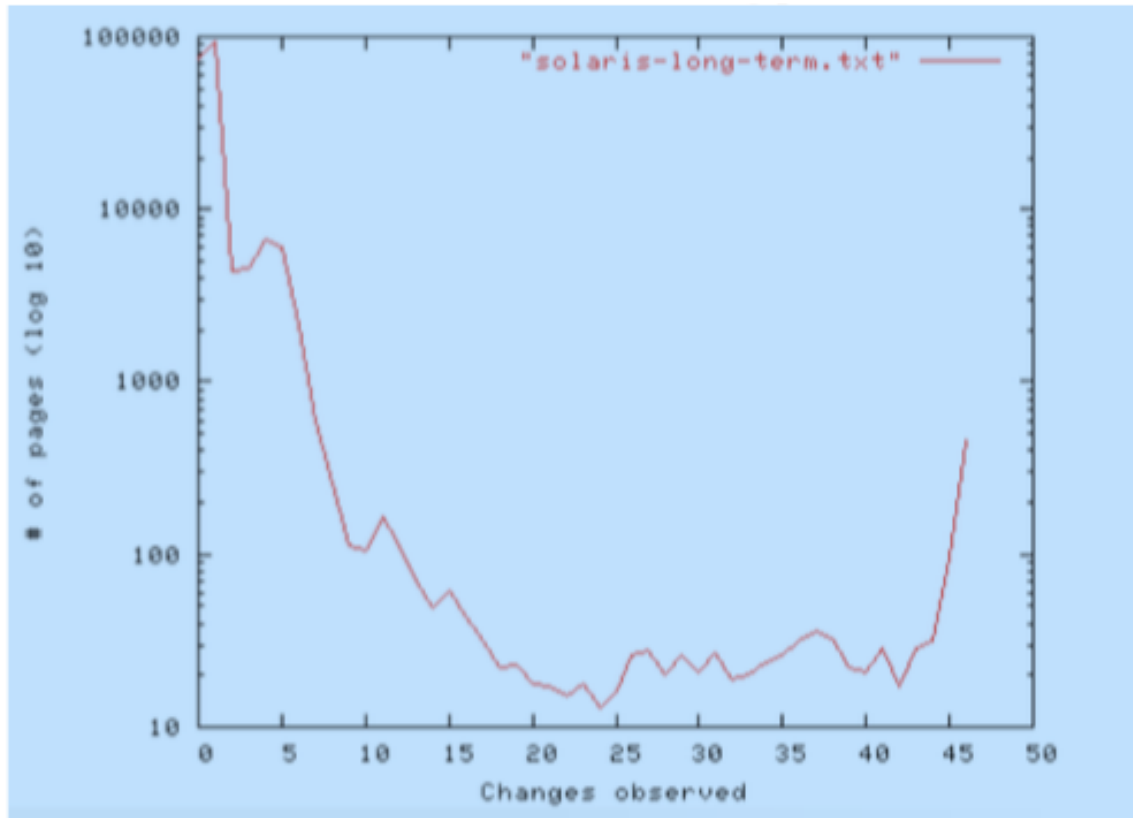


Figure 12: A graph of the number of changes in memory over time on a Solaris 8 machine set up as a DNS server with 768 MB of RAM

At this graph, axis xx' represents the days that the machine was running, and axis yy' the number of pages that have changed. In this study 86% of the memory was not altered.

Moreover, in the context of this research it has been proved that the metadata of various processes and other data, remained in memory for more than 14 days, while the system was used. Finally, we should mention that the possibility for the data to be replaced in memory is connected with the user's activities.

4.8 Conclusions

Summarizing, we can define the factors which affect the preservation of data in volatile memory. The type of operating system is an important factor, as is the available memory. The less effective the operating system is in the distribution of available

memory, the more sporadic will be the distribution. Moreover, the level of activity on the machine plays a huge role.

5 Methodology

Our next goal is to create a methodology adapted to the specificities of cloud services by using the theoretical background of the previous chapters. However, in order to achieve this, we will need to define the general rules that should govern such a methodology. Finally, we will present the methodology on which we will rely to create our own.

The science of Information Technology, in one way or another, is associated with most criminal investigations. Public prosecutor may issue a warrant for the investigation of emails and electronic documents of people who are suspected of murder or child pornography. Private companies are monitoring the personal computers of their employees, aiming to prevent leakage of company's secrets to competitors. Scams are ascertained through the collection and analysis of data, from the information system, of the organization which is under investigation. So there is a need for standardization of this specific process, through a commonly accepted methodology.

5.1 Requirements

The methodology of tracing digital evidence should be practical and based on the general procedure of collecting evidence. It should not be affected by technological changes, but it should be adjusted according to the constraints and specificities of the case and the environment in which it occurred. However, the most important requirement is that it should be well structured, in a way that the standardization will be in the form of an online tool.

Over the years, many digital forensic models have been proposed. In our research we will rely on the Law Enforcement Process Model, which we will present below.

This data collection and evaluation methodology had been standardized by the United States' Department of Justice. It is comprised of the following steps:

- *Preparation:* Knowledge about the types of devices commonly encountered, potential evidence sources, investigative tools, and equipment for collection, packaging and transportation of electronic evidence.
- *Preservation:* Securing and evaluating the crime scene; ensuring the safety of persons and protecting the integrity of all evidence.

- *Documentation*: Documentation of the scene, and electronic evidence.
- *Collection*: “The search for, recognition of, [and] collection of... electronic evidence.”
- *Examination*: “Helps to make the evidence visible and explain its origin and significance.”
- *Analysis*: “Looks at the product of the examination for its significance and probative value to the case.”
- *Reporting*: “A written report that outlines the examination process and the pertinent data recovered completes an examination.”

(Law Enforcement Process Model, 2008) – (Cybercrime and Cloud Forensics: Applications for Investigation Processes)

5.2 Proposed Methodology

In the previous chapters we have defined the general laws and rules that govern digital forensics. Then we defined cloud technology, cloud storage and how its use affects forensic investigations. Lastly, we mentioned in a separate chapter, the special role that RAM can play in digital forensics.

Using the theoretical background of this chapter and the conclusions of the previous chapters, we will create a methodology that can easily, efficiently and reliably be used for the forensic analysis of cloud services. The Law Enforcement Process methodology is the standard by which we will create our own framework of investigation.

In the following figure (Figure 13) we are presenting the proposed methodology and then we summarize its steps.

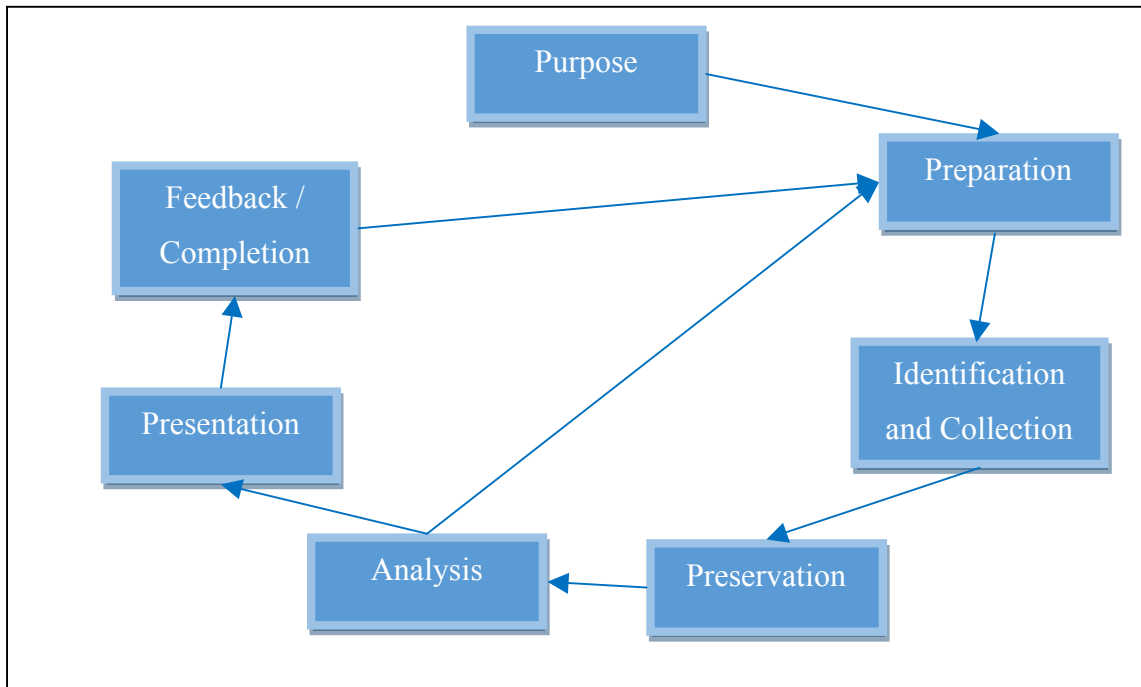


Figure 13: Proposed methodology

5.2.1 Purpose

At the beginning of an investigation it is important to define the purpose, nature and background of the analysis. We also have to define the boundaries of our research. At this stage we will mention the people that are involved, keywords, timetables that need to be respected, and any other relevant information. The primary purpose of the research can be quite generic, and as it progresses to focus on any issues that may arise.

5.2.2 Preparation

After defining the purpose, the next step in the investigation is the understanding of the requirements, and to ensure that the correct equipment and information are available. This step may include the acquisition of equipment and training of the investigators.

The preparation may also include the investigation of a particular program or a technology in general. For example, if the research is associated with a specific cloud storage service, the investigator may initially conduct a research by using virtual machines to understand the “behavior” and functioning. At this stage, the schedule of the investigation, the staff and its tasks are getting defined.

5.2.3 Identification and Collection

The next step, in a typical forensic investigation is the identification and collection of digital data. It includes the procedures and methods for recording the scene of the crime, as well as the operations that were performed for the collection of evidence and their safe storage.

In this phase, the investigator may discover that cloud storage services are being used. In this case, the investigator, firstly, will contact the service provider. If he is in possession of information that the provider can use (user name, access dates), then the provider, according to the current legislation, may grant access to the data.

5.2.4 Preservation (Forensic copy)

It is the absolute replica of the original digital evidence, by using standard and accepted practices. The complete and thorough recording of our steps ensures the reliability of our operations.

5.2.5 Analysis

At this phase, the significance of the collected data is defined, and the conclusions are summarized based on the evidence that were found. In case of discovery of new data, the process returns to the step of Preparation. The analysis will be continued with the already replicated data, and the new data will be analyzed when they will be available.

5.2.6 Presentation

In the next stage of our methodology, the data are recorded and presented to the assignors. The specialist should present his findings in a clear, concise, well-structured and precise report, in which he will explain all the conclusions that he has reached. The creation and use of a timeline of events will contribute to the understanding and explanation of the events' sequence.

5.2.7 Feedback / Completion

Feedback is the next step in our research. Therefore, we evaluate the results of our investigation, the correctness of the procedure and if the practices that we applied are recommended for reuse. The final step is the completion of the investigation. Based on investigator's feedback, the process may return to the Presentation phase. If no further investigation is required, then the case can be completed.

6 Investigation Methodology

6.1 Investigation Problem

As we have already mentioned, cloud is used to store large amounts of data, including illegal data and evidence of criminal acts. We notice that there is a lack of information about forensic analysis of cloud storage and the data remnants that are created by its use. Finally, there is a lack of information about the alterations, if any, that may occur to the files after the use of this service.

6.2 Investigation Purpose

The purpose of this research is to answer the investigation problem that was analyzed in the previous subchapter. Our goal is to determine whether there are data which will prove that there was an access and use of such services, and if there is a method for the identification and preservation of data that are related to these services.

The findings of our research will assist forensic investigators in identifying the use of cloud storage service and in providing a methodology for the identification and preservation of digital evidence by a widely acceptable forensic procedure.

6.3 Investigation Questions

The two questions that will try to answer, will be analyzed in the following subchapters.

6.3.1 Investigation Question 1

Which are the evidence / data remnants that are created by the use of cloud services and allowing us to verify whether in fact there was a use of such services?

This question leads to the following cases:

Case 1: There are no data remnants from the use of cloud services which will help with the identification of the service provider, the user's name, or the files that were transferred.

Case 2: There are data remnants from the use of cloud services which allow the identification of the service, the user's name, or the details of the files.

The 2nd case leads us to the following sub-questions:

- Which are the data that remain on the computer after the installation of the application software and its use for uploading and storage of data?
- Which are the data that remain on the computer after accessing the cloud service through a browser?
- Which data remain in the volatile memory when the application software is used, and which remain when a browser is used?

6.3.2 Investigation Question 2

The second question is the following:

How will the file upload and download processes, of a cloud service, affect the internal files and metadata?

6.4 Experimental Procedure

We will implement this procedure to answer the investigation questions, regarding the use of cloud storage services like Box. The diagram in Figure 14 presents the procedure that will follow. Starting with a “clean” installation, Box cloud storage service was examined in a variety of scenarios that involved the use of the application software and two different browsers. In each of these scenarios we retrieve and maintain the contents of the RAM and the hard drive of the computer system.

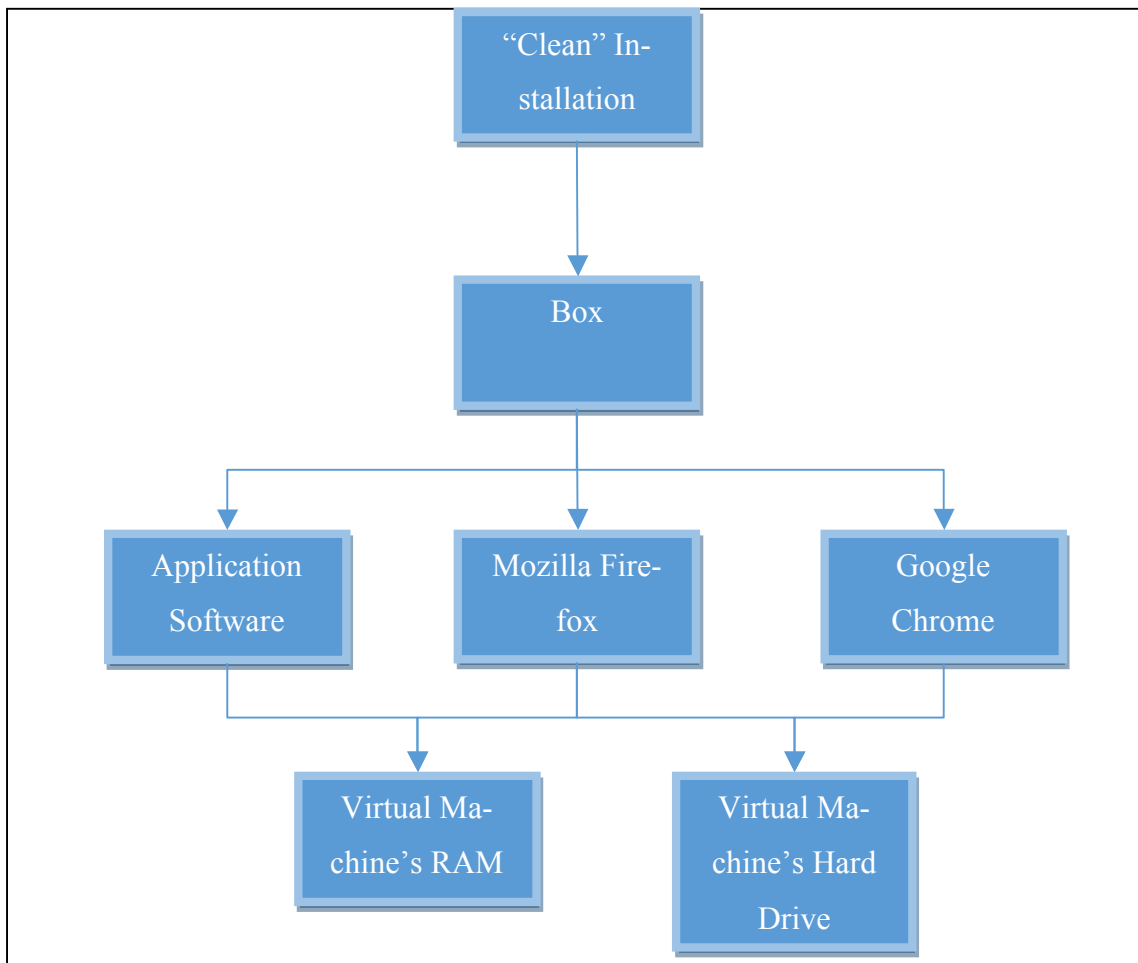


Figure 14: Investigation's experimental procedure

For the examination of these different scenarios, a number of Virtual Machines (VM) were created. The virtual machines allowed us to easily and quickly, use and examine Box cloud storage service. Also we were able to examine Box cloud storage service in conjunction with different browsers: Mozilla Firefox (FFX) and Google Chrome (GC).

If this procedure had been done through hardware, the needed time and generally the resources for the installation, deletion and re-installation would be burdensome.

6.4.1 Experimental Procedure for Answering the First Question

At the following tables we present the steps that we take, in the context of our investigation, to answer the first question that we posed.

Table 1: Investigation steps by using the Application Software

Steps	Procedure
1.	Installation, in a “clean” VM, of the cloud application software that we will use.
2.	Uploading of files from the computer to the server of the service, through the installed software.
3.	Recovery of the virtual machine’s volatile memory and the creation of its hard drive’s image.
4.	Examination of the data, to find information, and extraction of useful conclusions.
5.	Repetition of the procedure from step 1, in a new “clean” VM, though this time we will be downloading the files that are stored in the application’s server.

Finally, this procedure will be repeated for the Box cloud storage service through a browser.

Table 2: Investigation steps through the use of a browser

Steps	Procedure
1.	Installation, in a “clean” VM, the browser that we are going to use.
2.	Uploading of files from the computer to the server of the service through the browser.
3.	Recovery of the virtual machine’s volatile memory and the creation of it’s hard drive’s image.
4.	Examination of the data, to find information, and extraction of useful conclusions.
5.	Repetition of the procedure from step 1, though this time we will be downloading, through the browser, the files that are stored in the application’s server.

6.4.2 Experimental Procedure for Answering the Second Question

To answer the second investigation question, we use a different experimental procedure. We select the data that we will use and then we upload them, in the Box cloud storage service.

Thereafter, a different computer system is used for accessing the storage service and for downloading the files, which we will examine. The download of these files can be performed either by using the service’s application, or through a browser. Lastly, an analysis is performed to compare the original files with the ones that we downloaded. The procedure is summarized in the following tables:

Table 3: File handling through cloud storage service’s software

Steps	Procedure
1.	Creation of a new VM which will be used for accessing Box cloud application.
2.	Use of the VM and connection to the cloud application by using a browser and log in to the account that we use for this investigation.
3.	Browsing the files.
4.	Download the files that we are concerned with. Examination of files' metadata.

Table 4: File handling through a browser

Steps	Procedure
1.	Navigation to the page of the cloud storage application. Download and installation of its software.
2.	Account synchronization.
3.	We notice that the contents of the account are downloading to the VM.
4.	Examination of files’ metadata.
5.	Shutting down the virtual machine.

6.5 Hardware

The specifications of the computer system that we will use are described in the following table.

Table 5: Investigation's computer system

Investigation's computer system	Personal Computer
Operating System	Windows® 7 64-bit Ultimate SP1
Processor	Intel® Core™ i7-2600k @ 3.4 GHz
RAM	16 GB Dual-Channel DDR3 @ 1600 MHz
Storage	1TB Western Digital Hard Disk Drive 1TB Western Digital External Hard Drive

6.6 Software

In the following subchapter, we will briefly examine the tools and programs that we are going to use in our investigation. Programs which are used in the investigation procedure:

Access Data FTK Imager (version 3.4.3)

It is a suite of tools that provides us with data preview capabilities and image creation. It allows us to quickly evaluate digital evidence, in order to be able to determine if further investigation is required. Finally, it grants us the ability to create duplicates of digital data, without bringing about changes to the original evidence.

HexEdit (version 4.0)

It is a free editing program that allows us to analyze the files, regardless of size and type, in hexadecimal format.

DumpIt (version 1.3.2 revision 20110401)

It is a utility program that works in a console environment. It is a small executable file (517KB) that allows us to store the contents of RAM.

Oracle VM VirtualBox (version 5.1.10 revision 112026)

This is the program that we will use to create virtual machines. We should make a special mention of Snapshot mode that VirtualBox provides and which we will analyze subsequently.

ProDiscover Basic (version 7.0)

It is an image creator tool of various storage devices.

OSForensics (version 4.0.1001)

OSForensics is a digital research tool that allows us to extract data or to discover hidden information in a computer. It offers a variety of advanced features.

As part of our investigation we will use the operations of creating signatures of an operating system and the execution of hash function to verify the data integrity. Finally, we should mention that it is possible to install OSForensics to a removable storage device.

The following figure (Figure 15) shows the program's interface and the features that it offers.

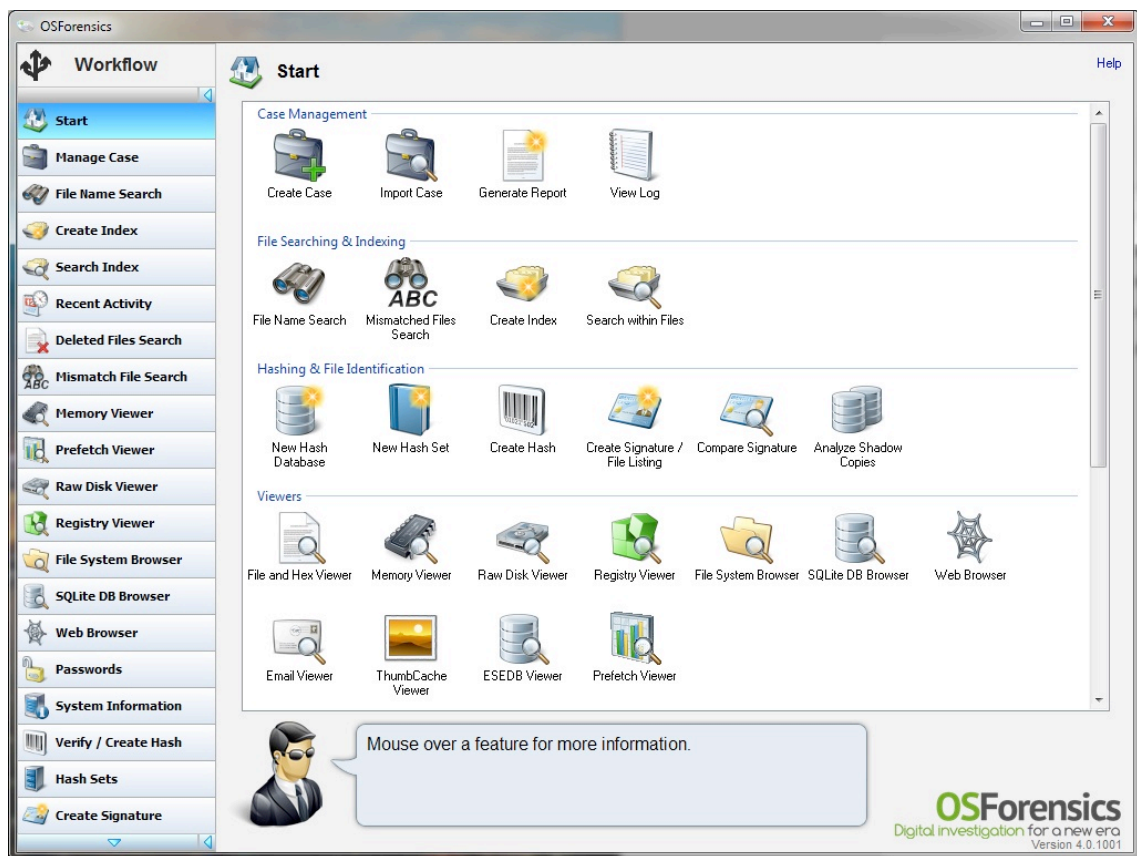


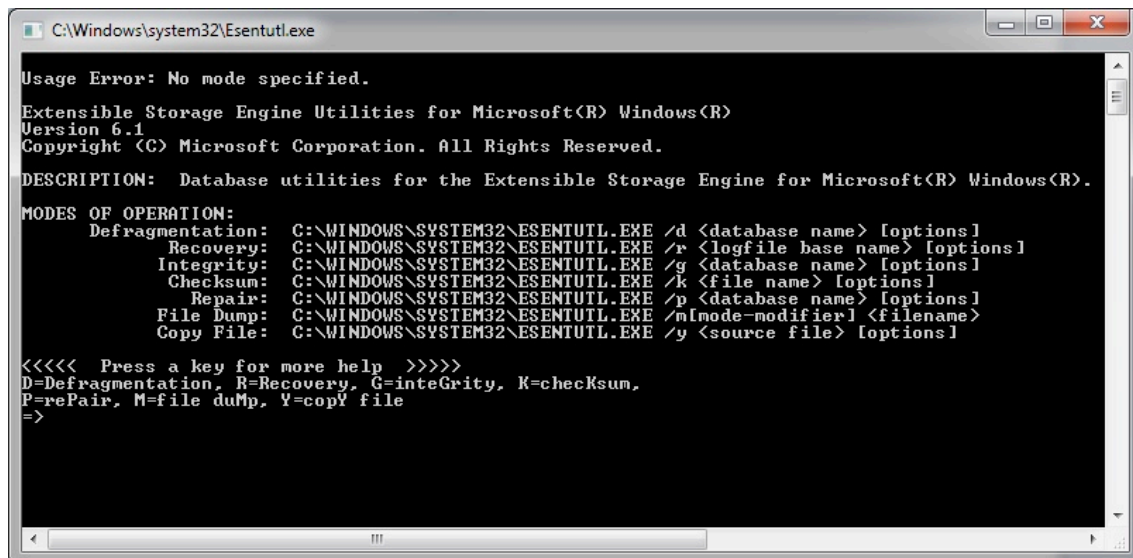
Figure 15: OSForensics interface

ESEDatabaseView (version 1.42)

ESEDatabaseView is a program of Nirsoft that was built to provide access to ESE (Extensible Storage Engine) databases. We use it to get an overview of the database and to verify the data that are stored there, because of our experiments.

Esentutl.exe

It is a command line tool that is integrated to Windows (as we can see at Figure 16). It provides utilities for the ESE databases and could, among other things, be used to display the metadata, or to recover an ESE database.



```
C:\Windows\system32\Esentutl.exe

Usage Error: No mode specified.

Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 6.1
Copyright (C) Microsoft Corporation. All Rights Reserved.

DESCRIPTION: Database utilities for the Extensible Storage Engine for Microsoft(R) Windows(R).

MODES OF OPERATION:
  Defragmentation: C:\WINDOWS\SYSTEM32\ESENTUTL.EXE /d <database name> [options]
  Recovery:       C:\WINDOWS\SYSTEM32\ESENTUTL.EXE /r <logfile base name> [options]
  Integrity:     C:\WINDOWS\SYSTEM32\ESENTUTL.EXE /g <database name> [options]
  Checksum:     C:\WINDOWS\SYSTEM32\ESENTUTL.EXE /k <file name> [options]
  Repair:       C:\WINDOWS\SYSTEM32\ESENTUTL.EXE /p <database name> [options]
  File Dump:   C:\WINDOWS\SYSTEM32\ESENTUTL.EXE /m[mode-modifier] <filename>
  Copy File:   C:\WINDOWS\SYSTEM32\ESENTUTL.EXE /y <source file> [options]

<<<< Press a key for more help >>>>
D=Defragmentation, R=Recovery, G=integrity, K=checksum,
P=rePair, M=file duMp, Y=copy file
=>
```

Figure 16: Esentutl.exe command line tool

CCleaner (version 5.24.5841)

It is a program that is used to clean our operating system from unwanted files and invalid registry entries.

Eraser (version 6.2.0.2979)

Eraser is an advanced security tool for Windows that allows us to completely remove sensitive data from our hard drive.

DB Browser for SQLite (Portable version 3.9.1)

As the title indicates, it is a free tool that allows us to create, design and edit SQLite databases.

Kali Linux (version 2016.2)

Kali is a Linux distribution that made a great effort of collecting and utilizing digital forensics software. We can download and use Kali, in the form of Live CD.

It is a parameterized operating system based on Ubuntu Linux distribution, which contains many useful tools that contribute to the work of a forensic investigator. A key advantage of this approach is that we operate in a non-changing or “dead” environment (Dead Analysis), which is appropriate way for computer forensic investigations.

Dcfldd

The command “dd” of Linux allows users to do a bit-to-bit copy of a medium. The tool dcfldd works similar to the command “dd”, but it has many features designed for the computer forensics.

Lastly, we should mention that the programs we use, are installed / stored in an external storage drive with size of 1 TB. This allows us to execute these tools quickly and easily, without making any changes to the computer that we investigate.

6.7 Creation of Virtual Machines

The Virtual Machines were created with Oracle’s VirtualBox v 5.1.10. Firstly, we created a VM, in which we installed the operating system of Windows 7 Ultimate 32-bit, on a virtual drive with a maximum size of 25 GB (NTFS) and 1 GB of RAM. As part of our research, we chose to allocate to our operating system the least resources possible, to limit the amount of data, which we will need to examine.

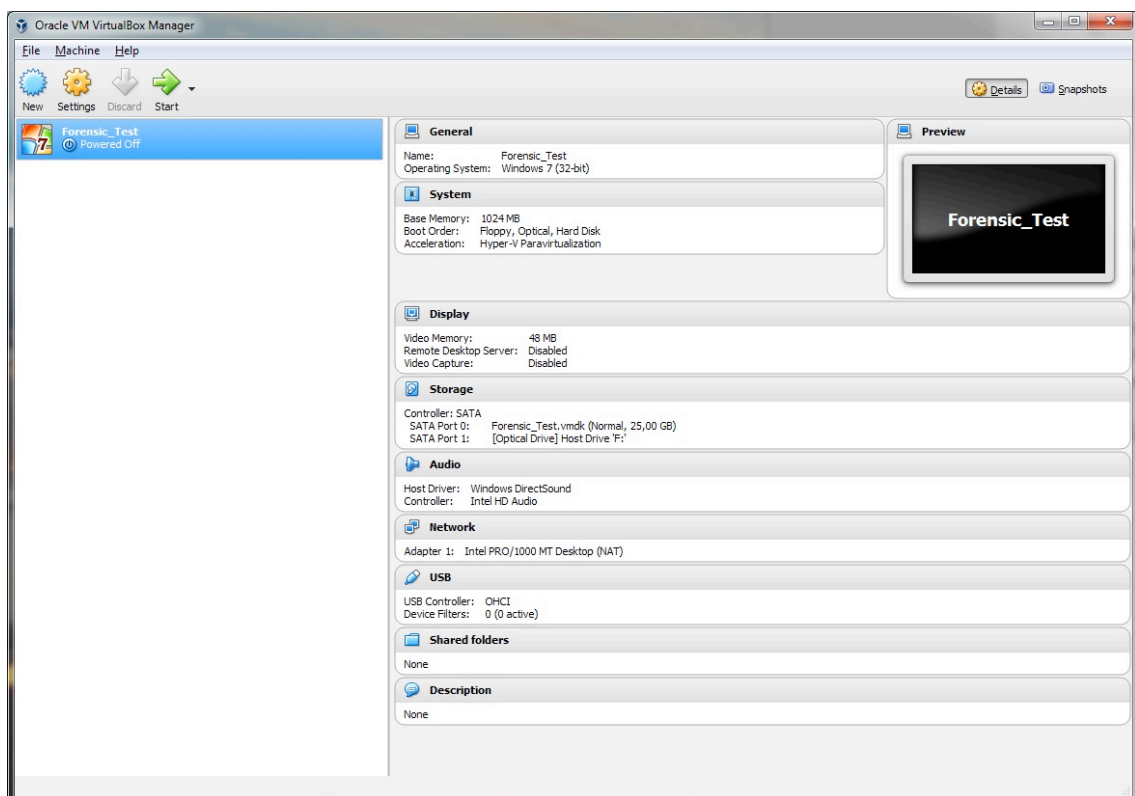


Figure 17: Virtual Machine’s features

For each scenario that we will examine, the creation of a new and clean VM is required, in order to exclude any possibility of finding any data that does not correspond to reality.

To avoid the time consuming process of creating new virtual machines and install the operating system of Windows, we will use the option of Snapshot (Figure 18).

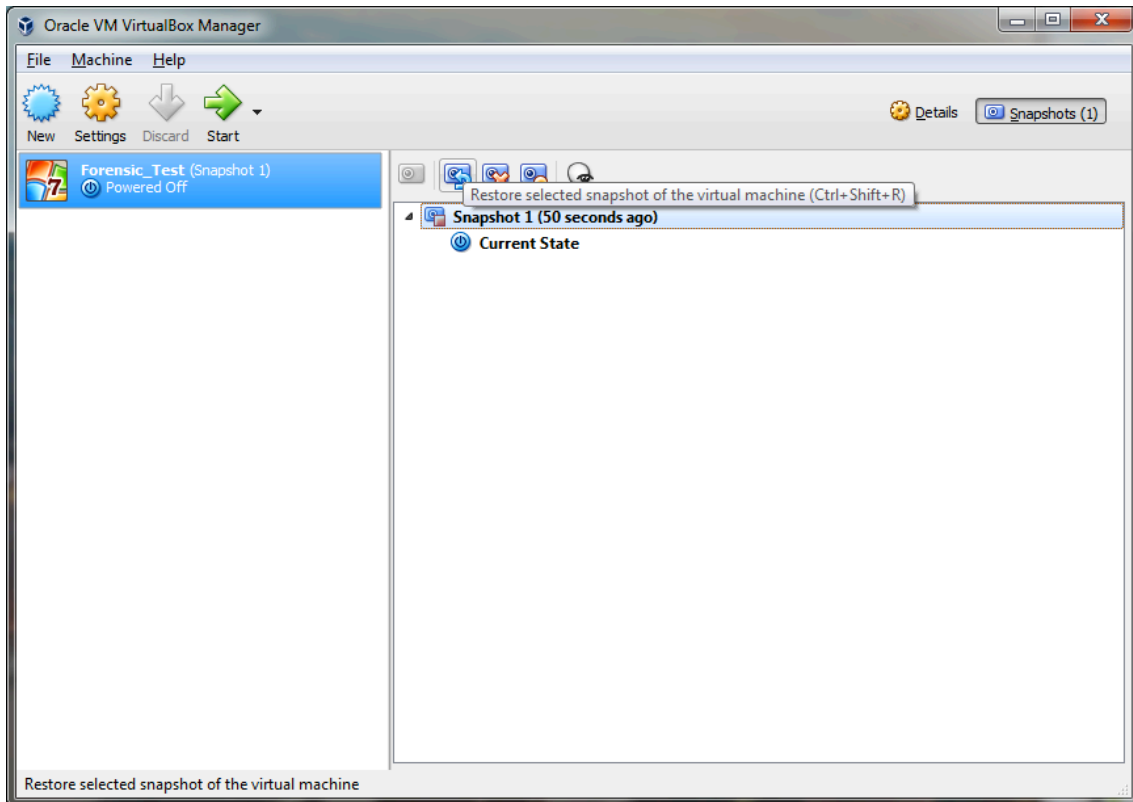


Figure 18: Virtual Machine's Snapshot

The Snapshot mode is used when we want to maintain the exact state of a virtual machine, in order to return to it repeatedly. A snapshot maintains the virtual machine exactly as it was when we took the snapshot. When we return to a snapshot, we discard all the changes that were made to the virtual machine by the time we took this snapshot.

6.8 Files

In our investigation we will use a variety of files. These files belong to several categories (e.g. .pdf, .jpeg, etc.). Specifically, we will visit the website of DigitalCorpora. This is a website that is used in the digital forensics training. It provides access to a number of files such as disk images, network packet dumps, cell phone dumps, etc.

We will select a set of files that we will use in our investigation. Finally, this website provides to us the ability to easily and quickly find the hash value and the metadata of the files that are of interest to us. The files are presented in the table below.

Table 6: Presentation of the files that we will be handling

Name	Size (bytes)	MD5 Hash	Date (Created/Accessed/Modified)
019192.jpg	62.206	5c1a7be3a7745f08da5c0f098ac5b975	25/11/2016
020958.txt	34.766	284ac397b1b5628c07884baca3939969	25/11/2016
028620.pdf	888.697	6294833fde8cb43dd82998ecbd93294f	25/11/2016
093340.doc	3.515.904	90a08c197d52a0d5f027ce44c8fb0a5f	25/11/2016

Afterwards we verify, by using the OSForensics toolset (as we see in Figure 19), that the hash values of the files, which we downloaded, remain unchanged.

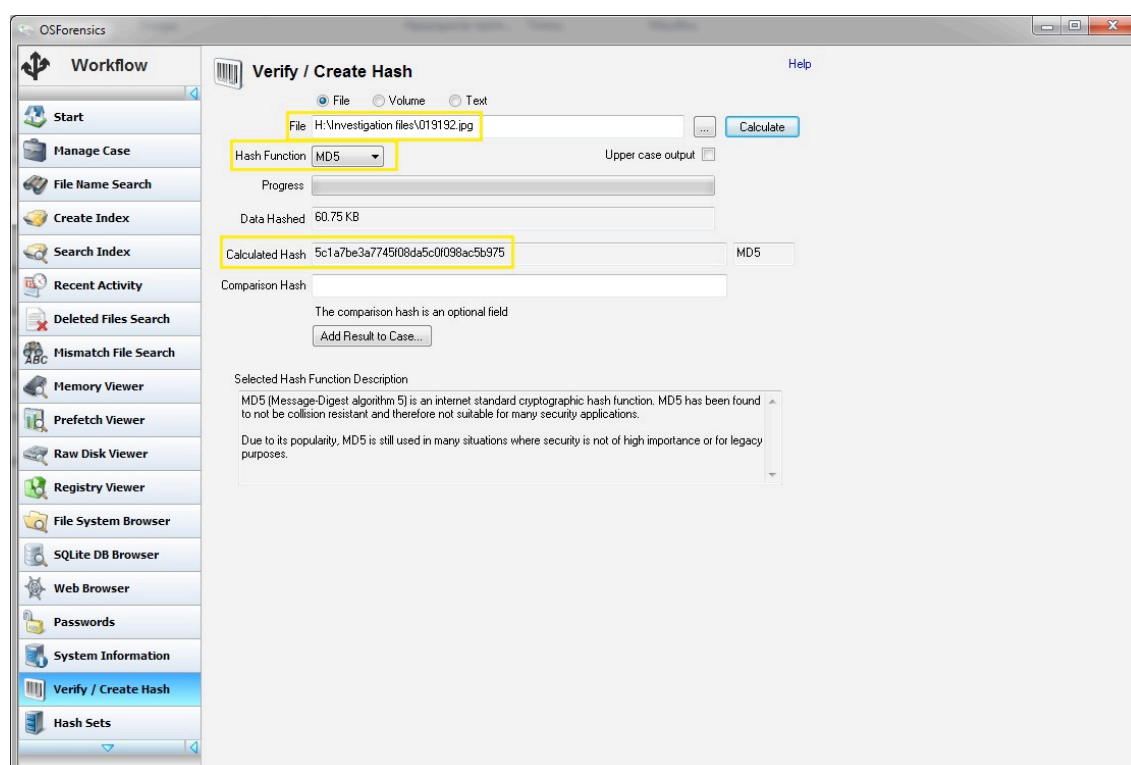


Figure 19: Procedure of creating Hash values

6.9 Creation of Forensic Images

First, we connect our USB external hard drive to the VM that is going to be examined. We use the DumpIt program (Figure 20) to acquire the computer's RAM. When the program completes its process, the contents of RAM will be stored in a file of the form computer name-date-time and with an extension of .raw (as we can see in Figure 21).

We need to clarify that DumpIt is a simple tool and it does not have any analysis capabilities.

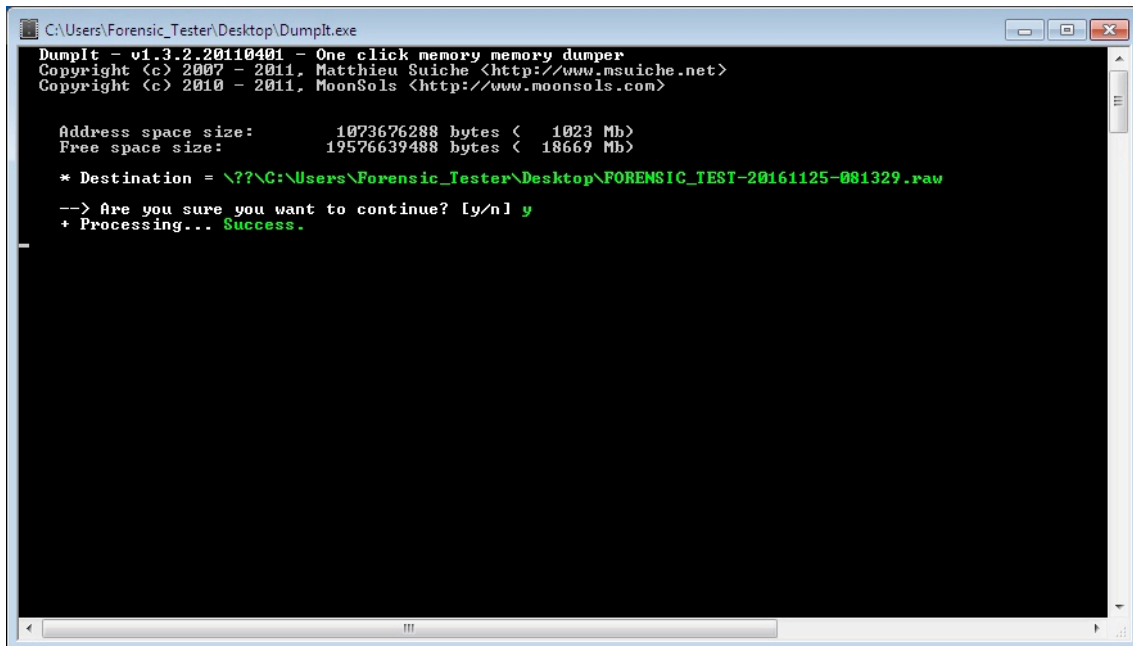


Figure 20: Use of the DumpIt program

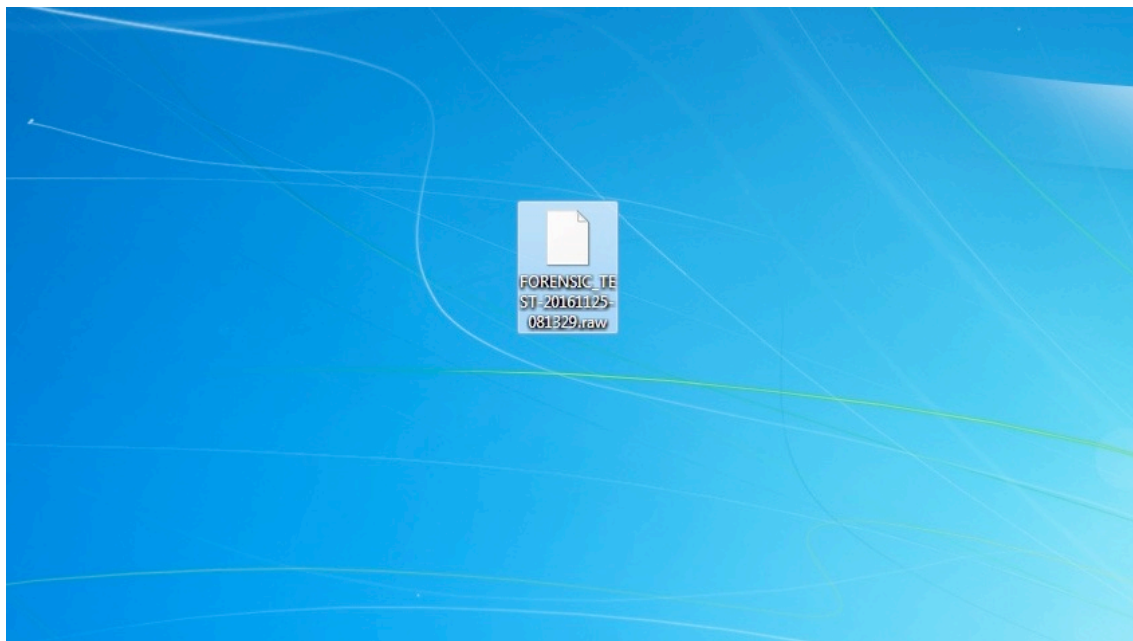


Figure 21: Form of the DumpIt file

The next step is to create an image of the system that we will investigate. We navigate through the BIOS settings and we choose the DVD-ROM as the first boot device. Afterwards, we restart the virtual machine, though we are running Kali's Live forensic mode and not the operating system of Windows.

We select Kali's Live forensic mode for the reasons we mentioned in the previous chapter (Figure 22).



Figure 22: Selection of Kali's operation mode

Once Kali operating system loads, we open a terminal window. Afterwards, by using the command `fdisk -l` we find useful information on the hard disk of the virtual machine `/dev/sda`, and for the external hard drive, where we are going to store the data `/dev/sdb` (as we can see in Figure 23).

```
root@kali:~# fdisk -l
Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x4486acfa

   Device   Boot  Start      End  Sectors  Size Id Type
  /dev/sda1 *    2048    206847    204800   100M 7 HPFS/NTFS/exFAT
  /dev/sda2           206848 52426751 52219904   24.9G 7 HPFS/NTFS/exFAT

Disk /dev/loop0: 2.5 GiB, 2667180032 bytes, 5209336 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sdb: 931.5 GiB, 1000170586112 bytes, 1953458176 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 6A70F870-01D4-4821-8BDA-458BF0CFFE1

   Device   Start      End  Sectors  Size Type
  /dev/sdb1    40    409639    409600   200M EFI System
  /dev/sdb2 411648 1953456127 1953044480 931.3G Microsoft basic data
root@kali:~#
```

Figure 23: Information about the hard drives

Next we will use the Dcfldd program. Initially, through the mount command, we create a virtual connection between the external hard drive and Kali operating system. We create the digital footprint of our objective by using the md5sum command (Figure 24). Finally, we start the process of creating the image and the digital footprint, by using the dcfldd command (as we can see in Figure 25).

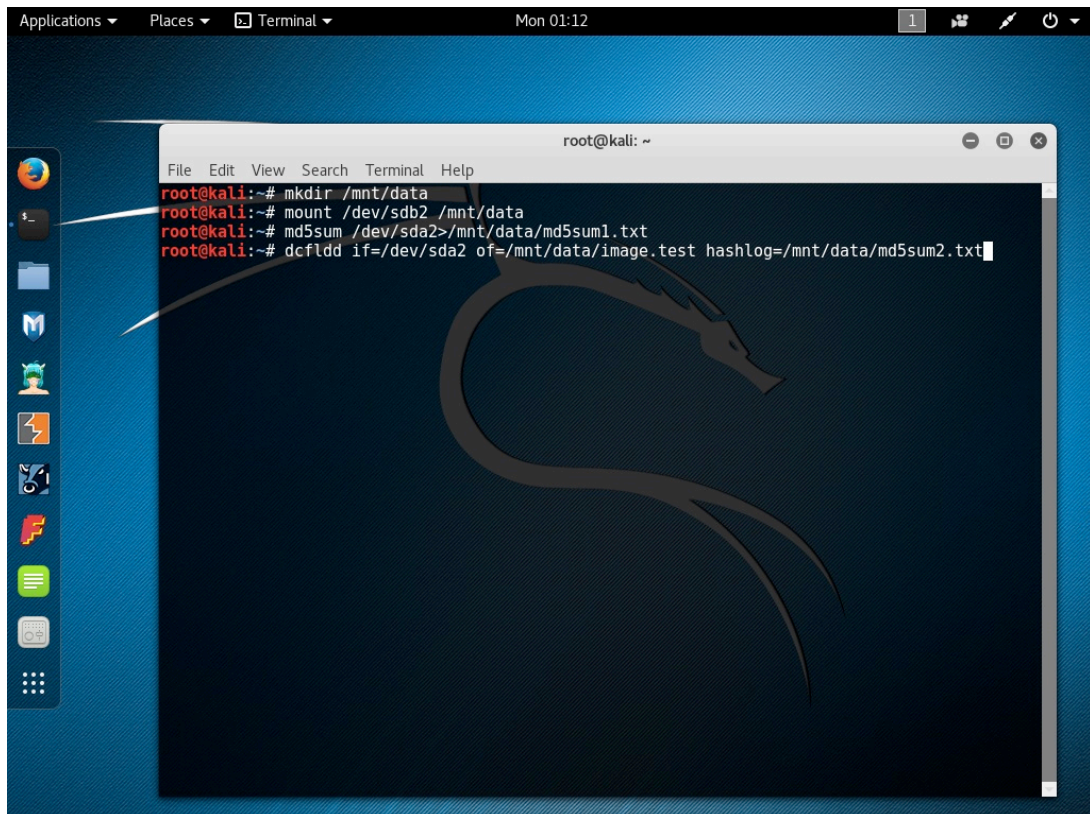


Figure 24: Command sequence for the creation of the image

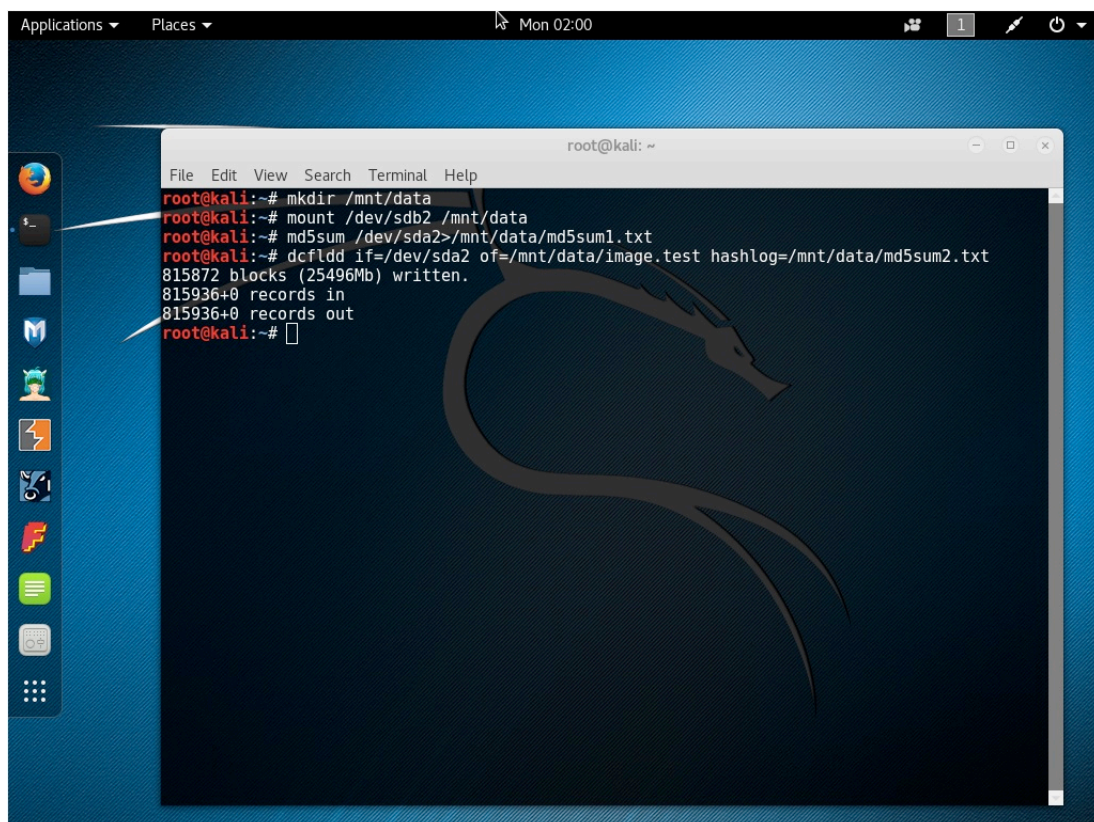


Figure 25: Completion of image creation

After the completion of the process, we compare the initial and final digital footprint in order to ensure the integrity of our data (as we can see below in Figure 26).

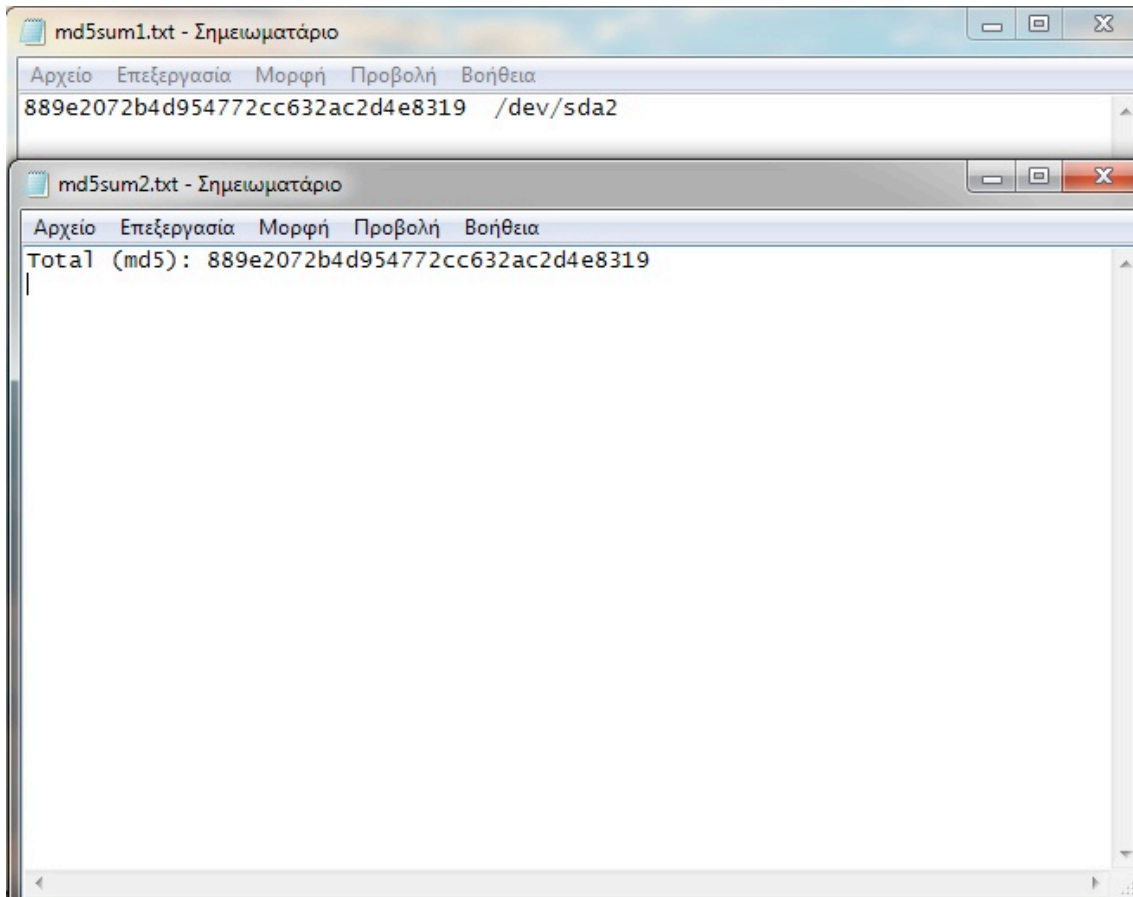


Figure 26: Confirmation of image integrity

This means that the image.dd file is an exact copy of the virtual machine's hard drive disk.

6.10 Analysis of Forensic Images

Now we can use several tools (e.g. FTK Imager) to analyze the image that we have acquired. Given the fact that our investigation is limited to a particular application, we will use simple methods and specific programs.

Before we proceed further, we should mention that we use a copy of the original image that we have acquired. We use FTK Imager to create forensic images of the files that we recovered in the previous step. Thus, the original files remain inaccessible and intact.

Firstly, we use ProDiscover Basic program (Figure 27). This program has the ability to create the files that are necessary, in order to be able to “load” the image that we creat-

ed, in a virtual machine. Specifically, based on the image.dd file it creates the image.vmdk file (as we can see in Figure 28 and Figure 29), which we will use next.

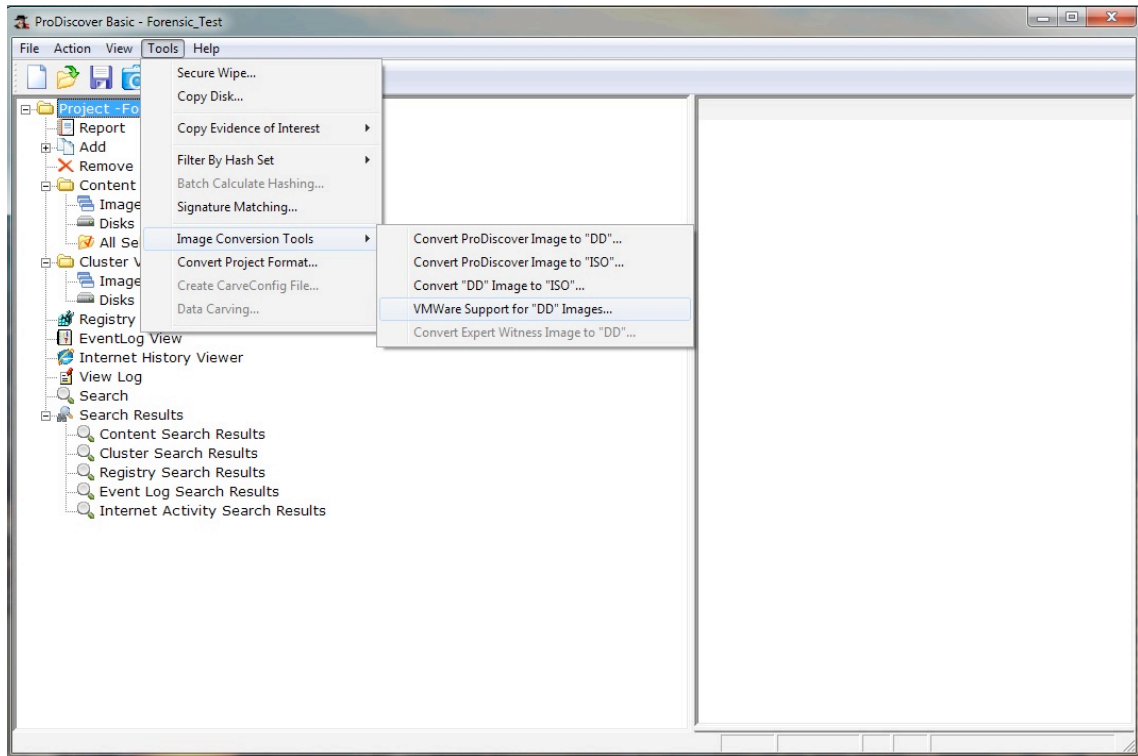


Figure 27: Screenshot of the ProDiscover program use

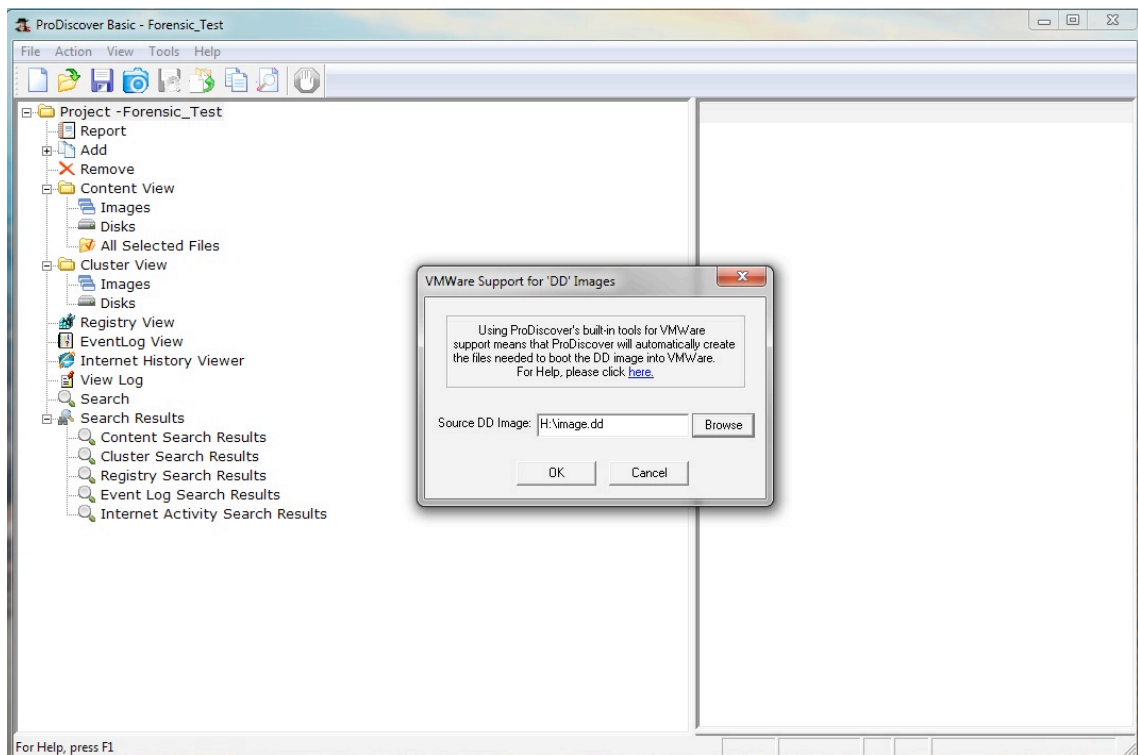


Figure 28: Procedure to create the image.vmdk file

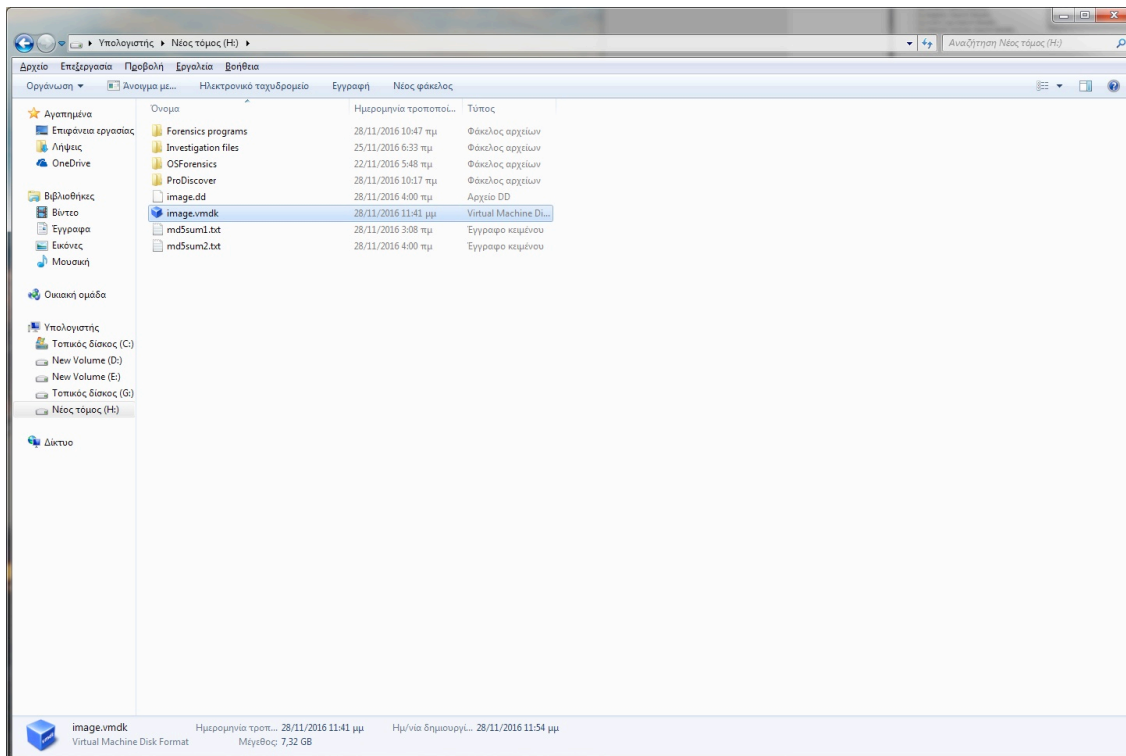


Figure 29: image.vmdk files created inside the external hard drive

We create a new virtual machine by using VirtualBox. We use the wizard and choose to install the operating system later (Figure 30). All the other settings are on default. Afterwards, we remove the default hard drive and choose to add the file that we created with ProDiscover Basic (as we can see in Figure 31 and Figure 32).

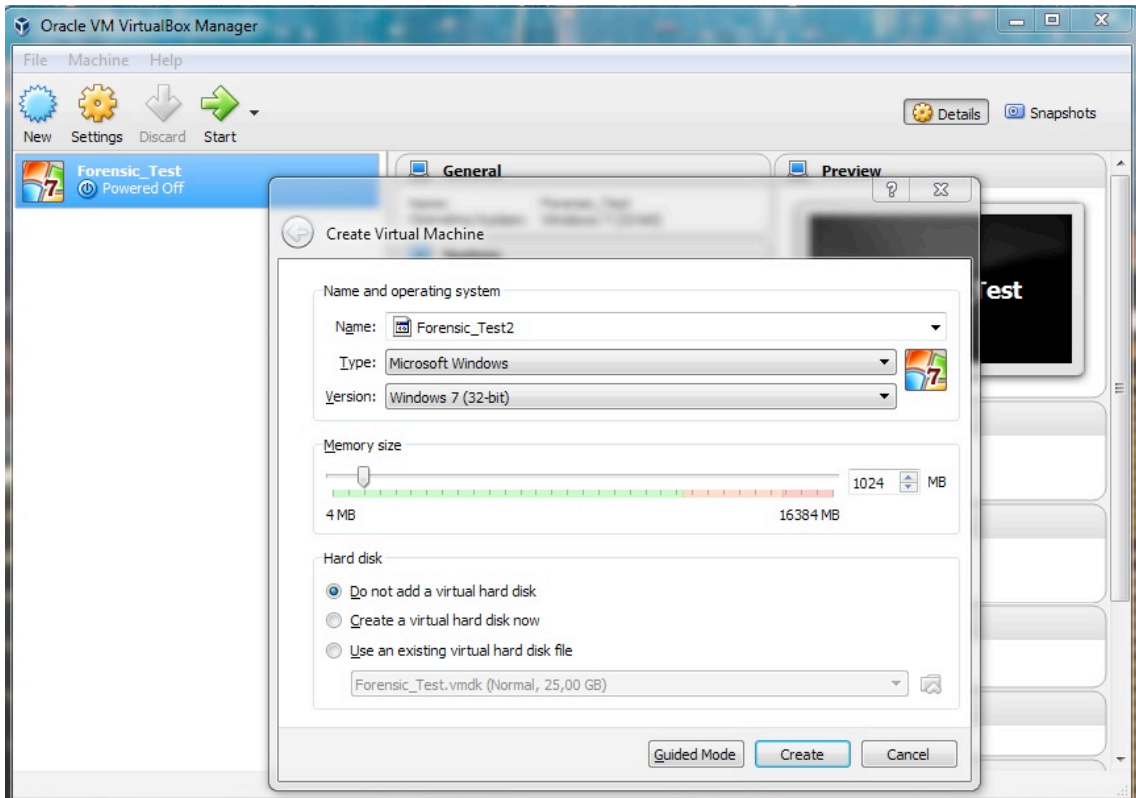


Figure 30: Creation of Virtual Machine and choosing to install the operating system later

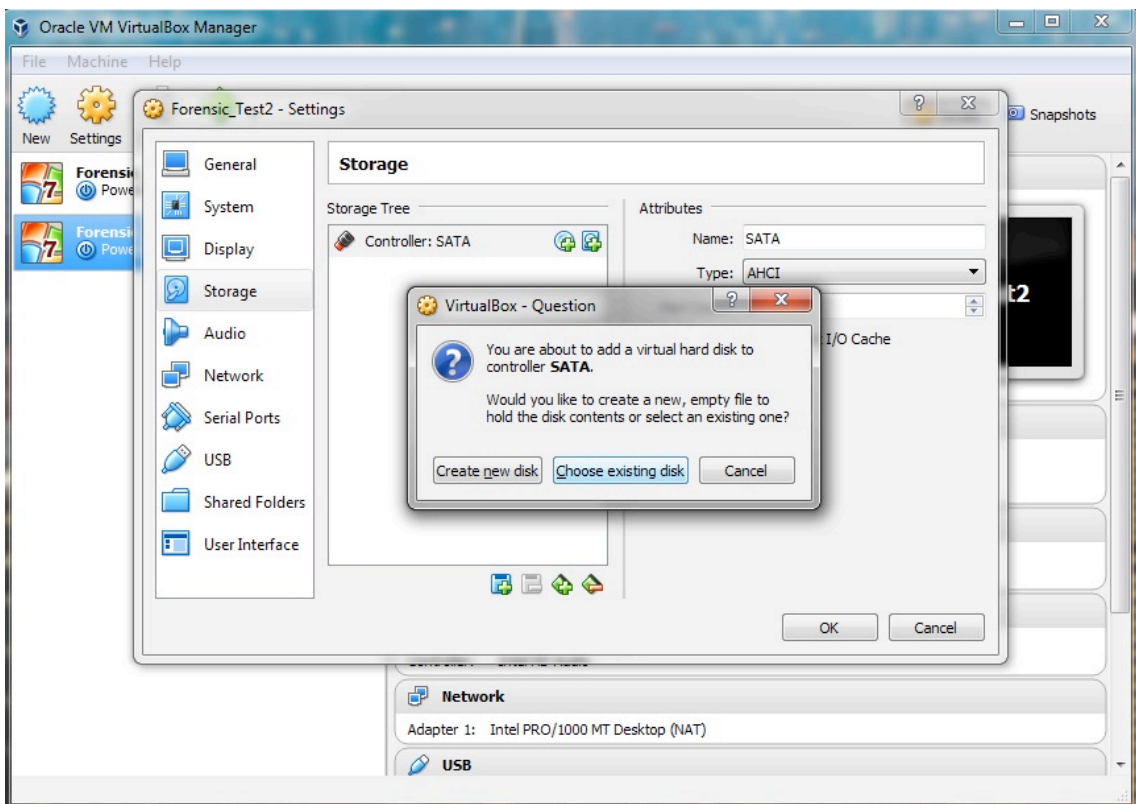


Figure 31: Removal of the default disk and addition of the file that we created (1)

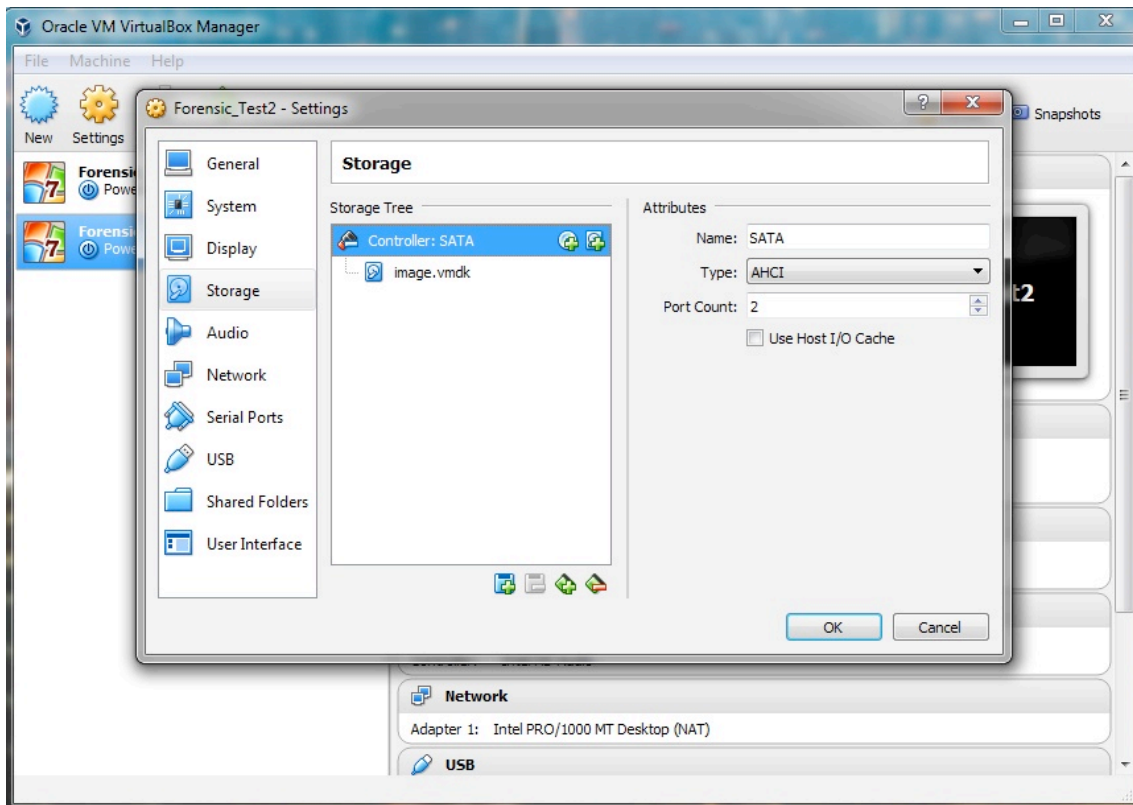


Figure 32: Removal of the default disk and addition of the file that we created (2)

This way we created a secure forensic virtual machine of the computer system to be tested.

6.11 Analysis of Browsers

6.11.1 Analysis of Mozilla Firefox (FFX)

The data that are generated from the use of Mozilla Firefox are stored in the following location (as we can see in Figure 33):

C:\Users\Forensic_Tester\AppData\Roaming\Mozilla\Firefox

Please note that if you want to be able to see the AppData file, you have to enable “Show hidden files, folders, and drives”, by opening a folder window and “click” on the Organize button, and then select “Folder and Search Options”. Then you have to click the View tab and select “Show hidden files and folders” in the list.

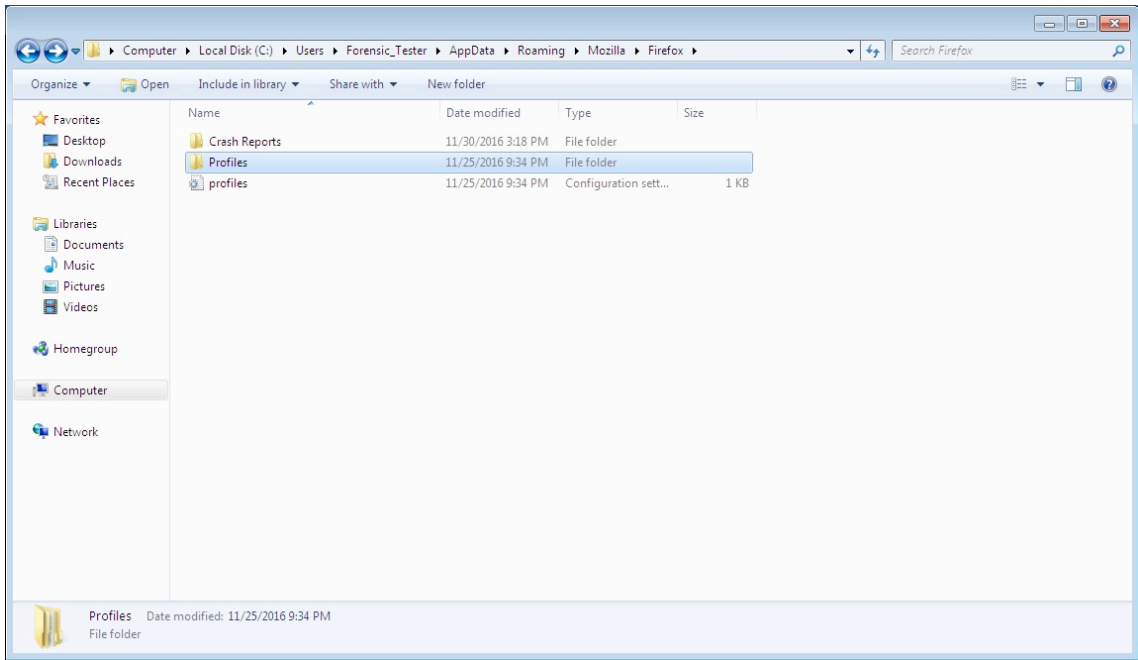


Figure 33: Presentation of Mozilla Firefox’s files

Also in the Profiles\xxxxxxxx.default (Figure 34) folder are stored, in a sqlite format, the data that are being generated while using the browser (History, Downloads, Login Credentials, etc.).

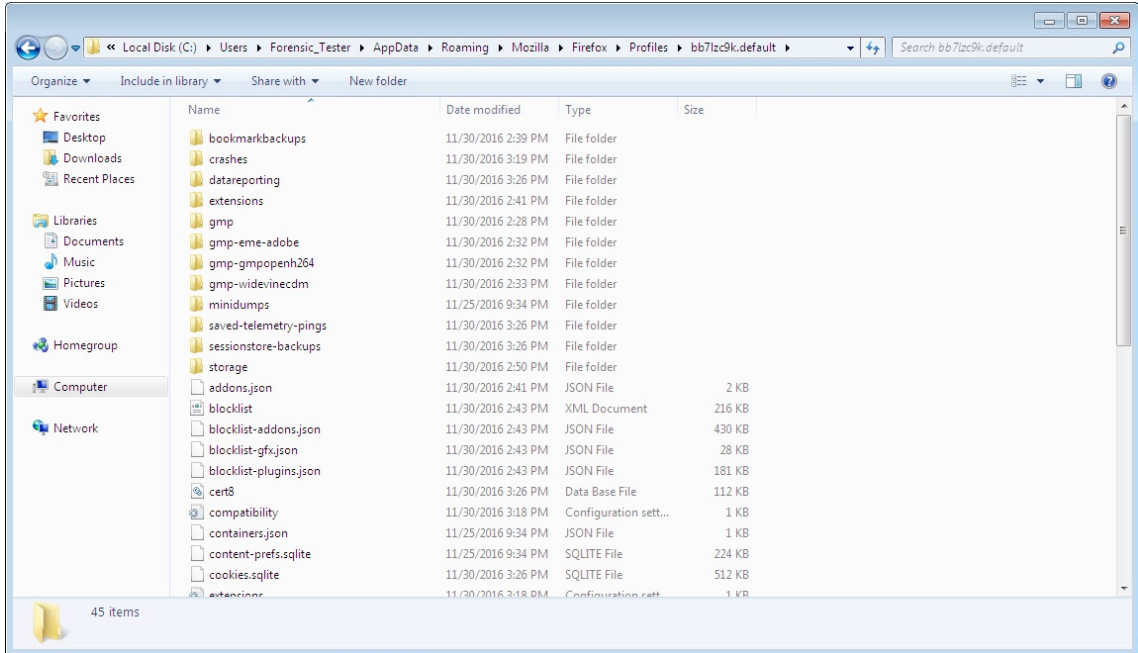


Figure 34: Folder of the to be examined SQL databases

By using the “DB Browser for SQLite” program, we examine the contents of these files. In “places.sqlite” file we find information about the addresses which we have visited, and the files which we have downloaded (Figure 35 and Figure 36).

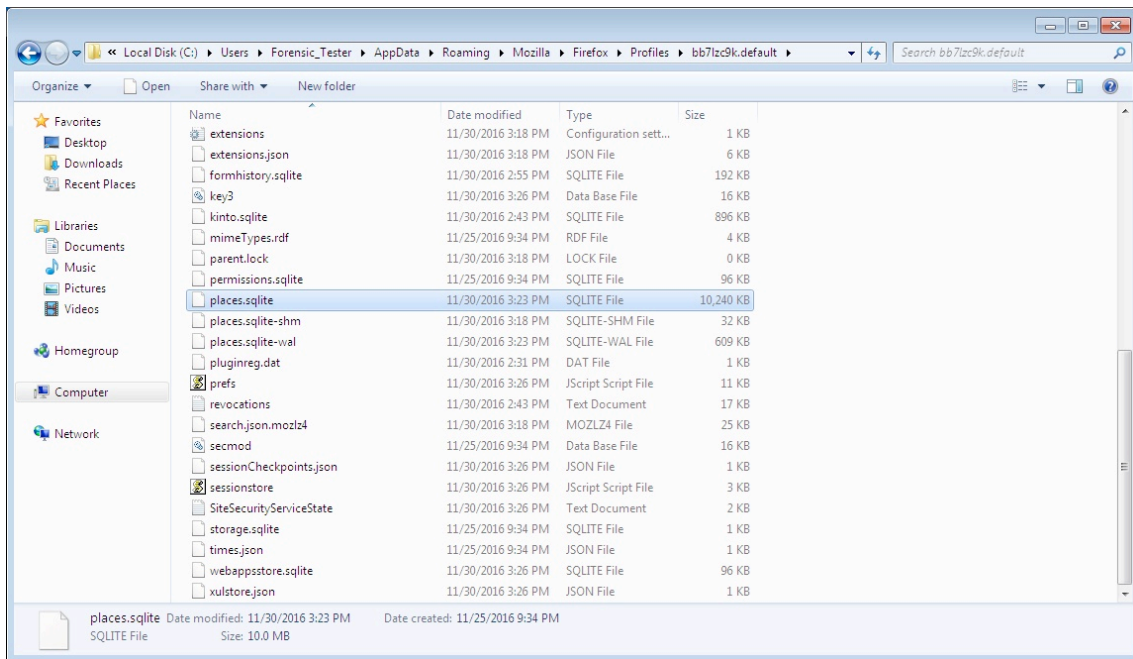


Figure 35: Places.sqlite file

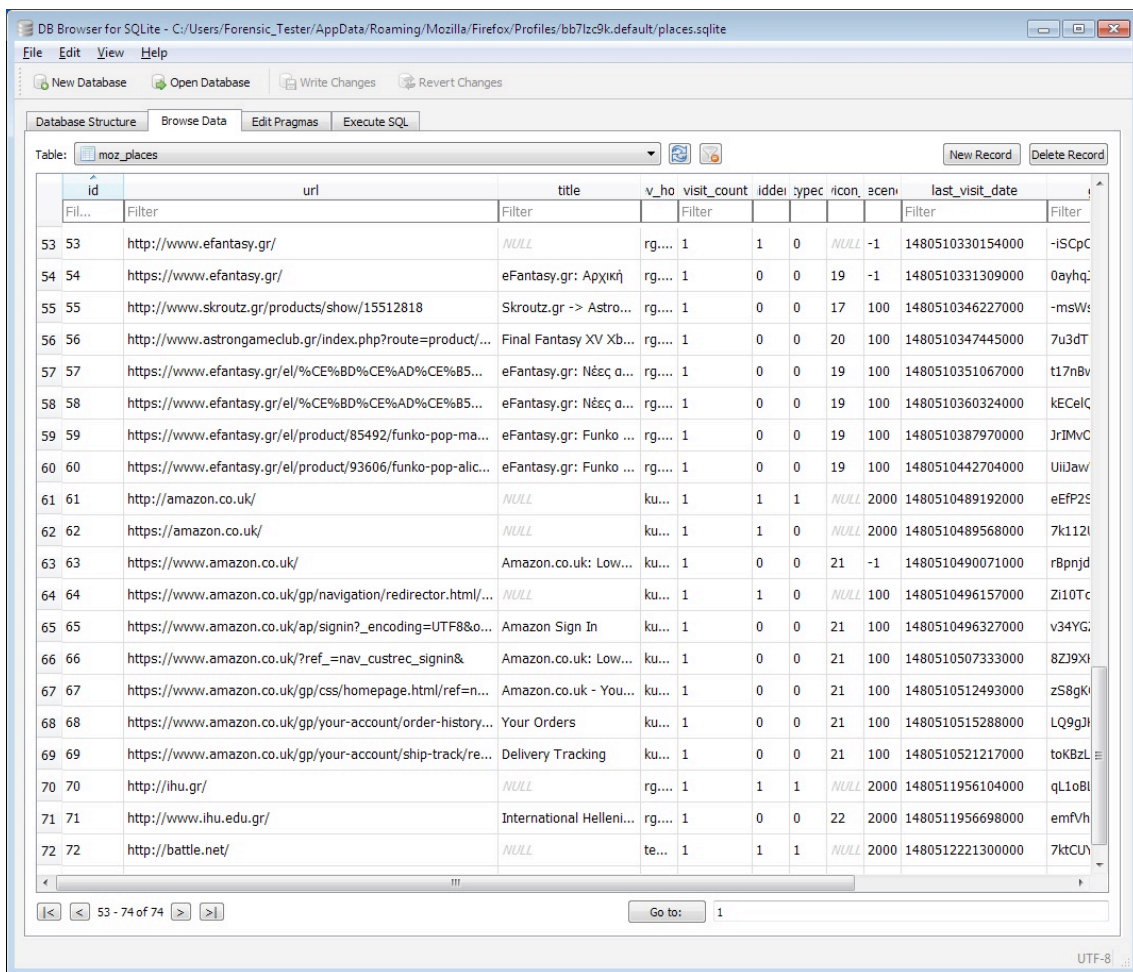


Figure 36: Investigation of Mozilla Firefox's database (places.sqlite)

6.11.2 Analysis of Google Chrome (GC)

The data that are generated from the use of Google Chrome are stored in the following location (as we can see in Figure 37): C:\Users\Forensic_Tester\AppData\Local\Google

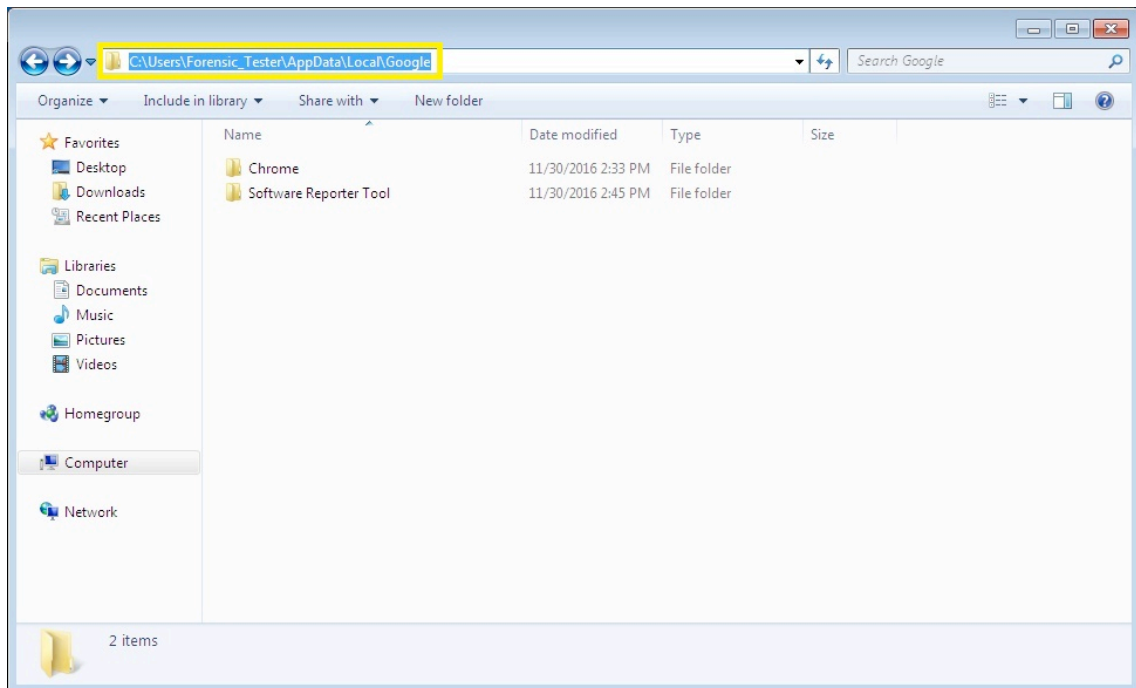


Figure 37: Presentation of Google Chrome's files

Also in the "Chrome\User Data" folder (Figure 38), in a sqlite format, the data that are being generated by using the browser (History, Downloads, Login Credentials. etc.).

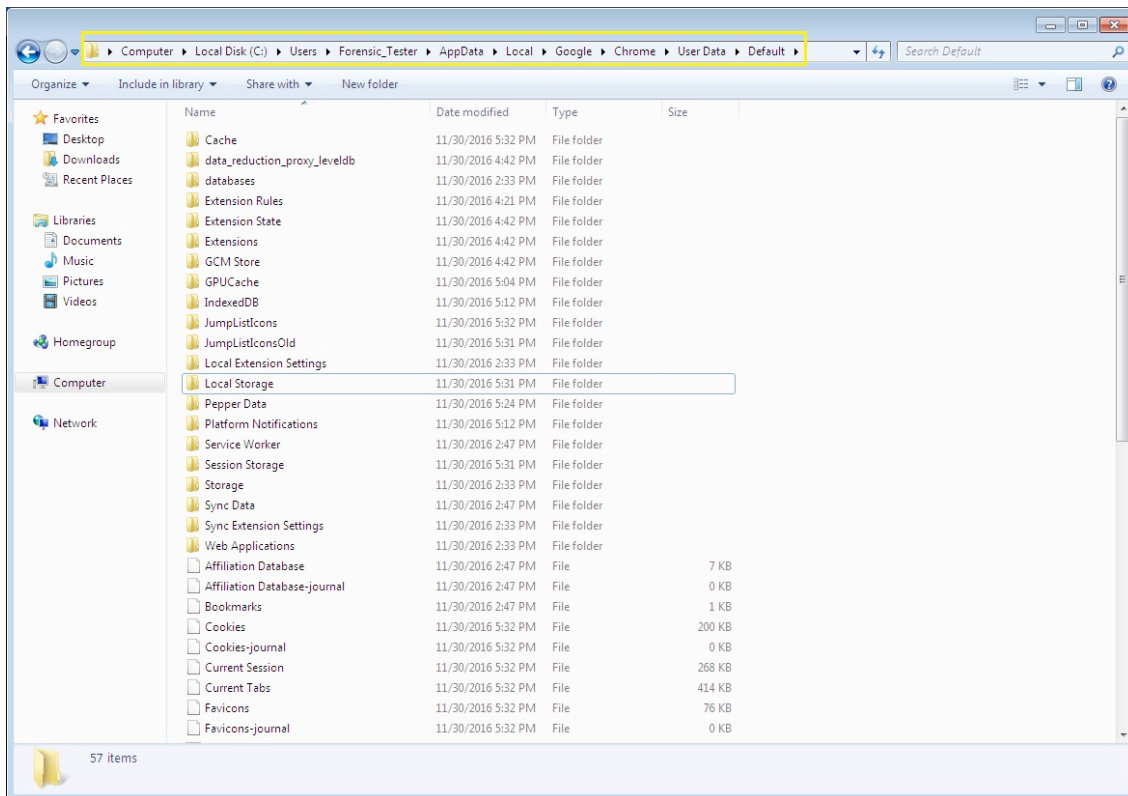


Figure 38: Folder of the to be examined SQL databases

By using the “DB Browser for SQLite” program, we examine the contents of these files. In “History” file we find information about the internet addresses which we have visited, and the files which we have downloaded (we can see below in Figure 39 and Figure 40).

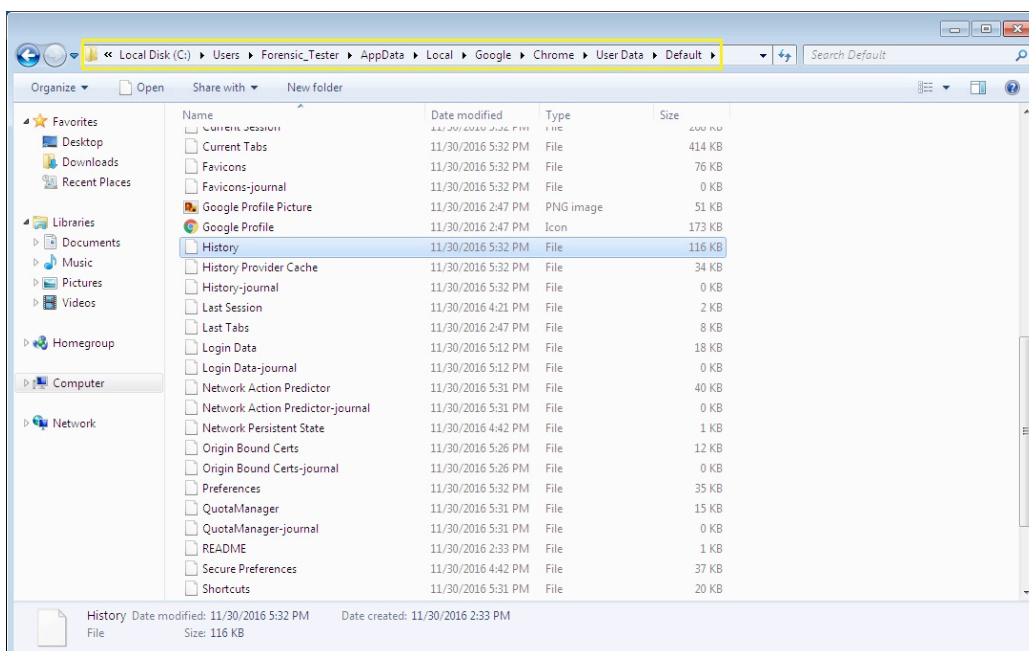


Figure 39: Google Chrome’s History file

id	url	title	visit_count	typed_count	last_visit_time	hidden
34	http://www.sport-fm.gr/		2	0	13124993362969969	0
35	http://www.skrouz.gr/search?keyphrase=final+fantasy...	Κατηγορίες αν...	1	0	13124993060262511	0
36	http://www.skrouz.gr/c/1413/playstation_4_games.ht...	Final Fantasy ...	1	0	13124993062385404	0
37	http://www.skrouz.gr/s/4711568/Final-Fantasy-XV-PS...	Final Fantasy ...	1	0	13124993062385404	0
38	http://www.skrouz.gr/search?keyphrase=the+last+gu...	the last guard...	1	0	13124993070066316	0
39	http://www.skrouz.gr/c/1413/playstation_4_games.ht...	the last guard...	2	0	13124993135683156	0
40	http://www.skrouz.gr/s/10523789/The-Last-Guardian-...	The Last Guar...	4	0	13124993096018783	0
41	http://www.skrouz.gr/products/show/26762146	Skrouz.gr -> ...	1	0	13124993082060038	0
42	http://www.public.gr/	Public.gr: uno...	1	1	13124993133483905	0
43	http://www.skrouz.gr/s/9234538/The-Last-Guardian-P...	The Last Guar...	1	0	13124993138588842	0
44	http://www.public.gr/search/public/searchResults.jsp;...	Αναζήτηση για...	1	0	13124993152797721	0
45	http://www.public.gr/search/public/searchResultsRefin...	Αναζήτηση για...	1	0	13124993154718697	0
46	https://www.google.gr/webhp?sourceid=chrome-insta...		1	0	13124993162860279	0
47	https://www.germanos.gr/		1	0	13124993164452342	0
48	https://www.germanos.gr/search?q=final%20fantasy	Αποτελέσματα...	1	0	13124993185149012	0
49	https://www.germanos.gr/search/?q=final%20fantasy	Αποτελέσματα...	2	0	13124993193950712	0
50	https://www.germanos.gr/product/final-fantasy-xv-del...	Final Fantasy ...	1	0	13124993191247525	0
51	https://www.germanos.gr/search?q=the%20last%20n...	Αποτελέσματα...	1	0	13124993206183092	0

Figure 40: Investigation of Google Chrome’s database (History)

6.12 Signature Comparison Methodology

As part of our research and for finding the changes that the installation and uninstallation of the Box cloud storage application lead, we will use the procedure of creating and comparing signatures, by using OSForensics (Figure 41).

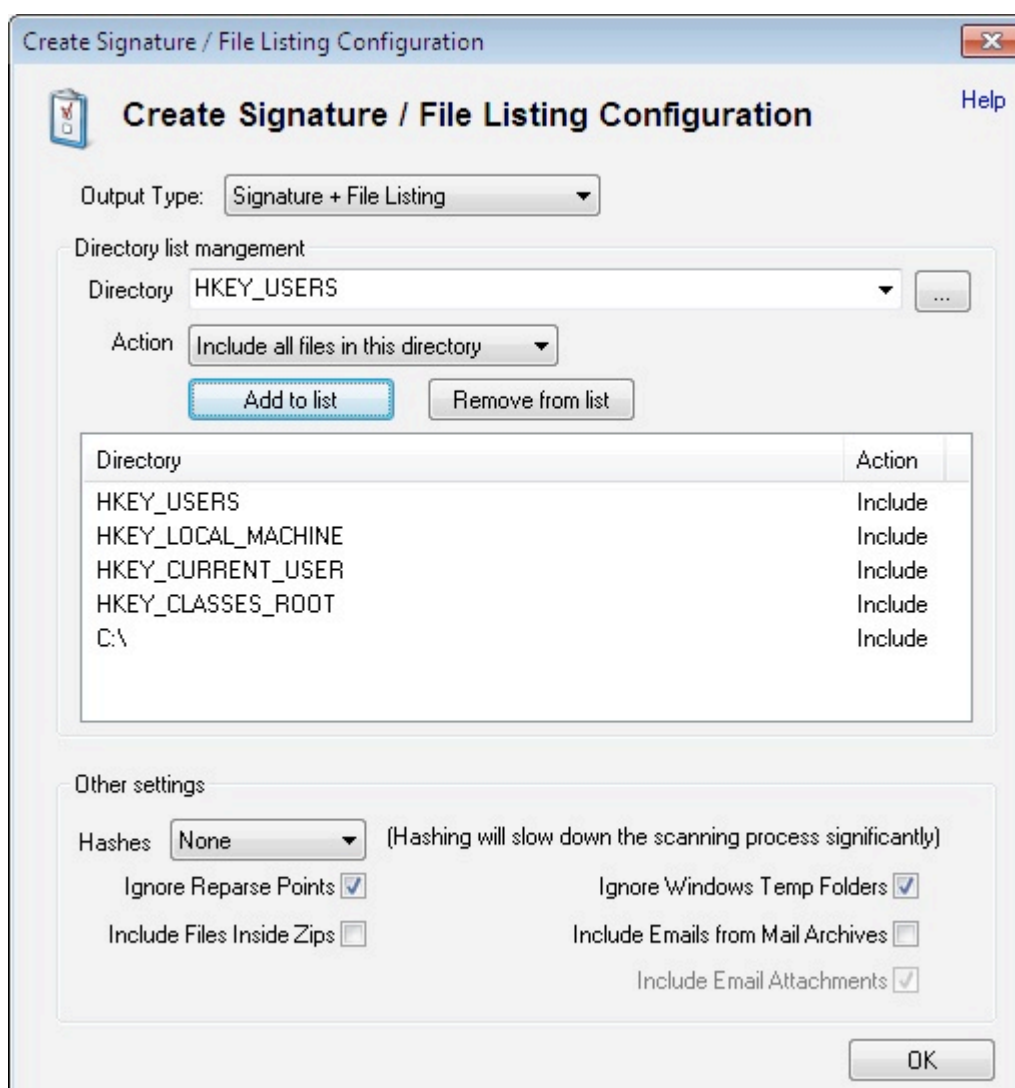


Figure 41: Snapshot from the signature creation process

OSForensics gives us the ability to create a digital forensic signature of a hard drive disk. We can discover the changes that took place in our computer system, by comparing digital signatures that were created at different times.

6.13 Limitations of the Investigation

Version Dependent: Due to the experimental nature of this investigation, the results apply only to the version of the software that was used during the investigation. *The previous versions of the software may have different results, and the subsequent changes in software may lead to different conclusions.* Moreover, the access to a cloud service through a browser is based on the information that the provider returns. However, this can be changed, since each provider updates the HTML, or any other code, used for the presentation of the information to the end user.

Operating System Dependent: The investigation was conducted by evaluating the changes that were made to the files of a computer system with Windows 7, and with the NTFS file system. Alternative operating systems such as Microsoft's XP, Vista, 8, 10, Apple's Mac OS, and the various distributions of Linux, may have different data remnants. Other file systems, such as EXT3, can also lead to different findings. Therefore, there might be different conclusions in relation to the survey questions, when Windows 7 and NTFS file system are not used.

6.14 Conclusions

This chapter describes the purpose of our investigation. We recorded the questions of our research, and through the methodology we determined the procedure that we are going to follow in the next chapters. We described the hardware and software that we will use, and we identified the limitations of our investigation.

7 Digital Forensic Investigation of Box Cloud Storage Service

7.1 Introduction

Box is an alternative solution for users who want to use a cloud storage service. Users may also access this service through their mobile devices, such as smartphones and tablets (Android, IOS).

Box offers free access to accounts with 10 GB of storage space and 250 MB file upload limit. Subscription payment in this application does not only increase the supplied storage space, but also the provided services, such as operations history and Log files. Box is oriented towards corporate use. The following figures (Figure 42 and Figure 43) show the offered services by the application.

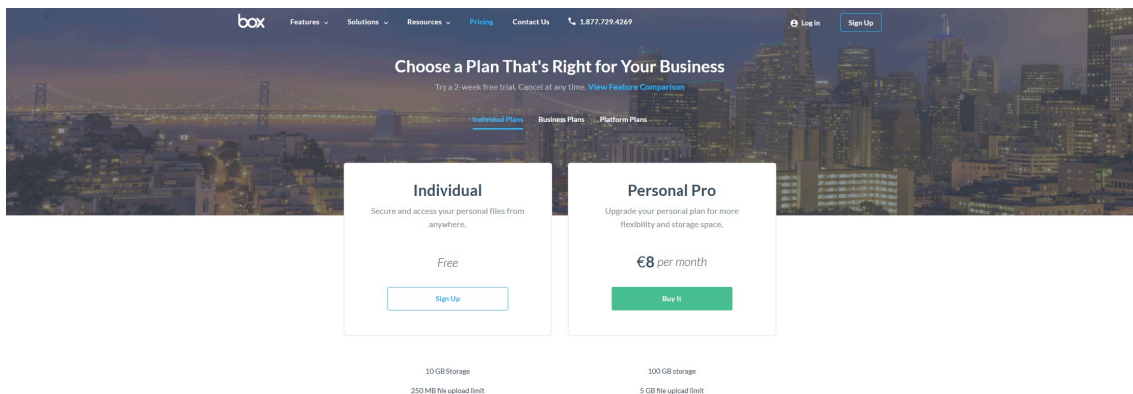


Figure 42: Presentation of Box's cloud storage services (1)

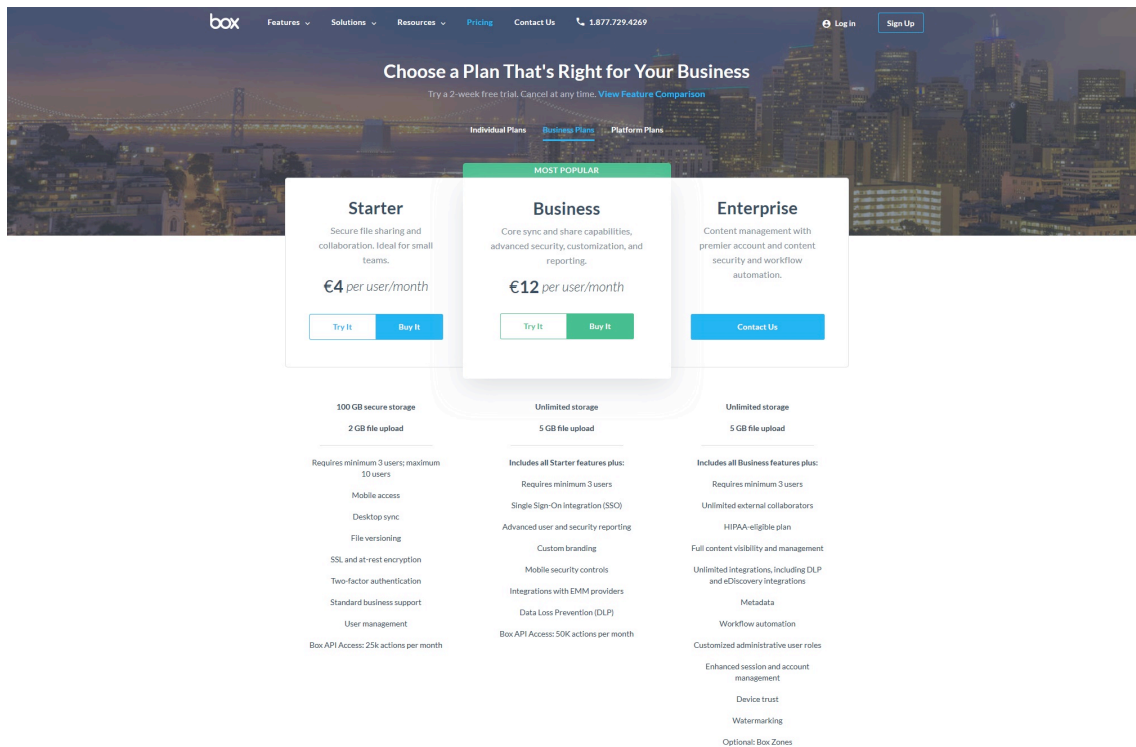


Figure 43: Presentation of Box's cloud storage services (2)

All accounts, even those that are free, allow us to share files or folders through a link. Box also incorporates the ability to add comments in our files. Finally, we can gain access to this application through its own free downloadable software, or through a browser.

7.2 Purpose/Objective

The purpose of this investigation is to identify the data remnants on a computer with Windows 7, after using the Box cloud storage service. These data remnants could be the user name, password, files that are stored in the account, and the related to these files metadata. Also in the context of our investigation we are using anti-forensic procedures, in order to be able to compare the initial and final state of the system.

7.3 Box Service Analysis in Windows 7 Environment

7.3.1 Preparation

In order to collect the data that are needed to answer the questions of our investigation, we created a virtual machine. By following the methodology, which we defined in

Chapter 6, we used Box cloud storage service to create notes and attach 4 files (.jpeg, .txt, .pdf, .doc). Lastly, we also examined the synchronization features that it offers.

For the preparation of Box's investigation, except from the software that we analyzed in Chapter 6, we also used:

- BoxSync Windows (version 4.0.7724.0)
- CCleaner (version 5.24.5841)
- Eraser (version 6.2.0.2979)
- ESEDatabase View (version 1.42)
- DB Browser for SQLite (portable version 3.9.1)
- Mozilla Firefox (version 50.0.2)
- Google Chrome (version 55.0.2883.75)

Finally, in the context of preparation we have used the signature creation procedure of OSForensics, before and after the installation of Box, in order to detect accurately and effectively the changes that were made to the operating system of the virtual machine.

7.3.2 Identification and Collection

In this investigation, the mean that contain the information needed to perform the analysis were identified. They are the RAM and the hard drive of the virtual machine. Following the procedures that we defined in Chapter 6, we recovered with a forensic acceptable way the RAM and the hard drive of the virtual machine.

7.3.3 Preservation

For this investigation we created a forensic copy of the two files that we acquired in the process of collection and recovery. To achieve this, we used the Access Data FTK Imager program.

7.3.4 Analysis

At this stage, we used a number of tools, such as OSForensics. Firstly, we want to define the changes, which are made on the operating system of Windows 7, after the installation and uninstallation of BoxSync.

We want to check if we can find out that this program was used, even if it was uninstalled from the operating system.

For this reason, we use OSForensics and the option of creating and comparing signatures. In the table below (Table 7) we see the files that were created after the installation of BoxSync service. In folder “C:\Program Files\Box\Box Sync” are installed the files that are necessary for the operation of the application.

Table 7: Executable files of Box

C:\Program Files\Box\Box Sync\BoxSync.exe 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync\BoxSyncMonitor.exe 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync\BoxSyncWindowsUI.dll 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync\bz2.pyd 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync\clr.pyd 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync_ctypes.pyd 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync_elementtree.pyd 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync_hashlib.pyd 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync_multiprocessing.pyd 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync_psutil_windows.pyd 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync_socket.pyd 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync_sqlite3.pyd 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync_ssl.pyd 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync_win32sysloader.pyd 12/4/2016,8:09:22 PM
C:\Program Files\Box\Box Sync_yappi.pyd 12/4/2016,8:09:22 PM

In folder “C:\Users\Forensic_Tester\AppData\Local\Box Sync\Logs” are stored the Log files (Table 8).

Table 8: Log files related to Box

C:\Users\Forensic_Tester\AppData\Local\Box Sync\Logs\Box Sync-4.0.7724.2016-12-04.log 12/4/2016,8:09:49 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\Logs\Box Sync-4.0.7724.2016-12-07.log 12/4/2016,8:09:49 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\Logs\Box Sync-4.0.7724.2016-12-14.log 12/4/2016,8:09:49 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\Logs\Box Sync-4.0.7724.log 12/4/2016,8:09:49 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\Logs\Cache\metrics.db 12/4/2016,8:09:49 PM

In folder “C:\Users\Forensic_Tester\AppData\Local\Box Sync” are installed the SQL databases that the application uses (Table 9).

Table 9: Application’s SQL databases

C:\Users\Forensic_Tester\AppData\Local\Box Sync\cacert.pem 12/4/2016,8:09:49 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\item_status.db 12/4/2016,8:09:50 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\last_migration_version 12/4/2016,8:09:49 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\monitor_state.db 12/4/2016,8:10:24 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\monitor_state.db-shm 12/4/2016,9:16:32 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\monitor_state.db-wal 12/4/2016,8:10:24 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\sync.db 12/4/2016,8:09:49 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\sync.db-shm 12/4/2016,8:09:50 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\sync.db-wal 12/4/2016,8:09:49 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\sync_root_folder.txt 12/4/2016,8:10:25 PM
C:\Users\Forensic_Tester\AppData\Local\Box Sync\wincrypto_pass.cfg 12/4/2016,8:10:18 PM

The files that we are transferring, are stored in the folder “C:\Users\Forensic_Tester\BoxSync” (Table 10).

Table 10: File storage folder

C:\Users\Forensic_Tester\Box Sync\desktop.ini 12/4/2016,8:10:24 PM

In the following tables we see the changes in the operating system’s Registry, after the installation of BoxSync (Table 11 and Table 12).

Table 11: Registry changes (1)

HKEY_CLASSES_ROOT\BoxDesktop.boxnote 12/4/2016,8:09:23 PM
HKEY_CLASSES_ROOT\BoxDesktop.boxnote\DefaultIcon| 12/4/2016,8:09:23 PM
HKEY_CLASSES_ROOT\BoxDesktop.boxnote\shell 12/4/2016,8:09:23 PM
HKEY_CLASSES_ROOT\BoxDesktop.boxnote\shell\open 12/4/2016,8:09:23 PM
HKEY_CLASSES_ROOT\BoxDesktop.boxnote\shell\open\command 12/4/2016,8:09:23 PM

Table 12: Registry changes (2)

HKEY_CLASSES_ROOT\Directory\shell\ContextMenuHandlers\BoxContextMenuClient 12/4/2016,8:09:23 PM

7.4 Use of the Application Software for Uploading Files

7.4.1 Event Logs Examination

Next we will examine the Log files. We find references to the file that we uploaded and the time that this action took place (Table 13 and Table 14). However, we notice that the hash value is not the same as the one that we calculated in Chapter 6. This is due to the fact that Box uses the SHA-1 hash function (Table 14). Lastly, we retrieve information about the file size (Table 14).

Table 13: Examination of Log files (1)

```
[32m 2016-12-04 21:59:19.326 1780 DEBUG LocalFSMonitor
local_sync_event_buil LocalSyncEventBuilder has received native event TN:
_00000002_, CREATE, new_state: (<LocalNativeState native_id:
LocalNativeIDWithCreationTimeStamp(inode=1125899906895063L,
native_item_type=0, content_created_at=427088328125L); parent_native_id:
LocalNativeIDWithoutCreationTimeStamp(inode=281474976762344L,
native_item_type=1); name: 019192.jpg; item_type: 0; is_deleted: False; checksum:
None; package_folder_transition: None; syncability: SYNCABLE; attributes: set([]);
content_updated_at: 366285561805; content_created_at: 427088328125; size: |
62206>), old_state: (None), shares_location: False
```

```
[36m 2016-12-04 21:59:19.858 1780 INFO LocalExecutor-1 box_fs_sync_api
Creating item on box. name="019192.jpg", item_type=0, parent_item_id=(u'0', 1)
```

Table 14: Examination of Log files (2)

```
[36m 2016-12-04 21:59:19.858 1780 INFO LocalExecutor-1 box_server_api
New item upload with parent box id 0 and name 019192.jpg

[36m 2016-12-04 21:59:24.326 1780 INFO LocalExecutor-1 network_layer
JSON response received for network request with content: {u'total_count': 1,
u'entries': [{u'item_status': u'active', u'content_created_at': u'2016-12-04T11:59:15-
08:00', u'id': u'108300074769', u'size': 62206, u'modified_by': {u'login':
u'██████████', u'type': u'user', u'id': u'575905111', u'name': u'Andreas
Patsarikas'}, u'file_version': {u'sha1':
u'2758004a300ad09b9344d9cb530cfb2a9e327b3e', u'type': u'file_version', u'id':
u'116503135249'}, u'created_by': {u'login': u'██████████@hotmail.com', u'type':
u'user', u'id': u'575905111', u'name': u'Andreas Patsarikas'}, u'etag': u'0',
u'purged_at': None, u'shared_link': None, u'path_collection': {u'total_count': 1,
u'entries': [{u'sequence_id': None, u'etag': None, u'type': u'folder', u'id': u'0',
u'name': u'All Files'}]}, u'description': u'', u'parent': {u'sequence_id': None, u'etag':
None, u'type': u'folder', u'id': u'0', u'name': u'All Files'}, u'trashed_at': None,
u'content_modified_at': u'2000-04-12T06:20:54-07:00', u'sequence_id': u'0', u'sha1':
u'2758004a300ad09b9344d9cb530cfb2a9e327b3e', u'name': u'019192.jpg', u'type':
u'file', u'created_at': u'2016-12-04T11:59:26-08:00', u'modified_at': u'2016-12-
04T11:59:26-08:00', u'owned_by': {u'login': u'██████████@hotmail.com', u'type':
u'user', u'id': u'575905111', u'name': u'Andreas Patsarikas'}}]}
```

In the next figure (Figure 44) we can see that the hash values are identical.

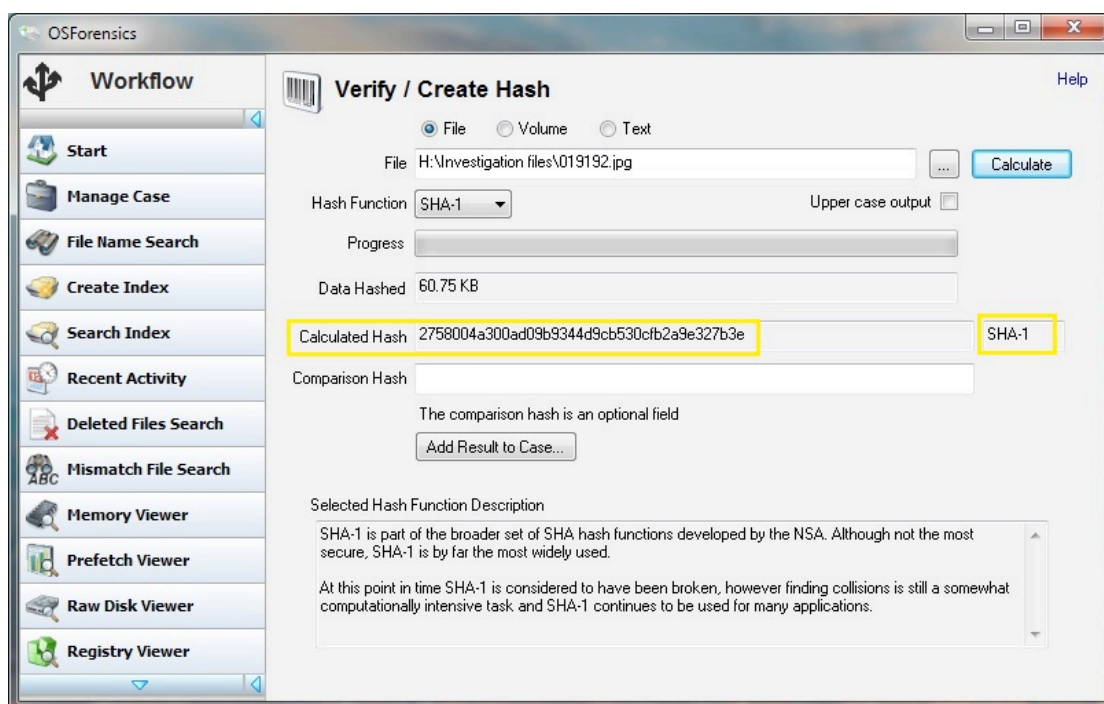


Figure 44: Use of SHA-1 hash function

Also we managed to find the user's name and email address that are associated with the user, the time and date that the log was made, as well as the account ID (as we can see in Table 14).

The next step of our research is to examine the application's SQL database, which is item_status.db. We discover the files that we uploaded and the time and date of occurrence of this action (Figure 45).

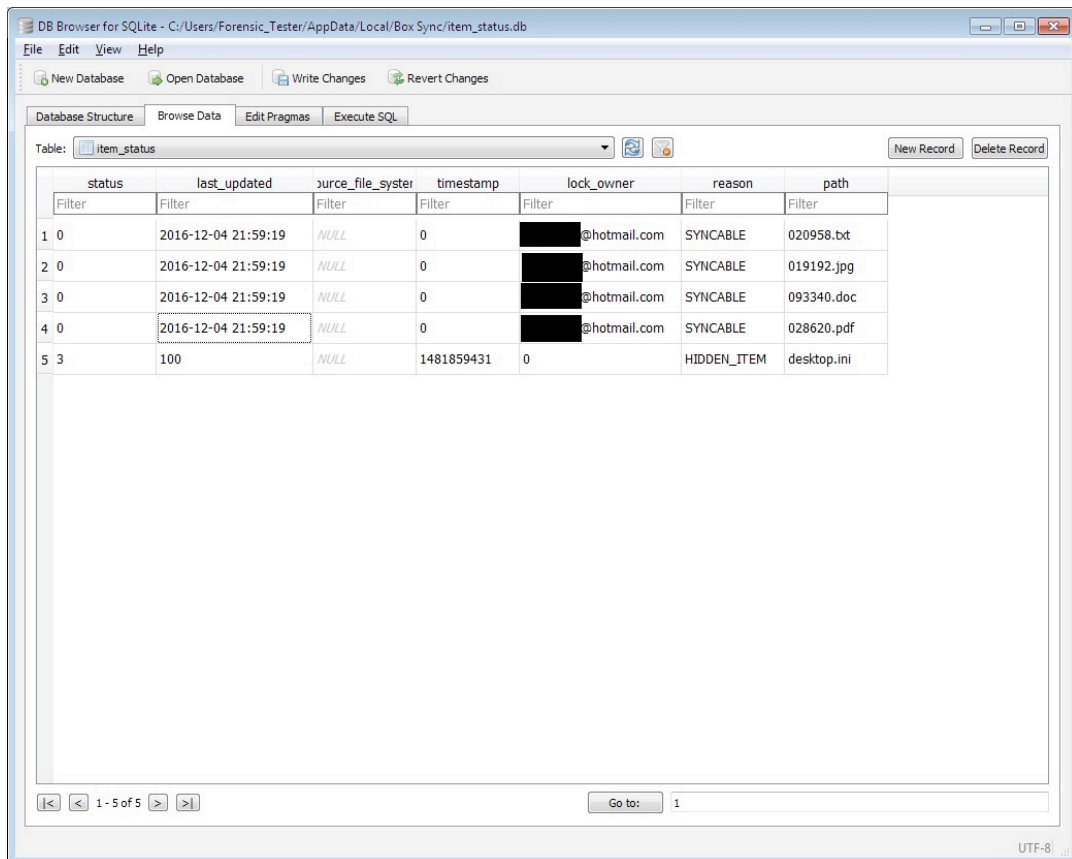


Figure 45: Discovery of email address, time, date and the name of the files we uploaded

The following table summarizes our findings in this scenario.

Table 15: Using Box's application software

Source	Findings
Logs	<p>Information about:</p> <ul style="list-style-type: none"> • the update of the service • the operations of the service • the name of the files, their size and their hash values

	<ul style="list-style-type: none"> • the time and date when we uploaded them • the ID, the name and email of the user
Database <ul style="list-style-type: none"> • item_status.db 	Information about: <ul style="list-style-type: none"> • the files we uploaded • the time and date when we uploaded them • the email of the user

7.4.2 Examination of RAM

At this stage of our investigation we will examine the RAM. We were able to successfully discover the user's name, his ID and the email address that is associated with this account (as it is shown in Figure 46).

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
00E9 04E0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00E9 04F0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00E9 0500:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00E9 0510:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00E9 0520:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00E9 0530:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00E9 0540:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00E9 0550:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00E9 0560:	00	00	00	00	00	00	00	00	00	00	00	00	03	22	0D	04"
00E9 0570:	29	2D	00	34	3A	35	39	41	4D	2C	20	44	65	63	20	31)-.4:59AM, Dec 1
00E9 0580:	36	6C	61	73	74	5F	73	79	6E	63	65	64	5F	74	69	6D	6last_synced_tim
00E9 0590:	65	38	0C	04	4F	33	00	43	3A	5C	55	73	65	72	73	5C	e8..03.C:\Users\
00E9 05A0:	46	6F	72	65	6E	73	69	63	5F	54	65	73	74	65	72	5C	Forensic_Tester\
00E9 05B0:	42	6F	78	20	53	79	6E	63	73	79	6E	63	5F	64	69	72	Box Syncsync_dir
00E9 05C0:	65	63	74	6F	72	79	5F	70	61	74	68	2C	0B	04	25	45	ectory_path,..%E
00E9 05D0:	00	34	32	37	30	38	37	35	37	32	32	32	32	73	79	6E	.427087572222syn
00E9 05E0:	63	5F	64	69	72	65	63	74	6F	72	79	5F	63	72	65	61	c_directory_crea
00E9 05F0:	74	69	6F	6E	5F	74	69	6D	65	27	0A	04	2B	35	00	32	tion_time'..+5.2
00E9 0600:	38	31	34	37	34	39	37	36	37	36	32	33	34	34	73	79	81474976762344sy
00E9 0610:	6E	63	5F	64	69	72	65	63	74	6F	72	79	5F	69	6E	6F	nc_directory_ino
00E9 0620:	64	65	1B	01	04	11	37	00	31	33	73	79	6E	63	33	5F	de....7.13sync3_
00E9 0630:	6D	69	67	72	61	74	69	6F	6E	5F	73	74	61	74	65	24	migration_state\$
00E9 0640:	09	04	35	25	00	68	74	74	70	73	3A	2F	2F	61	70	70	.5%.https://app
00E9 0650:	2E	62	6F	78	2E	63	6F	6D	2F	62	6F	78	5F	68	6F	6D	.box.com/box hom
00E9 0660:	65	70	61	67	65	27	08	04	31	2F	00	41	6E	64	72	65	epage'..1/ Andre
00E9 0670:	61	73	20	50	61	74	73	61	72	69	6B	61	73	64	69	73	as Patsarikasdis
00E9 0680:	70	6C	61	79	5F	75	73	65	72	5F	6E	61	6D	65	25	07	play_user name%
00E9 0690:	04	31	2B	00	46	61	6B	65	45	6E	74	65	72	70	72	69	.1+.FakeEnterpri
00E9 06A0:	73	65	4E	61	6D	65	65	6E	74	65	72	70	72	69	73	65	seNameenterprise
00E9 06B0:	5F	6E	61	6D	65	21	06	04	2D	27	00	46	61	6B	65	45	_name!..-'.FakeE
00E9 06C0:	6E	74	65	72	70	72	69	73	65	49	44	65	6E	74	65	72	nterpriseIDenter
00E9 06D0:	70	72	69	73	65	5F	69	64	22	05	04	35	21	00	6B	61	prise id"..5!
00E9 06E0:	61	64	61	64	38	37	40	68	6F	74	6D	61	69	6C	2E	63	████████@hotmail.c
00E9 06F0:	6F	6D	6C	6F	67	69	6E	5F	6E	61	6D	65	14	04	04	1F	omlogin name....
00E9 0700:	1B	00	35	37	35	39	30	35	31	31	31	75	73	65	72	5F	.57590511luser_
00E9 0710:	69	64	20	03	04	0F	43	00	31	75	73	65	72	5F	69	73	id ...C.luser_is
00E9 0720:	5F	63	75	72	72	65	6E	74	6C	79	5F	6C	6F	67	67	65	_currently_logge
00E9 0730:	64	5F	69	6E	0E	02	04	0F	1F	00	30	66	69	72	73	74	d_in.....0first
00E9 0740:	5F	72	75	6E	00	00	00	1C	37	00	39	73	79	6E	63	33	_run....7.9sync3
00E9 0750:	5F	6D	69	67	72	61	74	69	6F	6E	5F	73	74	61	74	65	_migration_state
00E9 0760:	00	00	00	08	00	00	00	00	FB	11	1A	84	EB	FO	A2	CB
00E9 0770:	B3	63	D1	20	DA	E0	5B	AD	0D	00	00	00	0D	01	0F	00	.c. ...[.....
00E9 0780:	03	0F	03	08	03	72	03	3C	03	06	02	00	02	09	01	06	r <

Figure 46: Discovery of username, email and ID in RAM

It is worth mentioning that we were also able to discover the password we entered to gain access to the Box cloud storage application (Figure 47).

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
096E 83B0:	7U	UU	b5	UU	3U	UU	b3	UU	bF	UU	b4	UU	b5	UU	2b	UU	p.e.=c.o.d.e.&
096E 83C0:	63	00	6C	00	69	00	65	00	6E	00	74	00	5F	00	69	00	c.l.i.e.n.t._i.
096E 83D0:	64	00	3D	00	64	00	78	00	6E	00	32	00	35	00	35	00	d.=d.x.n.2.5.5.
096E 83E0:	35	00	67	00	73	00	74	00	71	00	64	00	78	00	38	00	5.g.s.t.q.d.x.8.
096E 83F0:	6C	00	6B	00	74	00	34	00	38	00	71	00	30	00	68	00	l.k.t.4.8.q.0.h.
096E 8400:	61	00	76	00	71	00	6E	00	70	00	34	00	31	00	6F	00	a.v.q.n.p.4.1.o.
096E 8410:	61	00	78	00	26	00	62	00	6F	00	78	00	5F	00	6C	00	a.x.&.b.o.x._l.
096E 8420:	6F	00	67	00	69	00	6E	00	3D	00	6B	00	61	00	61	00	o.g.i.n.=k.a.a.
096E 8430:	64	00	61	00	64	00	38	00	37	00	25	00	34	00	30	00	d.a.d.8.7.%4.0.
096E 8440:	68	00	6F	00	74	00	6D	00	61	00	69	00	6C	00	2E	00	h.o.t.m.a.i.l...
096E 8450:	63	00	6F	00	6D	00	00	00	00	00	00	00	0C	56	E6	6C	c.o.m.....V.l
096E 8460:	40	00	00	00	00	00	00	00	34	6D	E6	6C	20	03	00	00	@.....4m.l...
096E 8470:	6C	6F	67	69	6E	3D	6B	61	61	64	61	64	38	37	40	68	login=kaadad87@h
096E 8480:	6F	74	6D	61	69	6C	2E	63	6F	6D	26	70	61	73	73	77	otmail.com&passw
096E 8490:	6F	72	64	3D	31	39	38	37	31	39	38	37	6B	26	72	65	ord=19871987k&re
096E 84A0:	6D	65	6D	62	65	72	5F	6C	6F	67	69	6E	3D	6F	6E	26	member_login=on&
096E 84B0:	6C	6F	67	69	6E	5F	73	75	62	6D	69	74	3D	4C	6F	67	login_submit=Log
096E 84C0:	67	69	6E	67	2B	69	6E	2E	2E	2E	26	64	6F	6C	6F	67	ging+in...&dolog
096E 84D0:	69	6E	3D	31	26	63	6C	69	65	6E	74	5F	69	64	3D	64	in=l&client_id=d
096E 84E0:	78	6E	32	35	35	35	67	73	74	71	64	78	38	6C	6B	74	xn2555gstqdx8lkt
096E 84F0:	34	38	71	30	68	61	76	71	6E	70	34	31	6F	61	78	26	48q0havqnp41oax&
096E 8500:	72	65	73	70	6F	6E	73	65	5F	74	79	70	65	3D	63	6F	response_type=co
096E 8510:	64	65	26	72	65	64	69	72	65	63	74	5F	75	72	69	3D	de&redirect_uri=
096E 8520:	68	74	74	70	73	25	33	41	25	32	46	25	32	46	61	63	https%3A%2F%2Fac
096E 8530:	63	6F	75	6E	74	2E	62	6F	78	2E	63	6F	6D	25	32	46	count.box.com%2F
096E 8540:	73	74	61	74	69	63	25	32	46	73	79	6E	63	5F	72	65	static%2Fsync_re
096E 8550:	64	69	72	65	63	74	2E	68	74	6D	6C	26	73	63	6F	70	direct.html&scop
096E 8560:	65	3D	72	6F	6F	74	5F	72	65	61	64	77	72	69	74	65	e=root_readwrite
096E 8570:	2B	69	74	65	6D	5F	64	65	6C	65	74	65	26	66	6F	6C	+item_delete&fol
096E 8580:	64	65	72	5F	69	64	3D	26	66	69	6C	65	5F	69	64	3D	der_id=&file_id=
096E 8590:	26	73	74	61	74	65	3D	62	6F	78	5F	63	73	72	66	5F	&state=box_csrf_
096E 85A0:	74	6F	6B	65	6E	5F	73	58	75	37	31	65	71	43	46	6A	token_sXu71eqCFj
096E 85B0:	34	53	6F	71	4C	32	26	72	65	67	5F	73	74	65	70	3D	4Sql2®_steps

Figure 47: Discovery of account's password

Next we focused on the discovery of the files that we uploaded. We successfully recovered the name, hash values, date and time of the files that we uploaded, and dates which are associated with the actions we performed (as we can see in Figure 48).

		00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
2AFC	0010:	4E	6F	6E	65	2C	20	75	27	6F	77	6E	65	64	5F	62	79	None, u'owned_by
2AFC	0020:	27	3A	20	7B	75	27	69	64	27	3A	20	75	27	35	37	35	': {u'id': u'575
2AFC	0030:	39	30	35	31	31	31	27	7D	2C	20	75	27	74	79	70	65	905111'}, u'type
2AFC	0040:	27	3A	20	75	27	66	69	6C	65	27	2C	20	75	27	69	64	': u'file', u'id
2AFC	0050:	27	3A	20	75	27	31	31	32	32	35	38	39	37	36	39	33	': u'11225897693
2AFC	0060:	31	27	2C	20	75	27	73	69	7A	65	27	3A	20	33	34	37	1', u'size': 347
2AFC	0070:	36	36	7D	2C	20	7B	75	27	73	68	61	31	27	3A	20	75	66}, {u'sha1': u
2AFC	0080:	27	32	37	35	38	30	30	34	61	33	30	30	61	64	30	39	'2758004a300ad09
2AFC	0090:	62	39	33	34	34	64	39	63	62	35	33	30	63	66	62	32	b9344d9cb530cfb2
2AFC	00A0:	61	39	65	33	32	37	62	33	65	27	2C	20	75	27	6E	61	a9e327b3e', u'na
2AFC	00B0:	6D	65	27	3A	20	75	27	30	31	39	31	39	32	2E	6A	70	me': u'019192.jp
2AFC	00C0:	67	27	2C	20	75	27	70	61	72	65	6E	74	27	3A	20	7B	s', u'parent': {
2AFC	00D0:	75	27	69	64	27	3A	20	75	27	30	27	7D	2C	20	75	27	u'id': u'0'}, u'
2AFC	00E0:	63	6F	6E	74	65	6E	74	5F	63	72	65	61	74	65	64	5F	content_created_
2AFC	00F0:	61	74	27	3A	20	75	27	32	30	31	36	2D	31	32	2D	30	at': u'2016-12-0
2AFC	0100:	34	54	31	31	3A	35	39	3A	31	35	2D	30	38	3A	30	30	4T11:59:15-08:00
2AFC	0110:	27	2C	20	75	27	63	72	65	61	74	65	64	5F	61	74	27	', u'created_at':
2AFC	0120:	3A	20	75	27	32	30	31	36	2D	31	32	2D	31	35	54	31	: u'2016-12-15T1
2AFC	0130:	39	3A	33	39	3A	31	38	2D	30	38	3A	30	30	27	2C	20	9:39:18-08:00',
2AFC	0140:	75	27	6D	6F	64	69	66	69	65	64	5F	61	74	27	3A	20	u'modified_at':
2AFC	0150:	75	27	32	30	31	36	2D	31	32	2D	31	35	54	31	39	3A	u'2016-12-15T19:
2AFC	0160:	33	39	3A	31	38	2D	30	38	3A	30	30	27	2C	20	75	27	39:18-08:00', u'
2AFC	0170:	69	74	65	6D	5F	73	74	61	74	75	73	27	3A	20	75	27	item_status': u'
2AFC	0180:	61	63	74	69	76	65	27	2C	20	75	27	63	6F	6E	74	65	active', u'conte
2AFC	0190:	6E	74	5F	6D	6F	64	69	66	69	65	64	5F	61	74	27	3A	nt_modified_at':
2AFC	01A0:	20	75	27	32	30	30	30	2D	30	34	2D	31	32	54	30	36	u'2000-04-12T06
2AFC	01B0:	3A	32	30	3A	35	34	2D	30	37	3A	30	30	27	2C	20	75	:20:54-07:00', u'
2AFC	01C0:	27	73	65	71	75	65	6E	63	65	5F	69	64	27	3A	20	75	'sequence_id': u
2AFC	01D0:	27	30	27	2C	20	75	27	65	74	61	67	27	3A	20	75	27	'0', u'etag': u'
2AFC	01E0:	30	27	2C	20	75	27	6C	6F	63	6B	27	3A	20	4E	6F	6E	0', u'lock': Non
2AFC	01F0:	65	2C	20	75	27	6F	77	6E	65	64	5F	62	79	27	3A	20	e, u'owned_by':
2AFC	0200:	7B	75	27	69	64	27	3A	20	75	27	35	37	35	39	30	35	{u'id': u'575905
2AFC	0210:	31	31	31	27	7D	2C	20	75	27	74	79	70	65	27	3A	20	111'}, u'type':
2AFC	0220:	75	27	66	69	6C	65	27	2C	20	75	27	69	64	27	3A	20	u'file', u'id':
2AFC	0230:	75	27	31	31	32	32	35	39	30	33	36	38	37	37	27	2C	u'112259036877',

Figure 48: Discovery of the files we transferred

To sum them up, with the examination of RAM we discovered information about:

- the username
- the email address that is associated with this account
- the user ID
- the password we entered to gain access to Box cloud storage application
- the name, hash values, date and time of the files that we uploaded
- the time and dates which are associated with the actions we performed

Table 16: Examination of RAM (use of Box's application software)

Source	Findings
Logs	<p>Information about:</p> <ul style="list-style-type: none"> • the update of the service • the operations of the service • the name of the files, their size and their hash values • the time and date when we uploaded them • the ID, the name and email of the user
Database <ul style="list-style-type: none"> • item_status.db 	<p>Information about:</p> <ul style="list-style-type: none"> • the files we uploaded • the time and date when we uploaded them • the email of the user
RAM	<p>Information about:</p> <ul style="list-style-type: none"> • the name, hash values and size of the files • the date and time when we uploaded them • the username, email address and user ID of the account that we used

7.5 Use of the Application Software for Retrieving Files

In this scenario we downloaded the files that we had stored on the application server. When we connect to the application server then the data of our folder, which are located locally on the computer, synchronize automatically with those on the server.

7.5.1 Event Logs Examination

By examining the log files, we discover the files that we downloaded, their hash values, their size, the date and time that we downloaded them (as we can see in Table 17).

Table 17: Examination of Log files (1)

```
36m2016-12-16 04:36:18.660 3368 INFO BoxFSMonitor network_layer |
JSON response received for network request with content: {u'items': [{u'sha1'
u'2758004a300ad09b9344d9cb530cfb2a9e327b3e', u'name': u'019192.jpg',
u'parent': {u'id': u'0'}, u'content_created_at': u'2016-12-04T11:59:15-08:00',
u'created_at': u'2016-12-04T11:59:26-08:00', u'modified_at': u'2016-12-
04T11:59:26-08:00', u'item_status': u'active', u'content_modified_at': u'2000-04-
12T06:20:54-07:00', u'sequence_id': u'0', u'etag': u'0', u'lock': None, u'owned_by':
{u'id': u'575905111'}, u'type': u'file', u'id': u'108300074769', u'size': 62206, {u'sha1':
u'a6440367100dbac450c1ff574ab374ccdcbbcd0a', u'name': u'020958.txt', u'parent':
{u'id': u'0'}, u'content_created_at': u'2016-12-04T11:59:15-08:00', u'created_at':
u'2016-12-04T11:59:26-08:00', u'modified_at': u'2016-12-04T11:59:26-08:00',
u'item_status': u'active', u'content_modified_at': u'1997-07-23T03:59:02-07:00',
u'sequence_id': u'0', u'etag': u'0', u'lock': None, u'owned_by': {u'id': u'575905111'},
u'type': u'file', u'id': u'108300081950', u'size': 34766, {u'sha1':
u'8fd64d66d0d5b36ba919f679f9c5302a83fcf8d1', u'name': u'028620.pdf', u'parent':
{u'id': u'0'}, u'content_created_at': u'2016-12-04T11:59:15-08:00', u'created_at':
u'2016-12-04T12:00:05-08:00', u'modified_at': u'2016-12-04T12:00:05-08:00',
u'item_status': u'active', u'content_modified_at': u'2004-07-20T03:29:00-07:00',
u'sequence_id': u'0', u'etag': u'0', u'lock': None, u'owned_by': {u'id': u'575905111'},
u'type': u'file', u'id': u'108300129720', u'size': 888697, {u'sha1':
u'172e4d9f01f33feb16fcfd5392f4b11ce706af29', u'name': u'093340.doc', u'parent':
{u'id': u'0'}, u'content_created_at': u'2016-12-04T11:59:15-08:00', u'created_at':
u'2016-12-04T12:01:11-08:00', u'modified_at': u'2016-12-04T12:01:11-08:00',
u'item_status': u'active', u'content_modified_at': u'2008-02-22T00:47:16-08:00',
u'sequence_id': u'0', u'etag': u'0', u'lock': None, u'owned_by': {u'id': u'575905111'},
u'type': u'file', u'id': u'108300255200', u'size': 3515904 ]}}
```

Finally, we recovered the user's name, the email address and the user ID that are associated with this account (as we can see in Table 18).

Table 18: Examination of Log files (2)

```
36m2016-12-16 04:34:17.851 4040 INFO CompleteAuthenticati network_layer
JSON response received for network request with content: {u'name': u'Andreas
Patsarikas', u'hostname': u'https://app.box.com/', u'enterprise': None, u'login':
u'kaadad87@hotmail.com', u'type': u'user', u'id': u'575905111' }
```

Next we head to the folder “C:\Users\Forensic_Tester\AppData\Roaming\Box Sync\UserData”. There in file “ChecksumHashFile.txt” we find the name of the files, their size and their hash values (Figure 49).

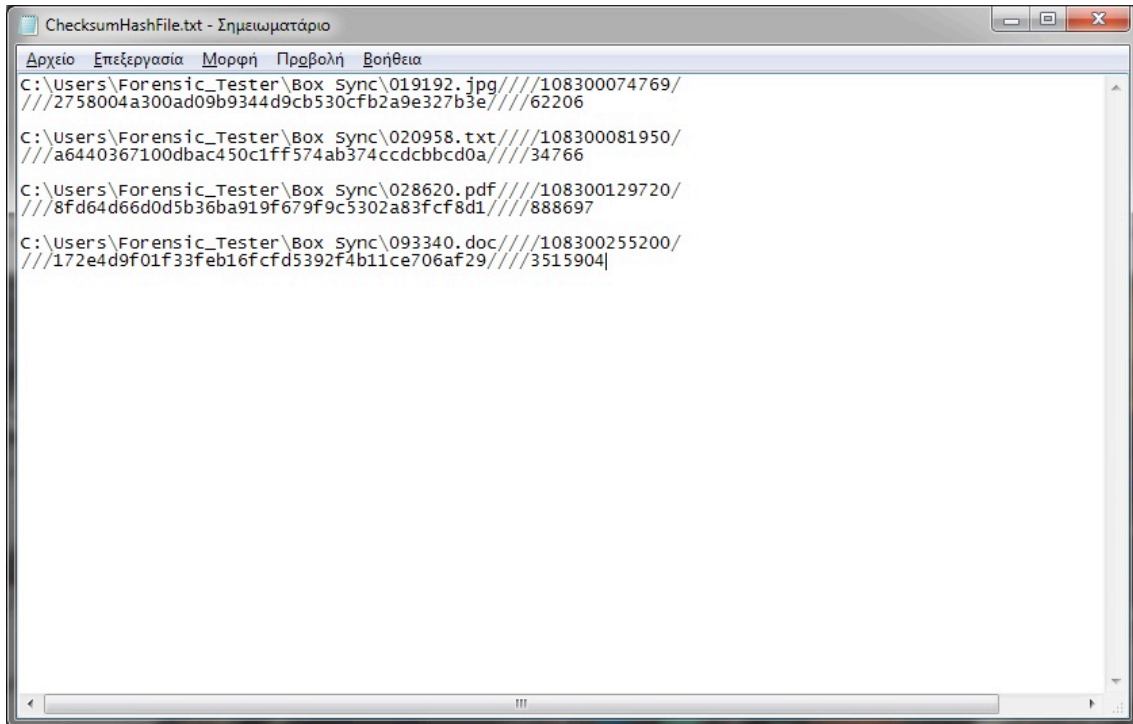


Figure 49: Discovery of the files we transferred

Summing up:

Table 19: Use of Box’s application software

Source	Findings
Logs	Information about: <ul style="list-style-type: none"> • the update of the service • the operations of the service • the name of the files, their size and their hash values • the time and date when we uploaded them • the ID, the name and email of the user
Database	Information about:

<ul style="list-style-type: none"> • item_status.db 	<ul style="list-style-type: none"> • the files we uploaded • the time and date when we uploaded them • the email of the user
C:\Users\Forensic_Tester\AppData\Roaming\Box Sync\UserData <ul style="list-style-type: none"> • ChecksumHashFile.txt 	Information about: <ul style="list-style-type: none"> • the name of the files • their size • their hash values

7.5.2 Examination of RAM

By examining the RAM, we found the name of files, their size, their hash values and the time and date we downloaded them (as shown in Figure 50).

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
1BC3 4B90:	31	38	20	30	32	3A	33	32	3A	34	32	2E	33	35	35	20	18 02:32:42.355
1BC3 4BA0:	31	37	34	38	20	44	45	42	55	47	20	20	20	4C	6F	63	1748 DEBUG Loc
1BC3 4BB0:	61	6C	45	78	65	63	75	74	6F	72	2D	38	20	20	20	20	ocalExecutor-8
1BC3 4BC0:	20	20	6C	61	73	74	5F	73	79	6E	63	5F	69	74	65	6D	last_sync_item
1BC3 4BD0:	5F	73	74	6F	72	65	20	20	70	65	72	73	69	73	74	5F	_store persist_
1BC3 4BE0:	75	70	64	61	74	65	64	5F	69	74	65	6D	5F	73	74	61	updated_item_sta
1BC3 4BF0:	74	65	73	3A	20	69	74	65	6D	5F	65	78	69	73	74	65	tes: item_existe
1BC3 4C00:	64	3D	54	72	75	65	2C	20	62	6F	78	5F	36	31	2C	20	d=True, box_61,
1BC3 4C10:	7B	75	27	6C	6F	63	6B	5F	69	64	27	3A	20	4E	6F	6E	{'lock_id': Non
1BC3 4C20:	65	2C	20	75	27	6C	6F	63	6B	5F	6F	77	6E	65	72	5F	e, 'lock_owner_
1BC3 4C30:	69	64	27	3A	20	4E	6F	6E	65	2C	20	75	27	62	6F	78	id': None, u'box
1BC3 4C40:	5F	69	64	27	3A	20	75	27	31	31	32	38	34	37	36	35	_id': u'11284765
1BC3 4C50:	30	37	30	30	27	2C	20	75	27	70	61	72	65	6E	74	5F	0700', u'parent_
1BC3 4C60:	69	74	65	6D	5F	69	64	27	3A	20	75	27	30	27	2C	20	item_id': u'0',
1BC3 4C70:	75	27	6E	61	6D	65	27	3A	20	75	27	30	31	39	31	39	u'name': u'01919
1BC3 4C80:	32	2E	6A	70	67	27	2C	20	75	27	63	68	65	63	6B	73	2.jpg', u'checks
1BC3 4C90:	75	6D	27	3A	20	75	27	32	37	35	38	30	30	34	61	33	um': u'2758004a3
1BC3 4CA0:	30	30	61	64	30	39	62	39	33	34	34	64	39	63	62	35	00ad09b9344d9cb5
1BC3 4CB0:	33	30	63	66	62	32	61	39	65	33	32	37	62	33	65	27	30cfb2a9e327b3e'
1BC3 4CC0:	2C	20	75	27	69	74	65	6D	5F	74	79	70	65	27	3A	20	, u'item_type':
1BC3 4CD0:	30	2C	20	75	27	69	73	5F	64	65	6C	65	74	65	64	27	0, u'is_deleted'
1BC3 4CE0:	3A	20	31	2C	20	75	27	73	69	7A	65	27	3A	20	36	32	: 1, u'size': 62
1BC3 4CF0:	32	30	36	2C	20	75	27	6F	77	6E	65	72	5F	69	64	27	206, u'owner_id'
1BC3 4D00:	3A	20	75	27	35	37	35	39	30	35	31	31	31	27	7D	1B	: u'575905111'}
1BC3 4D10:	5B	30	6D	0D	0A	1B	5B	33	32	6D	32	30	31	36	2D	31	[Om...[32m2016-1
1BC3 4D20:	32	2D	31	38	20	30	32	3A	33	32	3A	34	32	2E	33	37	2-18 02:32:42.37
1BC3 4D30:	31	20	31	37	34	38	20	44	45	42	55	47	20	20	20	4C	1 1748 DEBUG L
1BC3 4D40:	6F	63	61	6C	45	78	65	63	75	74	6F	72	2D	38	20	20	ocalExecutor-8
1BC3 4D50:	20	20	20	20	73	79	6E	63	5F	65	76	65	6E	74	5F	71	sync_event_q
1BC3 4D60:	75	65	75	65	20	20	20	20	20	20	55	70	64	61	74	69	ueue Update
1BC3 4D70:	6E	67	20	73	79	6E	63	20	65	76	65	6E	74	20	45	53	ng sync event ES
1BC3 4D80:	4E	3D	31	31	20	74	6F	20	53	55	43	43	45	45	44	45	N=11 to SUCCEDE
1BC3 4D90:	44	20	65	76	65	6E	74	20	73	74	61	74	65	2C	20	66	D event state, f
1BC3 4DA0:	72	6F	6D	20	49	4E	5F	50	52	4F	43	45	53	53	20	65	rom IN_PROCESS e
1BC3 4DB0:	76	65	6E	74	20	73	74	61	74	65	2C	20	69	6E	20	4C	vent state, in L
1BC3 4DC0:	4F	43	41	4C	20	67	72	61	70	68	2E	1B	5B	30	6D	0D	OCAL graph..[Om.

Figure 50: Examination of RAM (1)

Lastly, as shown by the following figure (Figure 51), we found information, such as the user's name, email address and user ID and the last time the user logged in, which are associated with the account that we used.

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
006D 5640:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
006D 5650:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
006D 5660:	00	00	00	00	00	00	00	00	00	00	00	00	03	22	0D	04"
006D 5670:	29	2D	00	32	3A	33	32	41	4D	2C	20	44	65	63	20	31)-.2:32AM, Dec 1
006D 5680:	38	6C	61	73	74	5F	73	79	6E	63	65	64	5F	74	69	6D	8last_synced_tim
006D 5690:	65	38	0C	04	4F	33	00	43	3A	5C	55	73	65	72	73	5C	e8..03.C:\Users\ Forensic_Tester\ Box Syncsync_dir ectory_path,..%E .427087572222syn c_directory_crea tion_time'+5.2 81474976762344sy nc_directory_ino de....7.13sync3_ migration_state\$..5%.https://app .box.com/box_hom epage'..1/.Andre as Patsarikasdis play_user_name%. .1+.FakeEnterpri seNameenterprise _name!..-'.FakeE nterpriseIDenter prise_id"..5!.. @hotmail.c omlogin name.... ..575905111user_ id ...C.luser is _currently_logge d_in.....0first _run....7.9sync3 _migration_state '..j...j.....
006D 56A0:	46	6F	72	65	6E	73	69	63	5F	54	65	73	74	65	72	5C	
006D 56B0:	42	6F	78	20	53	79	6E	63	73	79	6E	63	5F	64	69	72	
006D 56C0:	65	63	74	6F	72	79	5F	70	61	74	68	2C	0B	04	25	45	
006D 56D0:	00	34	32	37	30	38	37	35	37	32	32	32	32	73	79	6E	
006D 56E0:	63	5F	64	69	72	65	63	74	6F	72	79	5F	63	72	65	61	
006D 56F0:	74	69	6F	6E	5F	74	69	6D	65	27	0A	04	2B	35	00	32	
006D 5700:	38	31	34	37	34	39	37	36	37	36	32	33	34	34	73	79	
006D 5710:	6E	63	5F	64	69	72	65	63	74	6F	72	79	5F	69	6E	6F	
006D 5720:	64	65	1B	01	04	11	37	00	31	33	73	79	6E	63	33	5F	
006D 5730:	6D	69	67	72	61	74	69	6F	6E	5F	73	74	61	74	65	24	
006D 5740:	09	04	35	25	00	68	74	74	70	73	3A	2F	2F	61	70	70	
006D 5750:	2E	62	6F	78	2E	63	6F	6D	2F	62	6F	78	5F	68	6F	6D	
006D 5760:	65	70	61	67	65	27	08	04	31	2F	00	41	6E	64	72	65	
006D 5770:	61	73	20	50	61	74	73	61	72	69	6B	61	73	64	69	73	
006D 5780:	70	6C	61	79	5F	75	73	65	72	5F	6E	61	6D	65	25	07	
006D 5790:	04	31	2B	00	46	61	6B	65	45	6E	74	65	72	70	72	69	
006D 57A0:	73	65	4E	61	6D	65	65	6E	74	65	72	70	72	69	73	65	
006D 57B0:	5F	6E	61	6D	65	21	06	04	2D	27	00	46	61	6B	65	45	
006D 57C0:	6E	74	65	72	70	72	69	73	65	49	44	65	6E	74	65	72	
006D 57D0:	70	72	69	73	65	5F	69	64	22	05	04	35	21	00	6B	61	
006D 57E0:	61	64	61	64	38	37	40	68	6F	74	6D	61	69	6C	2E	63	
006D 57F0:	6F	6D	6C	6F	67	69	6E	5F	6E	61	6D	65	14	04	04	1F	
006D 5800:	1B	00	35	37	35	39	30	35	31	31	31	75	73	65	72	5F	
006D 5810:	69	64	20	03	04	0F	43	00	31	75	73	65	72	5F	69	73	
006D 5820:	5F	63	75	72	72	65	6E	74	6C	79	5F	6C	6F	67	67	65	
006D 5830:	64	5F	69	6E	0E	02	04	0F	1F	00	30	66	69	72	73	74	
006D 5840:	5F	72	75	6E	00	00	00	1C	37	00	39	73	79	6E	63	33	
006D 5850:	5F	6D	69	67	72	61	74	69	6F	6E	5F	73	74	61	74	65	
006D 5860:	60	D4	6A	07	80	D8	6A	07	02	00	00	00	00	00	00	00	

Figure 51: Discovery of user's name, email address and user ID

Summing up, the information that we recovered by examining RAM, are the following:

- the name of the files
- their size
- their hash values
- the time and date when we downloaded them
- information related to the account that we used, like the user's name, email address and user ID
- the last time that user logged in

7.6 Results of Box's Application Software Analysis

In the following table (Table 20) our findings from the scenario of file transferring through Box's application software are briefly presented.

Table 20: Use of Box's application software (summarized)

Source	Findings
Logs	Information about: <ul style="list-style-type: none"> • the update of the service • the operations of the service • the name of the files, their size and their hash values • the time and date when we uploaded them • the ID, the name and email address of the user
Database <ul style="list-style-type: none"> • item_status.db 	Information about: <ul style="list-style-type: none"> • the files we uploaded • the time and date when we uploaded them • the email address of the user
C:\Users\Forensic_Tester\AppData\Roaming\Box Sync\UserData <ul style="list-style-type: none"> • ChecksumHashFile.txt 	Information about: <ul style="list-style-type: none"> • the name of the files • their size • their hash values
RAM	Information about: <ul style="list-style-type: none"> • the name, hash values and size of the files • the date and time when we uploaded them • the username, email address

	<p>and user ID of the account that we used</p> <ul style="list-style-type: none"> • the last time that the user logged in
--	--

7.7 Access through Browser

In this subchapter we will use Box through a browser. In the following figure (Figure 52) we can see the application’s interface.

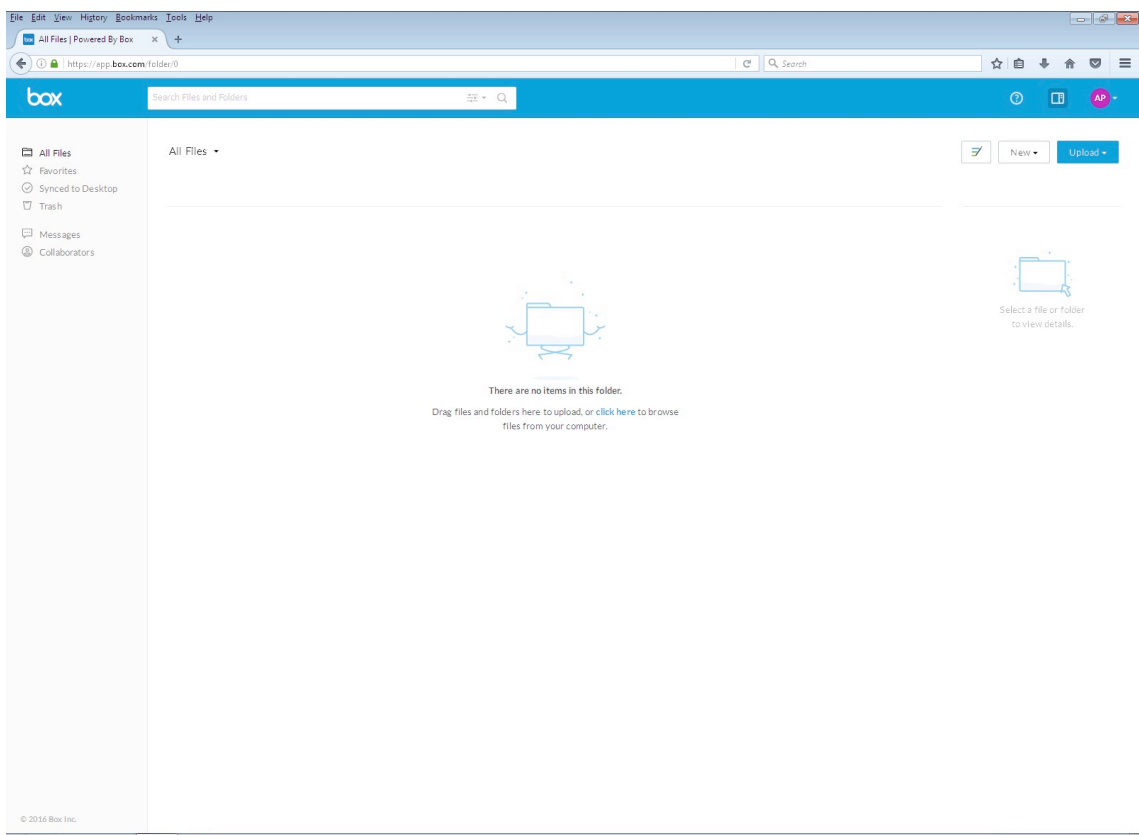


Figure 52: Application’s interface through a browser

7.7.1 Use of Mozilla Firefox

In this scenario we will use Mozilla Firefox, through which we will upload our files on the application server. By following the methodology, we have defined, we were able to identify many references that prove our access to Box cloud storage service.

The examination of Firefox’s History proves that indeed we gained access to the application’s website (as we can see in Figure 53).

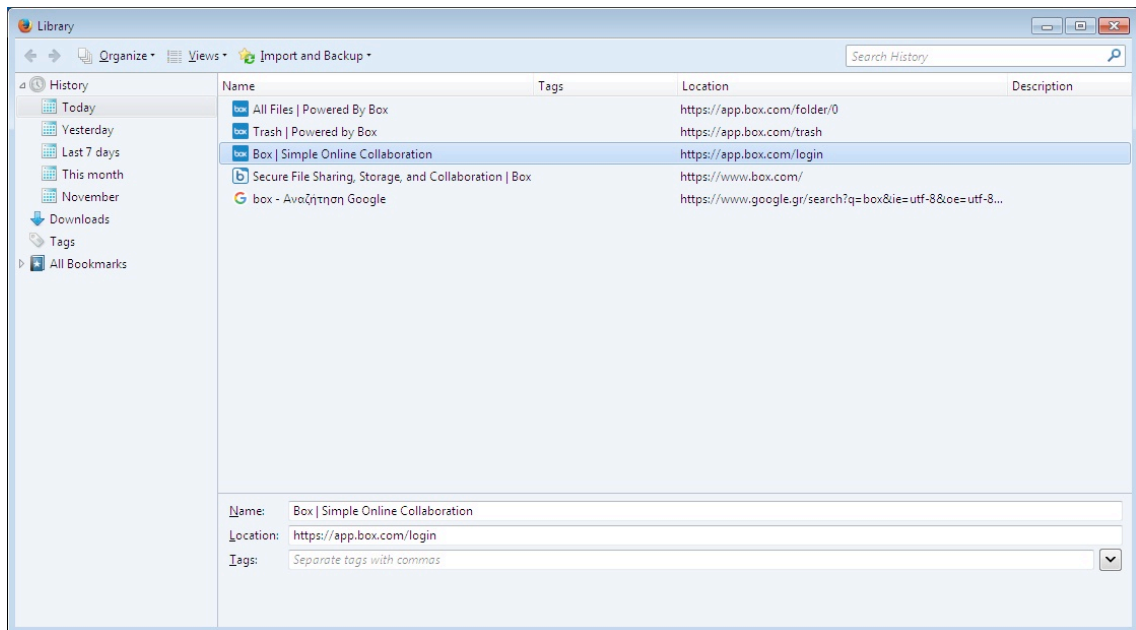


Figure 53: Mozilla Firefox's History

Also as we have seen in Chapter 6, all the data that are generated from the use of Mozilla Firefox are stored in the following location “C:\Users\Forensic_Tester\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxxx.default”. There we find “places.sqlite” database, where the History of the browser is stored, and “cookies.sqlite” where the browser cookies are stored. We will examine the contents of these files, by using the “DB Browser for SQLite” (as we can see in Figure 54 and Figure 55).

We discovered the name and type of the files that we uploaded to Box cloud storage service. We also found when we last visited the site, how many times and when we uploaded the files.

DB Browser for SQLite - C:/Users/Forensic_Tester/AppData/Roaming/Mozilla/Firefox/Profiles/bb7b39k.default/places.sqlite

File Edit View Help

New Database Open Database Write Changes Revert Changes

Database Structure Browse Data Edit Pragma Execute SQL

Table: moz_places

id	url	title	v_ho	t_co	idder	typec	icon	scen	last_visit_date	guid	foreign_count	
64	52	https://efantasy.gr/	rg...	1	1	0	NULL	1901	1480510329197000	zhsFTKGCjb95	0	
65	107	https://e3.boxcdn.net/box-installers/sync/Sync...	te...	0	0	0	NULL	0	1481766640332000	OYT-DB_PNYKp	0	
66	12	https://dl.google.com/tag/s/appguid%3D%7B8...	m...	0	0	0	NULL	0	148050985293000	_dRo-DySTGu_	0	
67	98	https://dl-web.dropbox.com/installer?juno=Tr...	m...	0	0	0	NULL	0	1480880999141000	ZFnp6qkcGqK7	0	
68	113	https://app.box.com/trash	Trash Powered by Box	m...	3	0	0	27	300	1482039293185000	iRy7tluNoE7	0
69	87	https://app.box.com/login/assertion?a=laLive...	NULL	m...	1	1	0	NULL	98	1480880819434000	43XbrVBE8H9H	0
70	101	https://app.box.com/login/assertion?a=laLive...	NULL	m...	1	1	0	NULL	98	1481766576086000	-cqeGTH5eI0B	0
71	91	https://app.box.com/login	Box Simple Online Collaboration	m...	3	0	0	27	270	1482031610742000	ESBenOMQbs90	0
72	89	https://app.box.com/folder/0	All Files Powered By Box	m...	9	0	0	27	670	1482039298188000	7a-TTUmF2NYk	0
73	99	https://app.box.com/files/0/f/0/1/f_10830012...	NULL	m...	2	1	0	NULL	195	1481766576383000	NriqQuCFUD70	0
74	120	https://app.box.com/file/112882998441	019192.jpg Powered By Box	m...	1	0	0	27	100	1482038677914000	yy3LMUqnesOT	0
75	102	https://app.box.com/file/108300129720	028620.pdf Powered By Box	m...	1	0	0	27	-1	1481766576899000	9s2vvpATnudA	0
76	93	https://app.box.com/apps	Box Simple Online Collaboration: Onl...	m...	1	0	0	28	98	1480880843571000	ESfv1L6u2yLr	0
77	88	https://app.box.com/	NULL	m...	7	1	0	NULL	610	1482031630343000	w4MFCEOgA3J	0
78	62	https://amazon.co.uk/	NULL	ku...	1	1	0	NULL	1901	1480510489568000	7k112URHJD-R	0
79	26	https://accounts.google.com/ServiceLogin?hl=...	YouTube	m...	1	0	0	14	94	1480509238434000	bEec2Tlnh3VZ	0
80	25	https://accounts.google.com/ServiceLogin?hl=...	YouTube	m...	1	0	0	14	94	1480509230753000	qecTOeL3HmDI	0
81	24	https://accounts.google.com/ServiceLogin?hl=...	NULL	m...	1	0	0	NULL	94	1480509229915000	SjNBUtC6Q2IL	0
82	27	https://accounts.google.com/CheckCookie?hl=...	Google Accounts	m...	1	0	0	14	94	1480509248125000	Eb3fUqUXsEse	0
83	100	https://account.box.com/login?redirect_url=%...	Box Simple Online Collaboration	m...	1	0	0	27	98	1481766563493000	j5Bzjhjed_1P	0

64 - 84 of 120

Go to: 1

UTF-8

Figure 54: Examination of Firefox's History database

DB Browser for SQLite - C:/Users/Forensic_Tester/AppData/Roaming/Mozilla/Firefox/Profiles/bb7b39k.default/cookies.sqlite

File Edit View Help

New Database Open Database Write Changes Revert Changes

Database Structure Browse Data Edit Pragma Execute SQL

Table: moz_cookies

id	baseDomain	Attri	name	value	host	path	expiry	lastAccessed	creationTime	isSecure
77	660	box.com	optimizelyEndUserId	oeu14808807...	.box.com	/	1796240796	14820398382...	14808807964...	0
78	661	box.com	_sdsat_session_count	1	www.box.com	/	1543952796	14820316054...	14808807965...	0
79	662	box.com	_sdsat_lt_pages_viewed	1	www.box.com	/	1543952796	14820316054...	14808807965...	0
80	664	box.com	box_marketing	1	.box.com	/	1512416796	14820398382...	14808807966...	1
81	665	box.com	_uc_referrer	direct	.www.box.com	/	1512416796	14820316054...	14808807969...	0
82	666	box.com	_uc_last_referrer	direct	.www.box.com	/	1512416796	14820316054...	14808807969...	0
83	667	box.com	_uc_initial_landing_page	https%3A/w...	.www.box.com	/	1512416796	14820316054...	14808807969...	0
84	668	box.com	_uc_current_session	true	.www.box.com	/	1480884396	14808807969...	14808807969...	0
85	669	box.com	_uc_visits	1	.www.box.com	/	1512416796	14820316054...	14808807969...	0
86	671	box.com	_jm_visits	1	www.box.com	/	1512416797	14820316054...	14808807970...	1
87	672	box.com	_jm_journey	%2Chttps%3...	www.box.com	/	1512416797	14820316054...	14808807970...	1
88	676	box.com	s_depth	1	.box.com	/	1480882598	14808809204...	14808807980...	0
89	683	box.com	AMCV_B9828F7954807624...	793872103%...	.box.com	/	1543952798	14820398382...	14808807965...	0
90	700	box.com	s_nrm	24681347130...	.box.com	/	1512416806	14820398382...	14808807980...	0
91	701	box.com	s_lv	1480880806331	.box.com	/	1575488806	14820398382...	14808807980...	0
92	702	box.com	s_lv_s	First%20visit	.box.com	/	1480882606	14808808953...	14808807980...	0
93	703	box.com	s_ppn	www.box.co...	.box.com	/	1480882606	14808808953...	14808807980...	0
94	711	box.com	lang	en-US	.box.com	/	1486237619	14820398382...	14808807937...	1
95	712	box.com	box_locale	en_US	.box.com	/	1486237619	14820398382...	14808807937...	1
96	714	box.com	dc575905111	6EC078381C1...	.account.box...	/	2427565619	14820398391...	14808808190...	1

77 - 97 of 369

Go to: 1

Open an existing database file

UTF-8

Figure 55: Examination of Firefox's Cookies database

The examination of RAM led us to the discovery of evidence that confirm the use of Box cloud storage service, the name of the files and the time and date when we uploaded them (Figure 56 and Figure 57).

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
18C5 1940:	6D	62	37	4E	50	59	6B	57	7A	72	7A	74	2D	26	72	65	mb7NPYkWrzt-&re
18C5 1950:	64	69	72	65	63	74	5F	75	72	6C	3D	25	32	46	6D	6F	direct_url=%2Fmo
18C5 1960:	63	2E	78	6F	62	2E	70	70	61	2E	62	00	05	42	DA	6F	c.xob.ppa.b..B.o
18C5 1970:	32	72	10	34	33	58	62	72	56	42	45	38	48	39	48	2B	2r.43XbrVBE8H9H+
18C5 1980:	12	85	7F	00	FC	78	56	0E	00	47	4F	2D	09	08	08	01	xV..GO-
18C5 1990:	01	06	25	08	05	68	74	74	70	73	3A	2F	2F	61	63	63	..%.https://acc
18C5 19A0:	6F	75	6E	74	2E	62	6F	78	2E	63	6F	6D	2F	6C	6F	67	ount.box.com/log
18C5 19B0:	69	6E	42	6F	78	20	7C	20	53	69	6D	70	6C	65	20	4F	inBox Simple O
18C5 19C0:	6E	6C	69	6E	65	20	43	6F	6C	6C	61	62	6F	72	61	74	nline Collaborat
18C5 19D0:	69	6F	6E	6D	6F	63	2E	78	6F	62	2E	74	6E	75	6F	63	ionmoc.xob.tnuoc
18C5 19E0:	63	61	2E	1B	62	00	05	42	DA	6E	7C	8B	A8	5F	4A	65	ca..b..B.n .._Je
18C5 19F0:	5A	62	6E	6B	7A	59	4C	6C	4A	2B	12	61	C3	AD	D9	81	ZbnkzYLlJ+.a....
18C5 1A00:	08	55	0E	00	49	75	25	09	08	08	01	01	06	25	08	05	.U..Iu%.....%..
18C5 1A10:	68	74	74	70	73	3A	2F	2F	77	77	77	2E	62	6F	78	2E	https://www.box.
18C5 1A20:	63	6F	6D	2F	65	6E	2D	67	62	2F	68	6F	6D	65	42	6F	com/en-gb/homeBc
18C5 1A30:	78	20	7C	20	53	65	63	75	72	65	20	46	69	6C	65	20	x Secure File
18C5 1A40:	53	68	61	72	69	6E	67	2C	20	53	74	6F	72	61	67	65	Sharing, Storage
18C5 1A50:	20	61	6E	64	20	43	6F	6C	6C	61	62	6F	72	61	74	69	and Collaborati
18C5 1A60:	6F	6E	6D	6F	63	2E	78	6F	62	2E	77	77	77	2E	1A	62	onmoc.xob.www..b
18C5 1A70:	00	05	42	DA	6D	BE	6F	B0	56	58	43	63	36	35	4E	44	..B.m.o.VXcc65ND
18C5 1A80:	34	46	35	32	2B	12	C9	E7	54	46	6E	59	0E	00	45	41	4F52+...TFnY..FA
18C5 1A90:	25	01	08	09	01	02	06	25	08	05	68	74	74	70	73	3A	%.....%..https:
18C5 1AA0:	2F	2F	61	70	70	2E	62	6F	78	2E	63	6F	6D	2F	66	6F	//app.box.com/fo
18C5 1AB0:	6C	64	65	72	2F	30	41	6C	6C	20	46	69	6C	65	73	20	lder/0All Files
18C5 1AC0:	7C	20	50	6F	77	65	72	65	64	20	42	79	20	42	6F	78	Powered By Box
18C5 1AD0:	6D	6F	63	2E	78	6F	62	2E	70	70	61	2E	0B	1B	0B	E7	moc.xob.ppa.....
18C5 1AE0:	00	05	43	E8	4A	A7	40	B0	37	61	2D	54	54	55	6D	46	..C.J.@.7a-TTUmf
18C5 1AF0:	32	4E	79	4B	2B	12	18	A5	5D	18	81	44	53	0F	00	81	2NyK+...].DS...
18C5 1B00:	65	4B	29	09	08	08	01	01	06	25	08	05	68	74	74	70	eK).....%.http
18C5 1B10:	73	3A	2F	2F	77	77	77	2E	67	6F	6F	67	6C	65	2E	67	s://www.google.g
18C5 1B20:	72	2F	73	65	61	72	63	68	3F	71	3D	62	6F	78	26	69	r/search?q=box&i
18C5 1B30:	65	3D	75	74	66	2D	38	26	6F	65	3D	75	74	66	2D	38	e=utf-8&oe=utf-8
18C5 1B40:	26	63	6C	69	65	6E	74	3D	66	69	72	65	66	6F	78	2D	&client=firefox-
18C5 1B50:	62	2D	61	62	26	67	77	73	5F	72	64	3D	63	72	26	65	b-ab&gws_rd=cr&e
18C5 1B60:	69	3D	6B	33	4A	45	57	4C	75	52	4A	73	54	53	67	41	i=k3JEWLuRJsTSgA
18C5 1B70:	62	63	73	36	54	67	41	67	62	6F	78	20	2D	20	CE	91	bcs6TgAgbox - ..
18C5 1B80:	CE	BD	CE	B1	CE	B6	CE	AE	CF	84	CE	B7	CF	83	CE	B7
18C5 1B90:	20	47	6F	6F	67	6C	65	72	67	2E	65	6C	67	6F	6F	67	Googlerg.elgoog
18C5 1BA0:	2E	77	77	77	2E	07	62	00	05	42	DA	6D	57	4D	58	4E	.www..b..B.mwMXN
18C5 1BB0:	57	33	4D	78	61	6B	6D	54	2D	6A	38	2B	12	BF	53	BD	W3MxakmT-j8+...S.
18C5 1BC0:	CB	75	F5	00	10	00	00	00	00	00	00	00	00	00	00	00	.u.....
18C5 1BD0:	00	35	72	0E	00	33	00	00	08	09	08	00	08	00	25	09	.5r..3.....%.
18C5 1BE0:	06	70	6C	61	63	65	3A	74	79	70	65	3D	33	26	73	6F	.place?type=3&so
18C5 1BF0:	72	74	3D	34	64	4E	4B	44	51	6B	38	65	68	63	6A	35	rt=4dNKDQk8ehcj5

Figure 56: Examination of RAM (1)

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
0178 2820:	20	31	37	34	38	20	49	4E	46	4F	20	20	20	20	42	6F	1748 INFO Bo
0178 2830:	78	45	78	65	63	75	74	6F	72	2D	31	36	20	20	20	20	xExecutor-16
0178 2840:	20	20	20	6C	6F	63	61	6C	5F	66	73	5F	73	79	6E	63	local_fs_sync
0178 2850:	5F	61	70	69	20	20	20	20	20	4D	6F	76	69	6E	67	20	_api Moving
0178 2860:	74	65	6D	70	20	66	69	6C	65	20	63	3A	5C	75	73	65	temp file c:\use
0178 2870:	72	73	5C	66	6F	72	65	6E	73	7E	31	5C	61	70	70	64	rs\forens~1\appd
0178 2880:	61	74	61	5C	6C	6F	63	61	6C	5C	74	65	6D	70	5C	74	ata\local\temp\t
0178 2890:	6D	70	76	66	64	6F	63	7A	20	74	6F	20	66	69	6E	61	mpvfdocz to fina
0178 28A0:	6C	20	64	65	73	74	69	6E	61	74	69	6F	6E	20	5C	5C	l destination \\
0178 28B0:	3F	5C	43	3A	5C	55	73	65	72	73	5C	46	6F	72	65	6E	?\C:\Users\Foren
0178 28C0:	73	69	63	5F	54	65	73	74	65	72	5C	42	6F	78	20	53	sic_Tester\Box S
0178 28D0:	79	6E	63	5C	30	31	39	31	39	32	2E	6A	70	67	1B	5B	ync\019192.jpg.[
0178 28E0:	30	6D	0D	0A	1B	5B	33	32	6D	32	30	31	36	2D	31	32	Im...[32m2016-12
0178 28F0:	2D	31	38	20	30	37	3A	32	35	3A	31	30	2E	32	38	32	-18 07:25:10.282
0178 2900:	20	31	37	34	38	20	44	45	42	55	47	20	20	20	42	6F	1748 DEBUG Bo
0178 2910:	78	45	78	65	63	75	74	6F	72	2D	31	36	20	20	20	20	xExecutor-16
0178 2920:	20	20	20	6C	6F	63	61	6C	5F	66	73	5F	73	79	6E	63	local_fs_sync
0178 2930:	5F	61	70	69	20	20	20	20	20	41	74	74	65	6D	70	74	_api Attempt
0178 2940:	69	6E	67	20	74	6F	20	73	65	74	20	74	69	6D	65	73	ing to set times
0178 2950:	74	61	6D	70	73	20	6F	66	20	5C	5C	3F	5C	43	3A	5C	tamps of \\?\C:\
0178 2960:	55	73	65	72	73	5C	46	6F	72	65	6E	73	69	63	5F	54	Users\Forensic_I
0178 2970:	65	73	74	65	72	5C	42	6F	78	20	53	79	6E	63	5C	30	ester\Box Sync\0
0178 2980:	31	39	31	39	32	2E	6A	70	67	20	74	6F	20	63	72	65	19192.jpg to cre
0178 2990:	61	74	65	64	5F	61	74	3D	39	35	35	35	34	35	36	35	ated_at=95554565
0178 29A0:	34	20	61	6E	64	20	75	70	64	61	74	65	64	5F	61	74	4 and updated_at
0178 29B0:	3D	39	35	35	35	34	35	36	35	34	1B	5B	30	6D	0D	0A	=955545654.[0m..
0178 29C0:	1B	5B	33	36	6D	32	30	31	36	2D	31	32	2D	31	38	20	.[36m2016-12-18
0178 29D0:	30	37	3A	32	35	3A	31	30	2E	32	38	32	20	31	37	34	07:25:10.282 174
0178 29E0:	38	20	49	4E	46	4F	20	20	20	20	42	6F	78	45	78	65	8 INFO Bo
0178 29F0:	63	75	74	6F	72	2D	31	36	20	20	20	20	20	20	20	66	Executor-16 f
0178 2A00:	73	5F	6D	6F	6E	69	74	6F	72	20	20	20	20	20	20	20	s_monitor
0178 2A10:	20	20	20	20	20	63	72	65	61	74	69	6E	67	20	6E	61	creating na
0178 2A20:	74	69	76	65	5F	73	74	61	74	65	20	66	6F	72	20	69	tive_state for i
0178 2A30:	64	3A	20	3C	4C	6F	63	61	6C	4E	61	74	69	76	65	53	d: <LocalNativeS
0178 2A40:	74	61	74	65	20	6E	61	74	69	76	65	5F	69	64	3A	20	tate native_id:
0178 2A50:	4C	6F	63	61	6C	4E	61	74	69	76	65	49	44	57	69	74	LocalNativeIDwit
0178 2A60:	68	43	72	65	61	74	69	6F	6E	54	69	6D	65	53	74	61	hCreationTimeSta
0178 2A70:	6D	70	28	69	6E	6F	64	65	3D	32	32	35	31	37	39	39	mp(inode=2251799

Figure 57: Examination of RAM (2)

Also we managed to successfully discover the contents of the uploaded files and the related metadata (as we can see in Figure 58, Figure 59 and Figure 60).

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	01	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
OE0A E000:	46	2D	31	2E	34	0A	00	00	3C	3C	0A	2F	54	79	70	65	F-1.4...<<	/Type														
OE0A E010:	20	2F	43	61	74	61	6C	6F	67	0A	2F	50	61	67	65	73	/Catalog.	Pages														
OE0A E020:	20	25	64	20	30	20	52	0A	3E	3E	0A	65	6E	64	6F	62	%d 0 R.>>.endobj															
OE0A E030:	6A	0A	00	00	00	00	00	00	3C	3C	0A	2F	54	79	70	65	j.....<<./Type															
OE0A E040:	20	2F	45	78	74	47	53	74	61	74	65	0A	2F	53	41	20	/ExtGState./SA															
OE0A E050:	74	72	75	65	0A	2F	53	4D	20	30	2E	30	32	0A	2F	63	true./SM 0.02./c															
OE0A E060:	61	20	31	2E	30	0A	2F	43	41	20	31	2E	30	0A	2F	41	a 1.0./CA 1.0./A															
OE0A E070:	49	53	20	66	61	6C	73	65	0A	2F	53	4D	61	73	6B	20	IS false./SMask															
OE0A E080:	2F	4E	6F	6E	65	3E	3E	0A	65	6E	64	6F	62	6A	0A	00	/None>>.endobj..															
OE0A E090:	5B	2F	50	61	74	74	65	72	6E	20	2F	44	65	76	69	63	[/Pattern /Devic															
OE0A E0A0:	65	52	47	42	5D	0A	65	6E	64	6F	62	6A	0A	00	00	00	eRGB].endobj....															
OE0A E0B0:	3C	3C	0A	2F	54	69	74	6C	65	20	00	00	0A	2F	43	72	<<./Title .../Cr															
OE0A E0C0:	65	61	74	6F	72	20	00	00	0A	2F	50	72	6F	64	75	63	erator .../Produc															
OE0A E0D0:	65	72	20	00	51	74	20	35	2E	37	2E	30	00	00	00	00	er 0t 5 7 0															
OE0A E0E0:	0A	2F	43	72	65	61	74	69	6F	6E	44	61	74	65	20	28	./CreationDate (
OE0A E0F0:	44	3A	25	64	25	30	32	64	25	30	32	64	25	30	32	64	D:%a%uza%uza%uza															
OE0A E100:	25	30	32	64	25	30	32	64	29	0A	00	00	3E	3E	0A	65	%02d%02d)...>>.e															
OE0A E110:	6E	64	6F	62	6A	0A	00	00	3C	3C	0A	2F	54	79	70	65	ndobj...<<./Type															
OE0A E120:	20	2F	50	61	67	65	73	0A	2F	4B	69	64	73	20	0A	5B	/Pages./Kids [.]															
OE0A E130:	0A	00	00	00	25	64	20	30	20	52	0A	00	2F	43	6F	75%d 0 R.../Cou															
OE0A E140:	6E	74	20	25	64	0A	00	00	2F	50	72	6F	63	53	65	74	nt %d.../ProcSet															
OE0A E150:	20	5B	2F	50	44	46	20	2F	54	65	78	74	20	2F	49	6D	[/PDF /Text /Im															
OE0A E160:	61	67	65	42	20	2F	49	6D	61	67	65	43	5D	0A	3E	3E	ageB /ImageC].>>															
OE0A E170:	0A	65	6E	64	6F	62	6A	0A	00	00	00	00	3C	3C	20	2F	.endobj.....<< /															
OE0A E180:	54	79	70	65	20	2F	46	6F	6E	74	44	65	73	63	72	69	Type /FontDescri															
OE0A E190:	70	74	6F	72	0A	2F	46	6F	6E	74	4E	61	6D	65	20	2F	ptor./FontName /															
OE0A E1A0:	51	00	00	00	0A	2F	46	6C	61	67	73	20	00	00	00	00	Q..../Flags															
OE0A E1B0:	0A	2F	46	6F	6E	74	42	42	6F	78	20	5B	00	00	00	00	./FontBBox [....															
OE0A E1C0:	5D	0A	2F	49	74	61	6C	69	63	41	6E	67	6C	65	20	00]./ItalicAngle .															
OE0A E1D0:	0A	2F	41	73	63	65	6E	74	20	00	00	00	0A	2F	44	65	./Ascent/De															
OE0A E1E0:	73	63	65	6E	74	20	00	00	0A	2F	43	61	70	48	65	69	scent .../CapHei															
OE0A E1F0:	67	68	74	20	00	00	00	00	0A	2F	53	74	65	6D	56	20	ght/StemV															
OE0A E200:	00	00	00	00	0A	2F	46	6F	6E	74	46	69	6C	65	32	20/FontFile2															
OE0A E210:	00	00	00	00	30	20	52	0A	3E	3E	20	65	6E	64	6F	620 R.>> endobj															
OE0A E220:	6A	0A	00	00	3C	3C	0A	2F	4C	65	6E	67	74	68	31	20	j...<<./Length1															
OE0A E230:	00	00	00	00	0A	2F	4C	65	6E	67	74	68	20	00	00	00/Length ...															
OE0A E240:	30	20	52	0A	00	00	00	00	2F	46	69	6C	74	65	72	20	0 R..../Filter															
OE0A E250:	2F	46	6C	61	74	65	44	65	63	6F	64	65	0A	00	00	00	/FlateDecode....															
OE0A E260:	3E	3E	0A	73	74	72	65	61	6D	0A	00	00	65	6E	64	73	>>.stream...ends															
OE0A E270:	74	72	65	61	6D	0A	65	6E	64	6F	62	6A	0A	00	00	00	ream.endobj....															
OE0A E280:	25	64	0A	65	6E	64	6F	62	6A	0A	00	00	3C	3C	20	2F	%d.endobj...<< /															
OE0A E290:	54	79	70	65	20	2F	46	6F	6E	74	0A	2F	53	75	62	74	Type /Font./Subt															
OE0A E2A0:	79	70	65	20	2F	43	49	44	46	6F	6E	74	54	79	70	65	ype /CIDFontType															

Figure 58: Discovery of files' metadata

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
01EA 5F70:	00	00	00	00	5C	D4	B3	68	00	00	00	00	00	00	00	00\..h.....
01EA 5F80:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00\..h.....
01EA 5F90:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00\..h.....
01EA 5FA0:	00	00	00	00	00	00	00	00	00	00	00	00	FF	FF	FF	FF\..h.....
01EA 5FB0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00\..h.....
01EA 5FC0:	00	00	00	00	00	00	00	00	B4	17	B3	68	54	E9	B3	68hT..h
01EA 5FD0:	00	00	00	00	5C	D4	B3	68	00	00	00	00	00	00	00	00\..h.....
01EA 5FE0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00\..h.....
01EA 5FF0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00\..h.....
01EA 6000:	0D	0A	20	20	20	44	4F	4E	41	4C	44	20	43	2E	20	42	.. DONALD C. B
01EA 6010:	52	4F	43	4B	45	54	54	2C	20	41	50	50	45	4C	4C	41	ROCKETT, APPELLA
01EA 6020:	4E	54	20	56	2E	20	53	50	4F	4B	41	4E	45	20	41	52	NT V. SPOKANE AR
01EA 6030:	43	41	44	45	53	2C	20	49	4E	43	2E	2C	20	45	54	20	CADES, INC., ET
01EA 6040:	41	4C	2E	0D	0A	4B	45	4E	4E	45	54	48	20	45	49	4B	AL...KENNETH EIK
01EA 6050:	45	4E	42	45	52	52	59	2C	20	41	54	54	4F	52	4E	45	ENBERRY, ATTORNE
01EA 6060:	59	20	47	45	4E	45	52	41	4C	20	4F	46	20	57	41	53	Y GENERAL OF WAS
01EA 6070:	48	49	4E	47	54	4F	4E	2C	20	45	54	20	41	4C	2E	2C	HINGTON, ET AL.,
01EA 6080:	20	41	50	50	45	4C	4C	41	4E	54	53	0D	0A	56	2E	20	APPELLANTS..V.
01EA 6090:	4A	2D	52	20	44	49	53	54	52	49	42	55	54	4F	52	53	J-R DISTRIBUTORS
01EA 60A0:	2C	20	49	4E	43	2E	2C	20	45	54	20	41	4C	2E	0D	0A	, INC., ET AL...
01EA 60B0:	0D	0A	20	20	20	4E	6F	2E	20	38	34	2D	32	38	2C	20	.. No. 84-28,
01EA 60C0:	4E	6F	2E	20	38	34	2D	31	34	33	0D	0A	0D	0A	20	20	No. 84-143....
01EA 60D0:	20	49	6E	20	74	68	65	20	53	75	70	72	65	6D	65	20	In the Supreme
01EA 60E0:	43	6F	75	72	74	20	6F	66	20	74	68	65	20	55	6E	69	Court of the Un
01EA 60F0:	74	65	64	20	53	74	61	74	65	73	0D	0A	0D	0A	20	20	ted States....
01EA 6100:	20	4F	43	54	4F	42	45	52	20	54	45	52	4D	2C	20	31	OCTOBER TERM, 1
01EA 6110:	39	38	34	0D	0A	0D	0A	20	20	20	4F	6E	20	41	70	70	984.... On App
01EA 6120:	65	61	6C	73	20	66	72	6F	6D	20	74	68	65	20	55	6E	eals from the Un
01EA 6130:	69	74	65	64	20	53	74	61	74	65	73	20	43	6F	75	72	ited States Cour
01EA 6140:	74	20	6F	66	20	41	70	70	65	61	6C	73	20	66	6F	72	t of Appeals for
01EA 6150:	20	74	68	65	20	4E	69	6E	74	68	0D	0A	43	69	72	63	the Ninth..Circ
01EA 6160:	75	69	74	0D	0A	0D	0A	20	20	20	42	72	69	65	66	20	uit.... Brief
01EA 6170:	66	6F	72	20	74	68	65	20	55	6E	69	74	65	64	20	53	for the United S
01EA 6180:	74	61	74	65	73	20	61	73	20	41	6D	69	63	75	73	20	tates as Amicus
01EA 6190:	43	75	72	69	61	65	20	53	75	70	70	6F	72	74	69	6E	Curiae Supportin
01EA 61A0:	67	20	41	70	70	65	6C	6C	61	6E	74	73	0D	0A	0D	0A	g Appellants....
01EA 61B0:	20	20	20	20	20	20	20	20	20	20	20	20	54	41	42	4C	TABL
01EA 61C0:	45	20	4F	46	20	43	4F	4E	54	45	4E	54	53	0D	0A	20	E OF CONTENTS..
01EA 61D0:	20	20	49	6E	74	65	72	65	73	74	20	6F	66	20	74	68	Interest of th
01EA 61E0:	65	20	55	6E	69	74	65	64	20	53	74	61	74	65	73	0D	e United States.
01EA 61F0:	0A	20	20	20	53	74	61	74	65	6D	65	6E	74	0D	0A	20	. Statement..
01EA 6200:	20	20	53	75	6D	6D	61	72	79	20	6F	66	20	74	68	65	Summary of the
01EA 6210:	20	61	72	67	75	6D	65	6E	74	0D	0A	20	20	20	41	72	argument.. Ar
01EA 6220:	67	75	6D	65	6E	74	0D	0A	20	20	20	20	20	20	54	68	gument.. Th

Figure 59: Discovery of contents (1)

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
075 OCA0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
075 OCB0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
075 OCC0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
075 OCD0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
075 OCE0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
075 OCF0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
075 OD00:	00	00	00	00	49	4E	54	45	47	52	41	54	45	44	20	43 INTEGRATED C
075 OD10:	4F	4E	54	52	4F	4C	20	53	59	53	54	45	4D	0D	0A	4D	ONTROL SYSTEM..M
075 OD20:	61	72	63	68	00	00	00	01	20	32	30	30	31	0D	0A	11	arch.... 2001...
075 OD30:	00	49	2E	20	20	53	65	6E	69	6F	72	20	74	65	61	6D	.I. Senior team
075 OD40:	20	6C	65	61	64	65	72	20	61	28	A8	42	00	73	73	65	leader a(.B.sse
075 OD50:	73	73	6D	65	6E	74	51	05	09	54	68	65	55	06	54	51	ssmentQ..TheU.TQ
075 OD60:	06	4C	53	06	41	56	06	20	69	73	20	66	40	0E	74	50	.LS.AV. is f@tP
075 OD70:	09	6D	6F	6E	00	40	80	02	74	68	20	6F	66	20	62	2C	.mon@..th of b,
075 OD80:	2C	62	2D	20	6F	6E	6C	79	2E	20	54	40	0F	66	75	6C	,b- only. T@ful
075 OD90:	6C	20	6E	61	72	72	61	74	69	76	65	00	14	00	08	20	l narrative....
075 ODA0:	77	68	69	70	11	66	6F	6C	6C	6F	77	73	20	63	6F	76	whip.follows cov
075 ODB0:	65	72	73	67	07	73	61	08	46	65	62	72	75	61	72	79	ersg.sa.February
075 ODC0:	20	61	08	01	02	28	6E	64	69	15	2E	71	1C	54	65	63	a... (ndi..g.Tec
075 ODD0:	68	6E	69	63	61	6C	42	0E	70	72	6F	67	72	61	6D	6D	hnicalB.programm
075 ODE0:	60	1C	63	20	50	72	30	05	65	73	73	80	20	14	80	42	`c Pr0.ess. ...B
075 ODF0:	0A	41	63	63	6F	6D	70	6C	69	73	68	71	30	73	51	1B	.Accomplishq0sQ.
075 OEO0:	49	6E	74	65	50	0E	74	65	64	20	43	60	2D	72	6F	6C	InteP.ted C`-rol
075 OE10:	20	53	79	73	04	00	40	04	74	65	6D	73	20	41	0F	43	Sys..@.tems.A.C
075 OE20:	68	72	70	56	54	72	65	6D	65	6C	20	68	61	73	20	62	hrpVlremel has b
075 OE30:	65	65	6E	20	61	64	64	50	10	74	6F	2C	48	0C	87	72	een addP.to,H.r
075 OE40:	24	4C	41	4E	4C	70	34	52	1C	70	36	81	1B	50	08	61	\$LANLp4R.p6..P.a
075 OE50:	20	50	6F	73	74	20	60	1B	64	75	60	1E	20	73	74	75	Post `du`. stu
075 OE60:	64	60	34	2C	72	08	63	16	41	6C	01	04	50	74	6C	60	d`4,r.c.Al..Pt1`
075 OE70:	0C	61	15	72	16	65	71	04	61	6C	6C	71	6E	68	40	0F	.a.r.eq.allqnh@.
075 OE80:	69	6E	74	65	72	76	69	65	77	60	0D	6E	64	20	73	68	interview`.nd sh
075 OE90:	6F	75	6C	64	70	00	08	40	0C	80	80	47	20	62	6F	61	ouldp..@...G boa
075 OEA0:	72	64	20	6E	65	78	74	83	23	80	06	50	65	72	70	49	rd next.#..PerpI
075 OEB0:	69	6E	65	20	4D	63	47	65	68	65	80	56	69	6C	6C	01	ine McGehe.Vill.
075 OEC0:	02	50	00	20	74	72	61	6E	73	66	65	72	61	0F	6F	77	.P. transfera.ow
075 OED0:	30	53	4E	53	20	64	69	76	69	73	69	60	0E	61	6E	64	OSNS divisi`.and
075 OEE0:	20	77	6F	72	6B	50	12	01	E1	40	81	80	B5	75	73	20	workP...@...us
075 OEF0:	37	35	25	80	8E	72	52	0F	72	65	6D	61	69	6E	81	EA	75%..rR.remain..
075 OF00:	70	18	41	01	79	65	61	72	61	30	61	72	74	69	63	69	p.A.yeara0artici
075 OF10:	70	70	5D	18	00	C0	70	64	60	1D	42	0B	80	42	76	65	pp]...pd`.B..Bve
075 OF20:	6E	74	60	14	80	8B	46	61	63	69	6C	69	74	69	65	73	nt`...Facilities
075 OF30:	20	64	65	73	69	67	6E	60	0B	74	4F	74	20	53	98	0D	design`.tOt S..
075 OF40:	00	08	61	6E	20	46	70	1B	63	69	73	63	6F	20	74	6F	..an Fp.cisco to
075 OF50:	20	65	6E	73	75	72	65	60	06	40	0D	63	70	53	80	4D	ensure`.@.cpS.M
075 OF60:	20	73	82	89	50	17	71	75	69	A0	06	0E	F1	70	07	60	s..P.qui....p.`
075 OF70:	1A	50	1C	50	05	6D	65	74	90	B2	00	50	72	65	70	30	P P met Press0

Figure 60: Discovery of file contents (2)

Finally, we could not find any information regarding the size and the hash values of the files that we transferred.

Download (Examination of RAM)

By examining the RAM, we discovered the name of the files that we downloaded, and the folder in which we stored them (Figure 61).

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
1017 51A0:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5
1017 51B0:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5
1017 51C0:	01	00	00	00	00	00	00	00	01	00	00	00	00	00	00	00
1017 51D0:	38	CC	CA	14	48	00	00	00	00	00	00	00	03	E5	E5	E5	8...H.....
1017 51E0:	A0	CF	C9	0B	31	E4	E5	E5	00	00	00	00	00	00	00	00	...1.....
1017 51F0:	00	00	00	00	00	00	00	00	00	01	E5	E5	E5	E5	E5	E5
1017 5200:	02	00	00	00	A8	AC	65	13	4D	00	00	00	05	00	01	00e.M.....
1017 5210:	3F	00	00	00	18	C2	9A	0E	6D	6F	7A	2D	69	63	6F	6E	?.....moz-icon
1017 5220:	3A	2F	2F	43	3A	5C	55	73	65	72	73	5C	46	6F	72	65	://C:\Users\Fore
1017 5230:	6E	73	69	63	5F	54	65	73	74	65	72	5C	44	6F	77	6E	nsic_Tester\Down
1017 5240:	6C	6F	61	64	73	5C	30	31	39	31	39	32	2E	6A	70	67	loads\019192.jpg
1017 5250:	3F	73	69	7A	65	3D	00	E5	6C	C2	9A	0E	08	00	00	00	?size=.1.....
1017 5260:	11	00	01	00	3F	00	00	00	6C	C2	9A	0E	6D	6F	7A	2D?...1...moz-
1017 5270:	69	63	6F	6E	00	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	icon.....
1017 5280:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5
1017 5290:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5
1017 52A0:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	BC	36	E3	5F6_
1017 52B0:	00	00	00	00	01	00	01	00	3F	00	00	00	C0	C2	9A	0E?
1017 52C0:	00	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5
1017 52D0:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5
1017 52E0:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5

Figure 61: Examination of RAM (3)

7.7.2 Use of Google Chrome

In this scenario we will use the Google Chrome browser. We navigate in folder “C:\Users\Forensic_Tester\AppData\Local\Google\Chrome\User Data\Default”, where the History and Cookies databases are located.

By studying the browser files, we discover entries that confirm our visit in Box’s website (History, Cookies). However, we were unable to discover any other information (Figure 62 and Figure 63).

id	url	title	visit_co...	typed_...	last_visit_time	hidden	favicon_id
78	https://account.box.com/login/?error=default&redirect_url=%2F&login=kaada87...	Box Simple Onli...	2	0	1312533052438...	0	0
77	https://account.box.com/login?redirect_url=%2F	All Files Powere...	3	0	1312533053224...	0	0
80	https://app.box.com/	All Files Powere...	5	0	1312657923013...	0	0
81	https://app.box.com/folder/0	All Files Powere...	6	0	1312658015441...	0	0
82	https://app.box.com/folders/sync/0	Synced to Deskt...	3	0	1312533059057...	0	0
84	https://app.box.com/login	Box Simple Onli...	2	0	1312657918551...	0	0
88	https://app.box.com/login/?error=default&redirect_url=%2F&login=kaada87%40h...	Box Simple Onli...	2	0	1312657921713...	0	0
79	https://app.box.com/login/assertion?a=IacLiveV1%21cEgqby2jeZ_1z0YM160ub...	All Files Powere...	1	0	1312533053224...	0	0
87	https://app.box.com/login?redirect_url=%2F	All Files Powere...	3	0	1312657923013...	0	0
85	https://app.box.com/settings/sync	Box Simple Onli...	1	0	1312533059495...	0	0
15	https://el-gr.facebook.com/	(2) Facebook	2	0	1312499230867...	0	0
32	https://elearn.ihu.edu.gr/		1	0	1312499276218...	0	0

Figure 62: Examination of Google Chrome’s History database

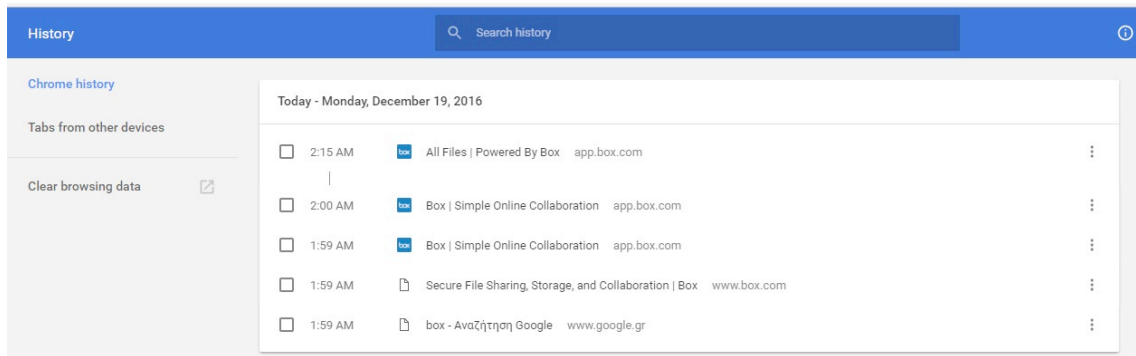


Figure 63: Examination of Google Chrome's History

The examination of RAM led us to the discovery of evidence that confirm the use of Box cloud storage service, the name of the files and the time and date when we uploaded them. Also we managed to successfully discover the contents of the uploaded files and the related to them metadata. Finally, we found information regarding their size and hash values (we can see all these in the following figures, Figure 64, Figure 65 and Figure 66).

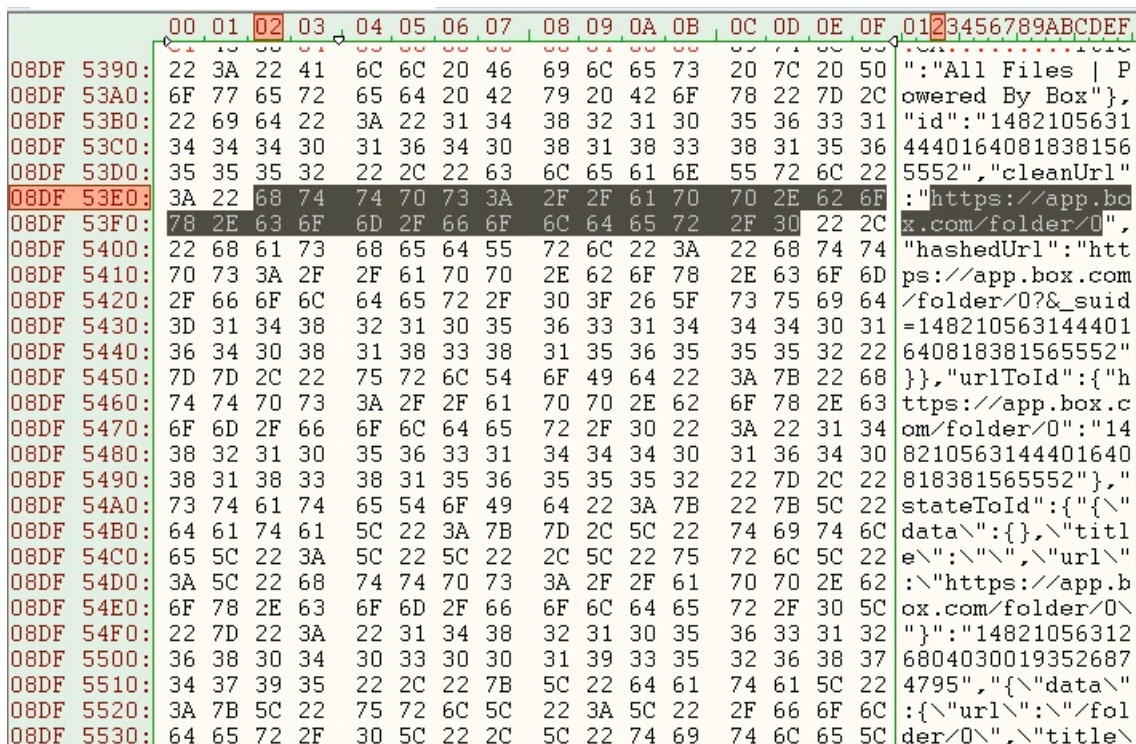


Figure 64: Examination of RAM (1)

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
0118 4060:	4C	29	5D	1B	5B	30	6D	0D	0A	1B	5B	33	36	6D	32	30	L)].[0m...[36m20
0118 4070:	31	36	2D	31	32	2D	31	39	20	30	32	3A	31	35	3A	33	16-12-19 02:15:3
0118 4080:	39	2E	34	31	38	20	31	37	38	34	20	49	4E	46	4F	20	9.418 1784 INFO
0118 4090:	20	20	20	42	6F	78	45	78	65	63	75	74	6F	72	2D	39	BoxExecutor-9
0118 40A0:	20	20	20	20	20	20	20	20	6C	6F	63	61	6C	5F	66	73	local_fs
0118 40B0:	5F	73	79	6E	63	5F	61	70	69	20	20	20	20	20	44	65	_sync_api De
0118 40C0:	6C	65	74	65	20	69	74	65	6D	20	6F	6E	20	6C	6F	63	lete item on loc
0118 40D0:	61	6C	2E	20	20	70	61	74	68	3D	30	31	39	31	39	32	al. path=019192
0118 40E0:	2E	6A	70	67	2E	20	20	69	74	65	6D	5F	74	79	70	65	.jpg. item_type
0118 40F0:	3D	30	2E	20	20	6F	6C	64	5F	69	74	65	6D	5F	73	74	=0. old_item_st
0118 4100:	61	74	65	3D	4C	6F	63	61	6C	49	74	65	6D	53	74	61	ate=LocalItemSta
0118 4110:	74	65	2C	20	69	74	65	6D	5F	69	64	3A	20	34	30	2C	te, item_id: 40,
0118 4120:	20	69	74	65	6D	5F	74	79	70	65	3A	20	30	2C	20	70	item_type: 0, p
0118 4130:	61	72	65	6E	74	5F	69	74	65	6D	5F	69	64	3A	20	30	arent item id: 0
0118 4140:	2C	20	6E	61	6D	65	3A	20	30	31	39	31	39	32	2E	6A	, name: 019192.j
0118 4150:	70	67	2C	20	73	69	7A	65	3A	20	36	32	32	30	36	2C	pg, size: 62206,

Figure 65: Examination of RAM (2)

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
06B9 1850:	74	72	61	73	68	65	64	27	2C	20	75	27	63	6F	6E	74	trashed', u'cont
06B9 1860:	65	6E	74	5F	63	72	65	61	74	65	64	5F	61	74	27	3A	ent_created_at':
06B9 1870:	20	75	27	32	30	30	30	2D	30	34	2D	31	32	54	30	36	u'2000-04-12T06
06B9 1880:	3A	32	30	3A	35	34	2D	30	37	3A	30	30	27	2C	20	75	:20:54-07:00', u
06B9 1890:	27	69	64	27	3A	20	75	27	31	31	32	39	39	33	32	30	'id': u'11299320
06B9 18A0:	37	37	33	31	27	2C	20	75	27	73	69	7A	65	27	3A	20	7731', u'size':
06B9 18B0:	36	32	32	30	36	2C	20	75	27	6D	6F	64	69	66	69	65	62206, u'modifie
06B9 18C0:	64	5F	62	79	27	3A	20	7B	75	27	6C	6F	67	69	6E	27	d_by': {u'login'
06B9 18D0:	3A	20	75	27	6B	61	61	64	61	64	38	37	40	68	6F	74	: u'██████████@hot
06B9 18E0:	6D	61	69	6C	2E	63	6F	6D	27	2C	20	75	27	74	79	70	mail.com', u'typ
06B9 18F0:	65	27	3A	20	75	27	75	73	65	72	27	2C	20	75	27	69	e': u'user', u'i
06B9 1900:	64	27	3A	20	75	27	35	37	35	39	30	35	31	31	31	27	d': u'575905111'
06B9 1910:	2C	20	75	27	6E	61	6D	65	27	3A	20	75	27	41	6E	64	, u'name': u'And
06B9 1920:	72	65	61	73	20	50	61	74	73	61	72	69	6B	61	73	27	reas Patsarikas'
06B9 1930:	7D	2C	20	75	27	66	69	6C	65	5F	76	65	72	73	69	6F	}, u'file_versio
06B9 1940:	6E	27	3A	20	7B	75	27	73	68	61	31	27	3A	20	75	27	n': {u'sha1': u'
06B9 1950:	32	37	35	38	30	30	34	61	33	30	30	61	64	30	39	62	2758004a300ad09b
06B9 1960:	39	33	34	34	64	39	63	62	35	33	30	63	66	62	32	61	9344d9cb530cfb2a
06B9 1970:	39	65	33	32	37	62	33	65	27	2C	20	75	27	74	79	70	9e327b3e', u'tvp
06B9 1980:	65	27	3A	20	75	27	66	69	6C	65	5F	76	65	72	73	69	e': u'file_versi
06B9 1990:	6F	6E	27	2C	20	75	27	69	64	27	3A	20	75	27	31	32	on', u'id': u'12
06B9 19A0:	31	33	39	34	32	37	33	34	35	39	27	7D	2C	20	75	27	1394273459'}, u'

Figure 66: Examination of RAM (3)

Download (Examination of RAM)

By examining the RAM, we discovered the name of the files that we downloaded, and the folder in which we stored them (Figure 67).

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
1017 51A0:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5
1017 51B0:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5
1017 51C0:	01	00	00	00	00	00	00	00	01	00	00	00	00	00	00	00
1017 51D0:	38	CC	CA	14	48	00	00	00	00	00	00	00	03	E5	E5	E5	8...H.....
1017 51E0:	A0	CF	C9	0B	31	E4	E5	E5	00	00	00	00	00	00	00	00	...1.....
1017 51F0:	00	00	00	00	00	00	00	00	00	01	E5	E5	E5	E5	E5	E5e.M.....
1017 5200:	02	00	00	00	A8	AC	65	13	4D	00	00	00	05	00	01	00moz-icon
1017 5210:	3F	00	00	00	18	C2	9A	0E	6D	6F	7A	2D	69	63	6F	6E	?.....moz-icon
1017 5220:	3A	2F	2F	43	3A	50	55	73	65	72	73	5C	46	6F	72	65	://C:\Users\Fore
1017 5230:	6E	73	69	63	5F	54	65	73	74	65	72	5C	44	6F	77	6E	nsic_Tester\Down
1017 5240:	6C	6F	61	64	73	5C	30	31	39	31	39	32	2E	6A	70	67	loads\019192.jpg
1017 5250:	3F	73	69	7A	65	3D	00	E5	6C	C2	9A	0E	08	00	00	00	?size=...l.....
1017 5260:	11	00	01	00	3F	00	00	00	6C	C2	9A	0E	6D	6F	7A	2D	...?...l...moz-
1017 5270:	69	63	6F	6E	00	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	icon.....
1017 5280:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5
1017 5290:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5
1017 52A0:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	BC	36	E3	5F6..
1017 52B0:	00	00	00	00	01	00	01	00	3F	00	00	00	C0	C2	9A	0E?.....
1017 52C0:	00	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5
1017 52D0:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5
1017 52E0:	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5	E5

Figure 67: Examination of RAM (4)

7.7.3 Conclusions

In the following table (Table 21) we summarize the findings from our access to Box cloud storage service through two browsers.

Table 21: Accessing Box through browser

Browser	Findings
Mozilla Firefox <ul style="list-style-type: none"> History Cookies RAM 	Proved our access to Box cloud storage service, when we last visited the site and how many times. <i>Upload</i> <ul style="list-style-type: none"> discovered the name and type of the files that we uploaded discovered the time and date when we uploaded them discovered the contents of the uploaded files and the related to them metadata <i>Download</i> <ul style="list-style-type: none"> discovered the name of the files and the folder in which we stored

	them
<p>Google Chrome</p> <ul style="list-style-type: none"> • History • Cookies • RAM 	<p>Proved our access to Box cloud storage service, when we last visited the site and how many times.</p> <p><i>Upload</i></p> <ul style="list-style-type: none"> • discovered the name and type of the files that we uploaded • discovered the time and date when we uploaded them • discovered their size and hash values • discovered the contents of the uploaded files and the related to them metadata <p><i>Download</i></p> <ul style="list-style-type: none"> • discovered the name of the files and the folder in which we stored them

7.8 Metadata

7.8.1 Use of Box's Application Software

In this scenario we downloaded the investigated files to our virtual machine, by using Box's application software. As it is shown in the following figure (Figure 68), the variables Date Created and Date Accessed got as a value the time and date that the download got completed. On the contrary the variable Date Modified was not affected.

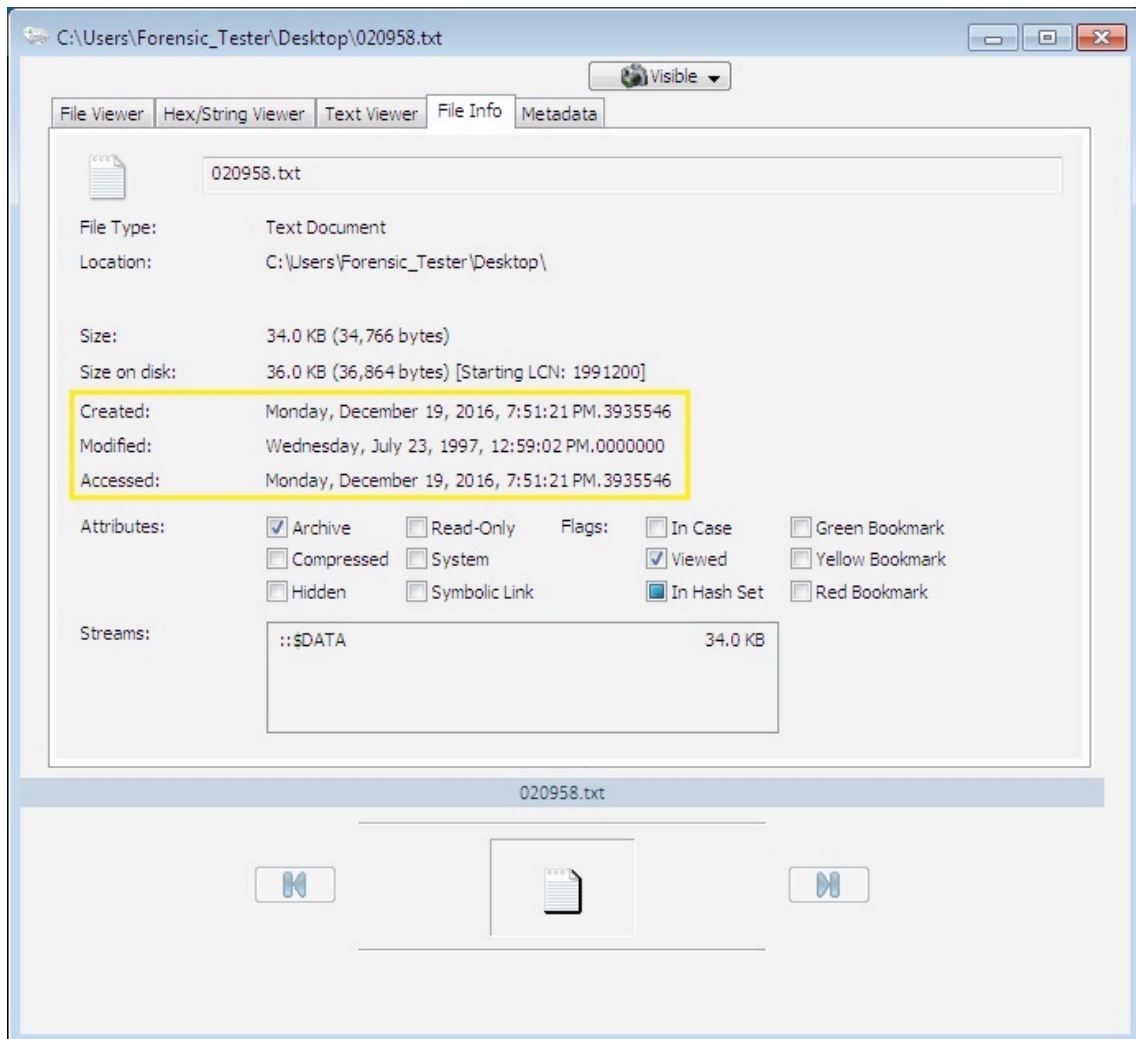


Figure 68: File's metadata through Box's application software

7.8.2 Use of Browser

In this subchapter we examined the alterations that were brought on the files' metadata by the use of Box through a web browser (Mozilla Firefox, Google Chrome).

The variables Date Created, Date Accessed and Date Modified of the files, got as a value the time and date that the download got completed (as we can see in Figure 69).

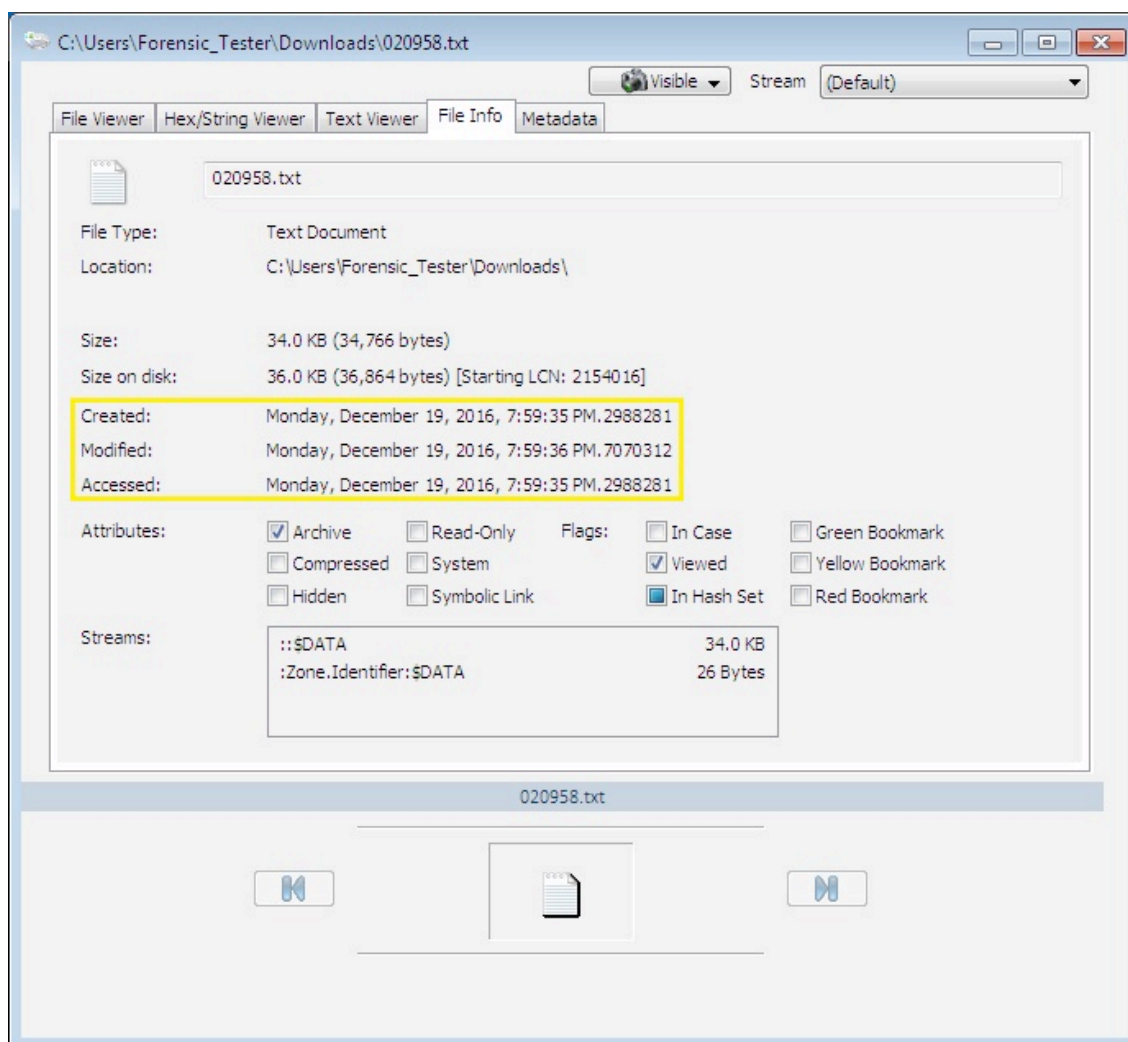


Figure 69: File's metadata through the use of a browser

It is worth noting that in both scenarios the rest metadata of the files were unaffected (Figure 70).

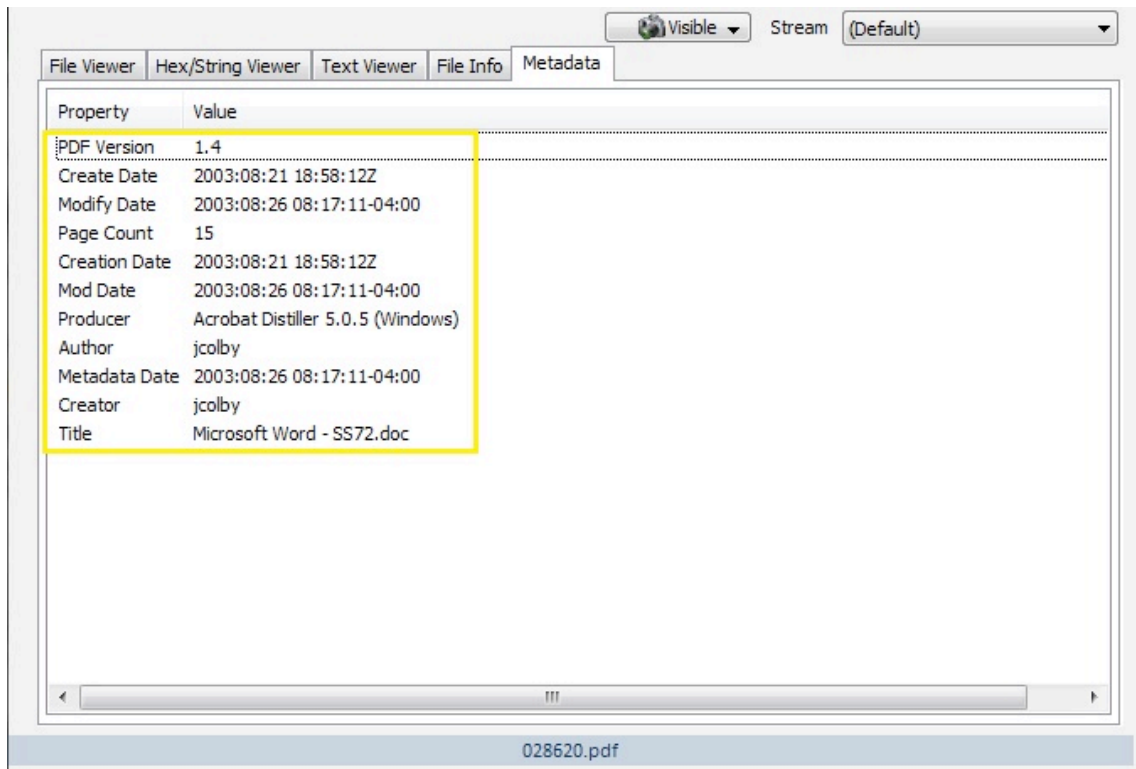


Figure 70: File's metadata

7.9 Deletion

In this subchapter we examine the behavior of the application when we delete the files.

7.9.1 First Scenario of File Deletion

In the first scenario we deleted the files that we have saved locally on our virtual machine, through the application software. The files that we deleted were transferred to the local recycling bin, while our account in Box's server was synchronized through the application software.

By examining the Log files, we discover the files that we deleted, their checksum and the time and date that this action took place (Table 22).

Table 22: Examination of Log files (1)

```
[32m2016-12-19 21:33:59.118 1800 DEBUG LocalExecutor-17
last_sync_item_store persist_updated_item_states: item_existed=True, local_144,
{u'parent_item_id': 0, u'name': u'019192.jpg', u'is_deleted': 1, u'local_id': 41,
u'inode': 2814749767149873L, u'checksum': None, u'native_item_type': 0, u'size':
62206, u'content_created_at': 366285561805L, u'content_updated_at':
366285561805L}
```

```
[32m2016-12-19 21:33:59.118 1800 DEBUG LocalExecutor-17
last_sync_item_store persist_updated_item_states: item_existed=True, box_79,
{u'lock_id': None, u'lock_owner_id': None, u'box_id': u'112993207731',
u'parent_item_id': u'0', u'name': u'019192.jpg', u'checksum':
u'2758004a300ad09b9344d9cb530cfb2a9e327b3e', u'item_type': 0, u'is_deleted': 1,
u'size': 62206, u'owner_id': u'575905111'}
```

Also we discover references to the files we deleted in folder “C:\Users\Forensic_Tester\AppData\Roaming\Box Desktop\UserData” as it is shown in the following figure (Figure 71).

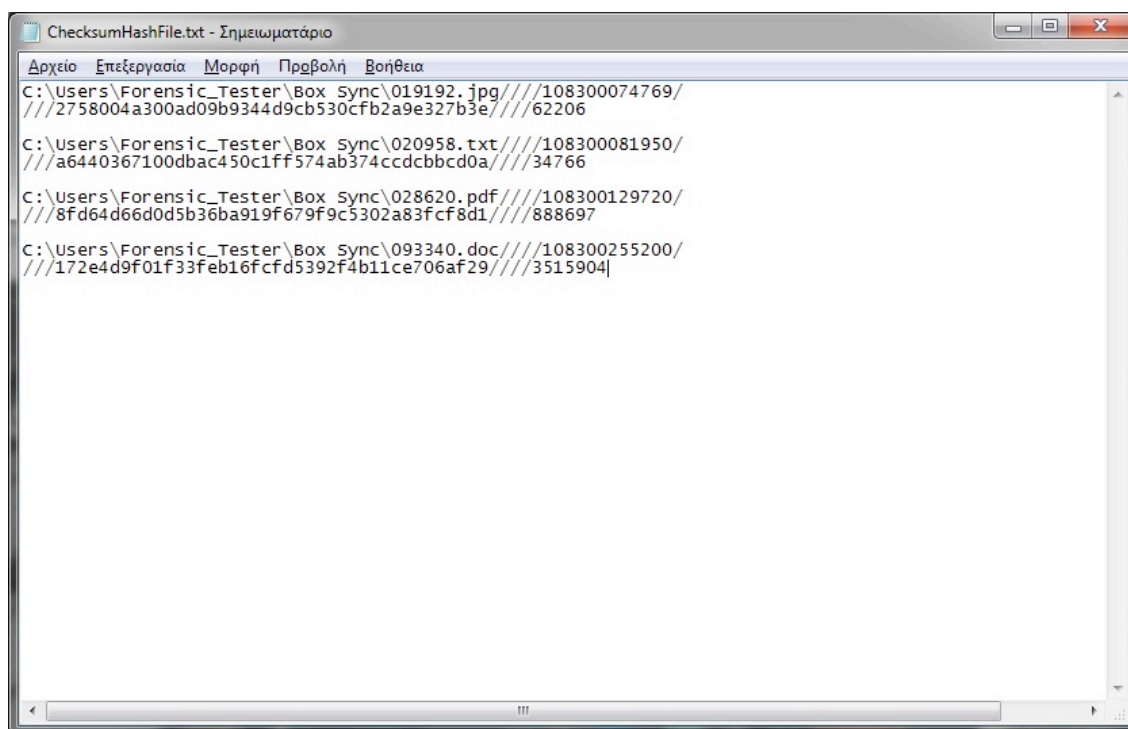


Figure 71: Discovery of the deleted files

7.9.2 Second Scenario of File Deletion

In the second scenario we connect to our account through Box’s application software, by using the virtual machine that we have created. Then, by using another virtual machine, we connect to our Box account -either through a browser or through the applica-

tion software- and delete the files of our choice. This results in the synchronization of our account and the deletion of the files from the application’s software shared folder “Box Sync” of the original virtual machine.

The information that we find are similar to these of the previous scenario, as it is shown from the examination of the log files (Table 23).

Table 23: Examination of Log files (2)

```
[36m2016-12-20 00:06:53.009 1736 INFO BoxFSMonitor fs_monitor
Processing item change TN: _00000008_; new_native_state: (<BoxNativeState
native_id: (u'113253743011', 0); parent_native_id: BoxNativeID(box_id=u'0',
native_item_type=1); name: 093340.doc; item_type: 0; is_deleted: True; checksum:
172e4d9f01f33feb16fcfd5392f4b11ce706af29; lock_state: None; syncability:
SYNCABLE; owner_id: 575905111; size: 3515904>) based on scanned item
_BoxScannedItem(scanned_item_type=u'NEW_STATE', native_id=(u'113253743011',
0), native_state=<box.sync.adapter.box.box_native_state.BoxNativeState object at
0x0D5B5630>, sequence_id=1)
```

7.9.3 File Deletion through Browser

The files that we delete are stored in “Trash” folder, regardless of the browser that we are going to use. We must manually take care of their deletion again from this folder. As it is illustrated in the following figure (Figure 72), we can recover those files within 30 days or else the service will delete them permanently.

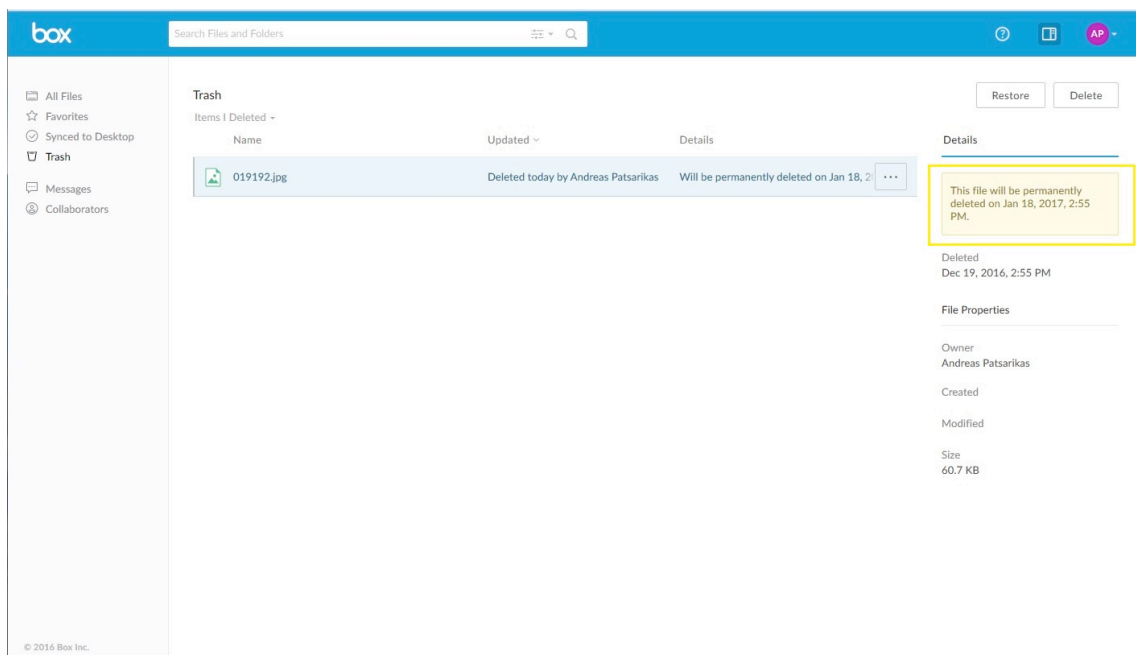


Figure 72: Box’s trash folder

7.10 Box’s Application Software Uninstallation

Lastly, we analyzed the behavior of Box cloud storage service during the uninstallation process, by comparing the signatures of the system.

In the first scenario we uninstalled the program through the Control Panel of the Windows 7 operating system. This way we found a plethora of references to Box’s application software in Window’s registry, while “BoxSync” folder remained intact.

In the second scenario we will use the program CCleaner for the uninstallation of Box’s application software. After uninstalling Box, we used the Registry Scan option to remove from Windows registry any remaining references to Box. In this scenario, we found again references to Box’s application software in Window’s registry, while “BoxSync” folder remained intact.

Finally, in the third scenario we also used Eraser, instead of only using CCleaner. We managed to completely delete “BoxSync” folder, though references to Box continued to exist in Windows registry.

Summing up, after uninstalling Box application software, we can safely say that the investigator is able to discover data which prove its use -in the worst case scenario- or even discover the files that we transferred through Box’s application software.

Table 24: Conclusions from the uninstallation of Box’s application software

Scenario	Findings
1 st Scenario: Normal uninstallation	<ul style="list-style-type: none"> • References to Box in registry • BoxSync folder remained intact
2 nd Scenario: Use of CCleaner	<ul style="list-style-type: none"> • References to Box in registry (though less than the 1st Scenario) • BoxSync folder remained intact
3 rd Scenario: Use of CCleaner and Eraser	<ul style="list-style-type: none"> • References to Box in registry (same with 2nd Scenario)

7.11 Presentation

In the following table (Table 25) we summarize our findings from the forensic investigation of Box cloud storage service.

Table 25: Forensic investigation's findings of Box cloud storage service

Operating System	Findings
Installation path Application's installation path	C:\Program Files\Box\ C:\Users\Forensic_Tester\AppData\Local\Box Sync\ C:\Users\Forensic_Tester\AppData\Roaming\Box Desktop C:\Users\Forensic_Tester\BoxSync
Uninstallation	References in Windows registry BoxSync folder remained intact (use of a specific program for its deletion)
Box's Application Software Analysis	Findings
Logs	Information about: <ul style="list-style-type: none"> the operations of the service the name of the files, their size and their hash values the time and date when we uploaded them the ID, name and email address of the user
Database <ul style="list-style-type: none"> item_status.db 	Information about: <ul style="list-style-type: none"> the name of the files, their size and their hash values
ChecksumHashFile.txt	Information about: <ul style="list-style-type: none"> the name of the files, their size and their hash values

RAM	<p>Information about:</p> <ul style="list-style-type: none"> • the name, hash values and size of the files • the time and date when we uploaded them • the username, email address and user ID of the account that we used • the last time that the user logged in
Box Analysis through a Browser	Findings
<p>Mozilla Firefox and Google Chrome</p> <ul style="list-style-type: none"> • History • Cookies • RAM 	<p>Proved our access to Box cloud storage service, when we last visited the site and how many times</p> <p><i>Upload</i></p> <ul style="list-style-type: none"> • discovered the name and type of the files that we uploaded • discovered the time and date when we uploaded them • discovered the contents of the uploaded files and the related to them metadata • discovered their size and hash values (only for Google Chrome) <p><i>Download</i></p> <ul style="list-style-type: none"> • discovered the name of the files and the folder in which we stored them
Metadata	Findings
<ul style="list-style-type: none"> • Date Created • Date Accessed • Date Modified 	<p>Downloaded the files through:</p> <p><i>Box's application software</i></p> <ul style="list-style-type: none"> • got as their value the time and date that the download of the file got completed • except from Date Modified that was not altered <p><i>a browser</i></p> <ul style="list-style-type: none"> • all of them got as their value the time and

	date that the download of the file got completed
File Deletion	Findings
Log files	<ul style="list-style-type: none"> • the files that we deleted • their hash values • the time and date that the deletion took place
File deletion through a browser	<ul style="list-style-type: none"> • temporary storage in Trash folder • recoverability of these files within 30 days

8 Investigation Conclusions

In this chapter we will examine whether we were able to answer the questions we had placed at the beginning of our investigation.

8.1 Investigation Objectives

As we have already stated, the focus of this research is to determine whether there are any data remnants from the use of cloud storage services in a computer system with Windows 7 as operating system. In the first Chapter we defined the objectives of our research:

Objective 1: Determine the theoretical background of digital forensics and cloud storage technology.

In Chapter 2 we analyzed digital forensics, the principles and the rules which are governing it. In Chapter 3 we defined cloud technology and how it affects digital forensics. In chapter 4 we analyzed and examined the “behavior” of RAM, and the data that we can discover in it.

Objective 2: Develop a framework of digital forensic analysis, that will help investigators to follow a standard procedure, when undertaking forensic analysis of cloud storage services.

In Chapter 5 we defined the proposed methodology.

In Chapter 6 we defined the investigation purpose, problem, and a set of questions. We set the experimental procedure, presented the forensic tools that we proposed, created a virtual machine, and extracted a hard drive image and the contents of RAM. Lastly, we examined the data that are generated from the use of various browsers.

Objective 3: Examine popular cloud storage services, like Box, and check if there are any data remnants to contribute to forensic research and analysis.

In Chapter 7 we examined Box cloud storage service. Based on our findings, we concluded that there is a wealth of data generated by the use of these services, either through software or through a browser.

Objective 4: Examine the effects, from a forensic standpoint, that the data traffic of these applications have (metadata, date of access, hash value modification).

Similarly, in chapter 7 we examined Box cloud storage service and discovered the changes that were brought about by file handling through this cloud service.

8.2 Investigation Findings

The role of Chapter 6 is to help us with the transition from the theoretical perspective of our investigation to the practical part of cloud services' examination. To achieve this, we raised a number of questions.

8.2.1 Investigation Question 1

The first investigation question is the following:

1. Which are the evidence / data remnants that are created by the use of cloud services and allowing us to verify whether in fact there was a use of such services?

In Chapter 7 we analyzed in depth the Box cloud storage service. We discovered the existence of digital evidence in a computer system with Windows 7 as operating system, by using the application software, or by using a browser. Also we discovered data remnants, even when we used anti-forensic procedures. Our investigation question 1 led to the following sub-questions:

Case 1: There are no data remnants from the use of cloud services which will help with the identification of the service provider, the user's name, or the files that were transferred.

Case 2: There are data remnants from the use of cloud services which are allowing the identification of the service, the user's name, or the details of the files.

As we have already defined, in the context of our investigation we discovered data remnants in our computer system. So the second Case is proved right and leads us to the following questions.

- Which are the data that remain on the computer after the installation of the application software and its use for uploading and storage of data?

The analysis results of the selected Box cloud storage service are presented in Chapter 7. Initially we focused on the use of Box and the data remnants which arise from its use. We defined the software installation locations, either in folder "AppData", "Roaming" or "Local". We have found the user name either in application's database, in browser's files or in RAM. It must be noted that we also found the password of the account, either

in RAM or in hard drive's files. Each investigator must focus his investigation on item_status.db file, which is a SQL database file, that is located at: C:\Users\Random_User\AppData\Local\BoxSync\item_status.db

- Which are the data that remain on the computer after accessing the cloud service through a browser?

Given that we accessed Box cloud storage service through two browsers, we successfully discovered the username of the account. We also found multiple URL that confirmed the use of this service. Finally, by examining the browsers' files we discovered the files that we transferred and information about them (hash values and dates).

- Which data remain in the volatile memory when the application software is used, and which remain when a browser is used?

Memory analysis revealed us a great wealth of information. Firstly, we discovered, in plaintext, the user name and password that we used for our access to Box cloud storage service. Finally, we managed to find out the names, sizes, hash values and content of the files that we transferred.

8.2.2 Investigation Question 2

The second investigation question is the following:

2. How are the file upload and download processes, of a cloud service, affect the internal files and metadata?

The process of transferring files does not change the contents of the folders, nor their relevant metadata, such as the creation date, author and hash value. Instead, what is changing are the variables Date created, Date accessed, and Date modified of the file. The values that these variables take, depend on the way the download of the files took place.

8.2.3 Special Mention and Further Research

We should particularly mention the fact that in the scenario that we tested, we were able to discover not only the username, but also the password. In addition, by creating a virtual machine, based on the hard drive that we recovered, we were able to gain access, automatically, to Box cloud storage service. This is happening because the software of this kind of applications auto-logs to the user account when the system startup. Lastly,

the areas where we can focus in a future investigation for, is to examine the network packets during the use of this service, as well as access it through smartphones.

Bibliography

- [1] Quick, D., Martini, B. and Choo, K. (2014), *Cloud Storage Forensics*, Waltham: Elsevier Inc.
- [2] Ruan, K. (2013), *Cybercrime and Cloud Forensics: Applications for Investigation Processes*, University College Dublin
- [3] Wheeler, A. and Winburn, M. (2015), *Cloud Storage Security*, Waltham: Elsevier Inc.
- [4] Sammons, J. (2015), *The Basic of Digital Forensics, 2nd Edition*, Waltham: Elsevier Inc.
- [5] Marinescu, D. (2015), *Cloud Computing: Theory and Practice*, Waltham: Elsevier Inc.
- [6] Barrett, D. and Kipper, G. (2010), *Virtualization and Forensics*, Burlington: Elsevier Inc.
- [7] Luttgens, J., Pepe, M. and Mandia, K. (2014), *Incident Response & Computer Forensics, Third Edition*, USA: McGraw-Hill Education
- [8] Watson, D. and Jones, A. (2013), *Digital Forensics Processing and Procedures*, Waltham: Elsevier Inc.
- [9] Aljawarneh, S. (2013), *Cloud Computing Advancements in Design, Implementation, and Technologies*, USA: IGI Global
- [10] Carvey, H. (2012), *Windows Forensics Analysis Toolkit*
- [11] Deloitte, (2009), *Cloud Computing Forecasting Change*
- [12] Chow, K. and Sheno, S. (2010), *Advances in Digital Forensics*
- [13] Iqbal, H. (2009), *Forensic Analysis of Physical Memory and Page File*
- [14] Altheide, C. and Carvey, H. (2011), *Digital Forensic with Open Source Tools*
- [15] Anon (2012), *Digital Investigations in the Cloud*
- [16] Koops, B., Leenes, R., De Hert, P. and Olislaegers, S. (2012), *Crime and Criminal Investigation in the Clouds*

Internet Sources

- [17] ACPO (2007), *Good Practise Guide for Digital Evidence*,

http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[Last Access December 2016]

[18] Box (2016), *Box Overview*, <https://www.box.com/personal>

[Last Access December 2016]

[19] Amari, K. (2009), *Techniques and Tools for Recovering and Analyzing Data from*, <https://www.sans.org/reading-room/whitepapers/forensics/techniques-tools-recovering-analyzing-data-volatile-memory-33049>

[Last Access December 2016]

[20] Digital Corpora, *thread1.zip*, <http://digitalcorpora.org/corpora/files/govdocs1/threads/>

[Last Access December 2016]

[21] Dykstra, J. (2013), *Seizing Electronic Evidence from Cloud Computing Environments*, <http://www.csee.umbc.edu/~dykstra/Seizing-Electronic-Evidence-from-Cloud-Computing-Environments.pdf>

[Last Access December 2016]

[22] Lawton, G. (2011), *Cloud Computing Crime Poses Unique Forensics Challenge*, <http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-crime-poses-unique-forensics-challenges>

[Last Access December 2016]

[23] McKemmish, R. (1999), *What is Forensic Computing?* http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi118.pdf

[Last Access December 2016]

[24] OSForensics, *Disk Drive Signatures*, <http://www.osforensics.com/compare-drive-signatures.html>

[Last Access December 2016]

[25] Alpeyev, P., Galante, J. and Yasu, M. (2011), *Amazon.com Server Said to Have Been Used in Sony Attack*, <http://www.bloomberg.com/news/2011-05-13/sony-network-said-to-have-been-invaded-by-hackers-using-amazon-com-server.html>

[Last Access December 2016]

[26] National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*,

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

[Last Access December 2016]

[27] Garfinkel, T., Pfaff, B., Chow, J. and Rosenblum, M. (2004), *Data Lifetime is a Systems Problem*,

<http://www-cs.stanford.edu/people/jchow/papers/lifetime-sigops04.pdf>

{Last Access December 2016]

[28] U.S Department of Justice (2004), *Forensic Examination of Digital Evidence*,
<https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>

[Last Access December 2016]

[29] Scientific Working Group (2008), *SWGDE Capture of Live Systems*,
<https://www.swgde.org/documents/Current%20Documents/2008-01-28%20SWGDE%20Capture%20of%20Live%20Systems%20v1.0>

[Last Access December 2016]

[30] Quora (2015), *Where and how is the registry stored in Windows?*

<https://www.quora.com/Where-and-how-is-the-registry-stored-in-Windows>

[Last Access December 2016]

[31] TalkCloudComputing (2012), *Reasons why Private Cloud is a preferable option*,
<http://talkcloudcomputing.com/reasons-why-private-cloud-is-a-preferable-option/>

[Last Access December 2016]

[32] Armedia (2012), *Federal cloud computing challenges part 1 – cloud deployment models*,

<http://www.amedia.com/blog/2012/03/federal-cloud-computing-challenges-part-1-cloud-deployment-models/>

[Last Access December 2016]

[33] TechTarget (2015), *Hybrid cloud*,

<http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud>

[Last Access December 2016]

Table of Figures

Figure 1: Phases of forensic investigation.....	16
Figure 2: Key features that compose Cloud-based systems.....	24
Figure 3: Service delivery models of a Cloud-based system	26
Figure 4: SaaS Infrastructure	27
Figure 5: PaaS Infrastructure	28
Figure 6: IaaS Infrastructure.....	29
Figure 7: Public Cloud	30
Figure 8: Private Cloud.....	31
Figure 9: Community Cloud.....	31
Figure 10: Hybrid Cloud	32
Figure 11: Deployment model matrix	33
Figure 12: A graph of the number of changes in memory over time on a Solaris 8 machine set up as a DNS server with 768 MB of RAM.....	39
Figure 13: Proposed methodology	43
Figure 14: Investigation's experimental procedure.....	47
Figure 15: OSForensics interface.....	51
Figure 16: Esentutl.exe command line tool	52
Figure 17: Virtual Machine's features	53
Figure 18: Virtual Machine's Snapshot.....	54
Figure 19: Procedure of creating Hash values	55
Figure 20: Use of the DumpIt program.....	56
Figure 21: Form of the DumpIt file.....	56
Figure 22: Selection of Kali's operation mode.....	57
Figure 23: Information about the hard drives	58
Figure 24: Command sequence for the creation of the image	59
Figure 25: Completion of image creation	59
Figure 26: Confirmation of image integrity	60

Figure 27: Screenshot of the ProDiscover program use	61
Figure 28: Procedure to create the image.vmdk file.....	61
Figure 29: image.vmdk files created inside the external hard drive	62
Figure 30: Creation of Virtual Machine and choosing to install the operating system later	63
Figure 31: Removal of the default disk and addition of the file that we created (1)	63
Figure 32: Removal of the default disk and addition of the file that we created (2)	64
Figure 33: Presentation of Mozilla Firefox's files	65
Figure 34: Folder of the to be examined SQL databases.....	65
Figure 35: Places.sqlite file	66
Figure 36: Investigation of Mozilla Firefox's database (places.sqlite)	66
Figure 37: Presentation of Google Chrome's files.....	67
Figure 38: Folder of the to be examined SQL databases.....	68
Figure 39: Google Chrome's History file	68
Figure 40: Investigation of Google Chrome's database (History).....	69
Figure 41: Snapshot from the signature creation process.....	70
Figure 42: Presentation of Box's cloud storage services (1)	72
Figure 43: Presentation of Box's cloud storage services (2)	73
Figure 44: Use of SHA-1 hash function	78
Figure 45: Discovery of email address, time, date and the name of the files we uploaded.....	79
Figure 46: Discovery of username, email and ID in RAM	81
Figure 47: Discovery of account's password	82
Figure 48: Discovery of the files we transferred	83
Figure 49: Discovery of the files we transferred	86
Figure 50: Examination of RAM (1)	87
Figure 51: Discovery of user's name, email address and user ID.....	88
Figure 52: Application's interface through a browser	90

Figure 53: Mozilla Firefox's History	91
Figure 54: Examination of Firefox's History database	92
Figure 55: Examination of Firefox's Cookies database	92
Figure 56: Examination of RAM (1)	93
Figure 57: Examination of RAM (2)	94
Figure 58: Discovery of files' metadata	95
Figure 59: Discovery of contents (1)	96
Figure 60: Discovery of file contents (2)	97
Figure 61: Examination of RAM (3)	98
Figure 62: Examination of Google Chrome's History database	98
Figure 63: Examination of Google Chrome's History	99
Figure 64: Examination of RAM (1)	99
Figure 65: Examination of RAM (2)	100
Figure 66: Examination of RAM (3)	100
Figure 67: Examination of RAM (4)	101
Figure 68: File's metadata through Box's application software	103
Figure 69: File's metadata through the use of a browser	104
Figure 70: File's metadata	105
Figure 71: Discovery of the deleted files	106
Figure 72: Box's trash folder	107

Table of Tables

Table 1: Investigation steps by using the Application Software 48

Table 2: Investigation steps through the use of a browser 48

Table 3: File handling through cloud storage service’s software..... 49

Table 4: File handling through a browser 49

Table 5: Investigation’s computer system 50

Table 6: Presentation of the files that we will be handling..... 55

Table 7: Executable files of Box 75

Table 8: Log files related to Box..... 75

Table 9: Application’s SQL databases 76

Table 10: File storage folder..... 76

Table 11: Registry changes (1) 76

Table 12: Registry changes (2) 76

Table 13: Examination of Log files (1)..... 77

Table 14: Examination of Log files (2)..... 78

Table 15: Using Box’s application software..... 79

Table 16: Examination of RAM (use of Box’s application software) 84

Table 17: Examination of Log files (1)..... 85

Table 18: Examination of Log files (2)..... 85

Table 19: Use of Box’s application software 86

Table 20: Use of Box’s application software (summarized) 89

Table 21: Accessing Box through browser 101

Table 22: Examination of Log files (1)..... 106

Table 23: Examination of Log files (2)..... 107

Table 24: Conclusions from the uninstallation of Box’s application software .. 108

Table 25: Forensic investigation’s findings of Box cloud storage service 109

