Applied Forensics

EHC LVL5 - S02 2021/2022

Toqa Mahmoud

CU1900305

The Knowledge Hub Universities

TABLE OF CONTENTS

LIST OF TABLES

LIST OF SCREENSHOTS

INTRODUCTION

As stated by Biscom, more than 25% of employees steal sensitive data when they leave their business. Customer lists, secret formulas, source code, strategy papers, and other trade secrets are among the most regularly taken intellectual property. When an ex-employee leaves to work for a competitor or starts a brand new business, the data is commonly utilized against the company (Opsitnick et al., 2021). Digital forensics is the systematic collection of processes and techniques for extracting evidence from machines and hard disks. This data can then be evaluated for pertinent information, which frequently leads to incontrovertible proof of the accused theft of intellectual property. Therefore even if the data stolen in an IP Theft case is no longer in the victim's hands, evidence remains on the suspect's devices, which can be used to prove what happened (Damon S., 2013).

The purpose of this report is to provide corroborative evidence of the motivation, opportunity and intent leading to the fraud perpetrated by castor troy. The facts presented within this report are those within preparer's own area of expertise and knowledge and do not extend to matters and knowledge outside such expertise

SUMMARY OF CASE

An employee abruptly left my company that he has worked at for the past 5 years. During his tenure, he was involved in a top-secret project and had access to some critical intellectual property. Due to the sensitive nature of the project and his sudden departure, company counsel would like to know if any of that information was accessed or copied. During his tenure, the company gave the employee PC and mobile phone to be used for business purposes. Therefore, a forensic examination was conducted by analyzing the image, looking for critical Intelligent Property and investigating whether these files have been transferred out from the system.

FORENSIC EXAMINATION

I explored in the deep shadows of the Operating System and File System while completing the assessment, examining, theorizing, and verifying the minute minutiae of what gets stored or left behind. You presumably already know that every encounter you have with the gadget is documented in some way. Consider the easy step of placing a new flash drive into a machine running Microsoft Windows' USB port. There is a brief pause, followed by an audible tone and a notification in the Task Bar stating that the drive is now available for usage. The Windows OS is busily collecting down all kinds of facts about the item and storing it away for later use within the fraction of a minute between when it is inserted and when it is made available. What's fascinating is that the Operating System and System Files save thousands of such types of digital trails, all of which are accessible to forensic investigators. (Damon S., 2013).

METHODOLOGY

Employee data theft is most common soon before or shortly after an employee's firing or resignation from a business. Other than text messages on a mobile, on a standard Windows installation, these locations are:

- USB activities
- Accessed or deleted files
- Email accounts
- Internet history report
- Programs installed

As a result, I suspected the employee was engaging in odd behavior, such as:

- Inserting a personal USB or hard drive into a computer.
- Arriving at work at strange hours or setting up remote desktop connections after hours.
- Using the company network to transfer big amounts of data.
- Using cloud storage services such as Dropbox or Google Drive.
- Using personal accounts to send messages with attachments.
- Installing data-copying and data-transfer programs.
- Suspicious communication with third parties..

USB ACTIVITY ANALYSIS

Many USB devices today have sufficient storage capacity to preserve a whole copy of a user's hard disc. As a result, they are one of the most commonly utilised techniques for data theft. As mentioned previously, the great news is that utilising a USB device leaves a data trail that can be quite useful in an inquiry.

I began by looking at the suspect’s USB usage, as this can provide various important details about what was attached to the machine and when. I made certain to record the USB device's serial number and/or brand, as well as the first and last times it was attached to the computer. Additionally, confirm that a distinct USB device was attached each time. (Opsitnick et al., 2021).

FILES RECENTLY OPENED

While knowing that a USB device was connected to a computer is crucial, analyzing what files were viewed and potentially transmitted to the device is much more crucial. The Microsoft Windows OS creates numerous artefacts when a user views a file or folder. These artefacts show what's been viewed, when it was viewed, and from where it came. When these artefacts are paired with a USB activity timeline, there's a good chance that content was transferred off the system..

Finally, the artefacts may include data on the location of the file. The artefact will identify if a file was opened from a USB drive, providing verifiable evidence that the suspect has a USB drive containing specified files (Opsitnick et al., 2021).

PERSONAL EMAIL ACCOUNTS

Some employees may send files to their personal email accounts, such as Yahoo or Gmail, using their corporate email. As a result, I made it a point to search through the employee's work email to find and document any proof of misbehaviour (Opsitnick et al., 2021).

INTERNET HISTORY REPORT

A report of recent Internet searches, web sites and pages viewed, cookies from websites, and Internet downloads can be generated. Such data is useful in determining what an individual considered essential or even their mental condition. Analysts noticed, for example, that people searched for ways to secretly erase or copy data and studied websites that were essentially "how to guides" for performing various nefarious behaviours (Opsitnick et al., 2021).

INSTALLED PROGRAMS

Looking at the programmes the suspect installed on their machine helped me figure out how they used it. For example, how did he examine or alter images if he had them? How did he open ZIP and RAR files and extract information if he possessed them? How did he watch digital movies if he had them? (Pixley et al., 2019)

SMS MESSAGES

Since we have the suspect's mobile phone it is crucial to analyze text messages. These messages often contain intimate, revealing material that may be pertinent to a civil or criminal case (Pixley et al., 2019).

WHAT COMPUTER FORENSICS TOOLS WERE USED?

The forensic tools employed in the performance of this investigation were as follows:

- **Magnet Axiom – V4.6**
  A GUI tool which can recover and analyze digital evidence from the most sources, such as Windows, Mac, Linux systems, including Android and IOS Mobiles, all in one case file.
- **Autopsy® – Sleuth Kit 4.19**
  A graphical interface to **The Sleuth Kit®** and other digital forensics tools, as well as a digital forensics platform. To investigate what happened on a computer, law enforcement, military, and corporate examiners use it
  - **RegRipper –** Used in Autopsy's registry analysis to find documents and USB devices that have been accessed recently

Magnet Axiom is more user friendly than Autopsy however Axiom is a paid software. On the other hand, Autopsy is an open-source software. While investigating with both tools, I personally did not feel much of a difference in the artifacts output between them. The only difference is that Axiom reads and analyzes the software/OS information in more details.

WHAT SYSTEMS/TECHNOLOGIES EXAMINED?

There were 2 systems that were investigated thoroughly which are – Winxp.E01 and Mobile.zip. More information on each device is shown below in tables 1 & 2. All information was extracted mostly from Axiom.

Table 1 Technology #1

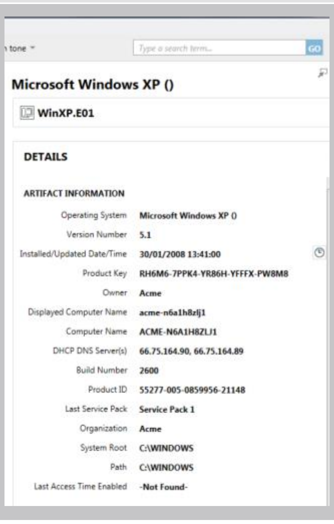
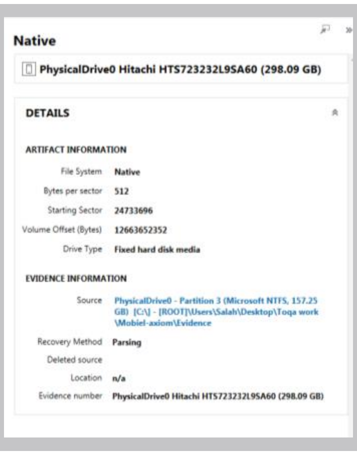
Technology #1	Winxp.E01
Type	Image
Image Hash	MD5: 0f2878011ca9f0a06e72cac56dabc443
Operating System	Microsoft Windows XP
Install Date	2008-01-30 13:41:00 EET
Owner	Acme
Account Name	ACME-N6A1H8ZLJ1
Details	 Microsoft Windows XP () WinXP.E01 DETAILS ARTIFACT INFORMATION Operating System: Microsoft Windows XP () Version Number: 5.1 Installed/Updated Date/Time: 30/01/2008 13:41:00 Product Key: RH6M6-7PPK4-YR86H-YFFFX-PW8M8 Owner: Acme Displayed Computer Name: acme-n6a1h8zlj1 Computer Name: ACME-N6A1H8ZLJ1 DHCP DNS Server(s): 66.75.164.90, 66.75.164.89 Build Number: 2600 Product ID: 55277-005-0859956-21148 Last Service Pack: Service Pack 1 Organization: Acme System Root: C:\WINDOWS Path: C:\WINDOWS Last Access Time Enabled: -Not Found-

Table 2 Technology #2

Technology #2	Mobile.zip
Type	Fixed Hard Disks Media
Device Name	Hitachi HTS723232L9SA60
Device ID	83edc3b2-3df8-59d9-8465-015bb9b7238f
Install Date	N/A
Owner	N/A
Account Name	N/A

Details	

Native

PhysicalDrive0 Hitachi HTS723232L9SA60 (298.09 GB)

DETAILS

ARTIFACT INFORMATION

File System	Native
Bytes per sector	512
Starting Sector	24733696
Volume Offset (Bytes)	12663652352
Drive Type	Fixed hard disk media

EVIDENCE INFORMATION

Source	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 157.25 GB) [C:\] - [ROOT]\Users\Salah\Desktop\Toqa work \Mobiel-axiom\Evidence
Recovery Method	Parsing
Deleted source	
Location	n/a
Evidence number	PhysicalDrive0 Hitachi HTS723232L9SA60 (298.09 GB)

EVIDENCE CLASSES

Table 3 summarizes the important evidences that were discovered in the investigation.

Table 3 Evidence Classes

Evidence Class	Description	Type
1	Winzip installed	Program
2	Ntuser.dat	File
3	system	File
4	Messages	SMS
5	Messages	SMS

EVIDENCE CLASS 1

Table 4 shows information about the installed program “WinZip”.

Table 4 Software Name WinZip 11.1 v 11.1.7466

Item	**WinXP.E01**
Software Name	WinZip 11.1 v 11.1.7466
Path	/Img_WinXP.E01/vol_vol2/system32/config/software
Hash Value	MD5: bbef3c212333dec3baac154bfaecd74d SHA-256: 13b156f677ba1db0925876f1c48fd4e5009e5e7337f32ee1cea08f0fa3941fd5
Created time	2008-01-30 07:29:12 EET
Accessed time	2008-01-30 16:51:23 EET

Modified time	2008-01-30 16:51:23 EET

EXHIBIT A

All WinZip's data table 4 are shown in screenshot 1 below with more details.

ANALYSIS

WinZip is is a trialware file archiver and compressor, mostly used to compress files and folders before transferring it from one place to another. The fact that Castor Troy did install this software means that he needed it to engage in some activity relating to extracting or compressing data.

EVIDENCE CLASS 2

EXHIBIT B

Table 5 shows information about "NTUSER.DAT", which is found inside the user Castor Troy. This file ensures that any changes made in the user account are saved and loaded when they sign in back again. This file contains very important information that will be discussed below.

Item	**WinXP.E01**
File Name	NTUSER.DAT
Path	/Img_WinXP.E01/vol_vol2/Documents and Settings/Castor Troy/NTUSER.DAT/
Hash Value	MD5: ea09ed13af1342c6ae345edd39cb5f89 SHA-256: 19a1777a10f121034948966ee30c5b6105004c5447159c7669ea71e13b572b94
Created time	2008-01-31 06:32:20 EET
Accessed time	2008-01-30 16:51:20 EET
Modified time	2008-01-30 16:51:20 EET

Table 5 NTUSER.DAT

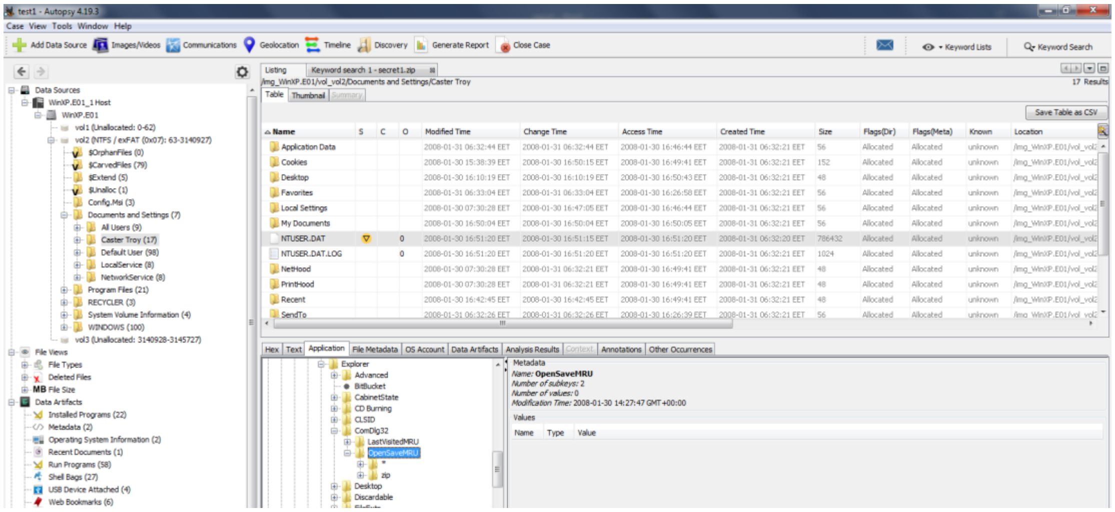
1 – COMDLG32

Location: Software/Microsoft/Windows/CurrentVersion/Explorer/Comdlg32

By investigation this directory, I found out that there are 2 sub-folders:

1. OpenSaveMRU – Modification time: 2008-01-30 14:27:47 GMT +00:00

   Note: The abbreviation MRU stands for "most recently used".



/img_WinXP.E01/vol_vol2/Documents and Settings/Caster Troy

17 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Application Data				2008-01-31 06:32:44 EET	2008-01-31 06:32:44 EET	2008-01-30 16:46:44 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
Cookies				2008-01-30 15:38:39 EET	2008-01-30 16:50:15 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	152	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
Desktop				2008-01-30 16:10:19 EET	2008-01-30 16:10:19 EET	2008-01-30 16:50:43 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
Favorites				2008-01-31 06:33:04 EET	2008-01-31 06:33:04 EET	2008-01-30 16:26:58 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
Local Settings				2008-01-30 07:30:28 EET	2008-01-30 16:47:05 EET	2008-01-30 16:46:44 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
My Documents				2008-01-30 16:50:04 EET	2008-01-30 16:50:04 EET	2008-01-30 16:50:05 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
NTUSER.DAT	▽		0	2008-01-30 16:51:20 EET	2008-01-30 16:51:15 EET	2008-01-30 16:51:20 EET	2008-01-31 06:32:20 EET	786432	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
NTUSER.DAT.LOG			0	2008-01-30 16:51:20 EET	2008-01-30 16:51:20 EET	2008-01-30 16:51:20 EET	2008-01-31 06:32:21 EET	1024	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
NetHood				2008-01-30 07:30:28 EET	2008-01-31 06:32:21 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
PrintHood				2008-01-30 07:30:28 EET	2008-01-31 06:32:21 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
Recent				2008-01-30 16:42:45 EET	2008-01-30 16:42:45 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
SendTo				2008-01-31 06:32:26 EET	2008-01-31 06:32:26 EET	2008-01-30 16:26:39 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2

Metadata
Name: **OpenSaveMRU**
Number of subkeys: 2
Number of values: 0
Modification Time: 2008-01-30 14:27:47 GMT +00:00

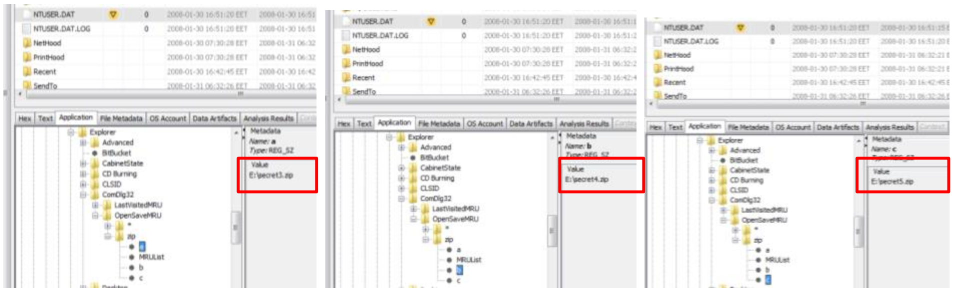
Values

Name	Type	Value

Screenshot 1 OpenSaveMRU

- This key tracks files that have been opened or saved within a Windows shell dialog box, as shown below.

Screenshot 2 OpenSaveMRU Values

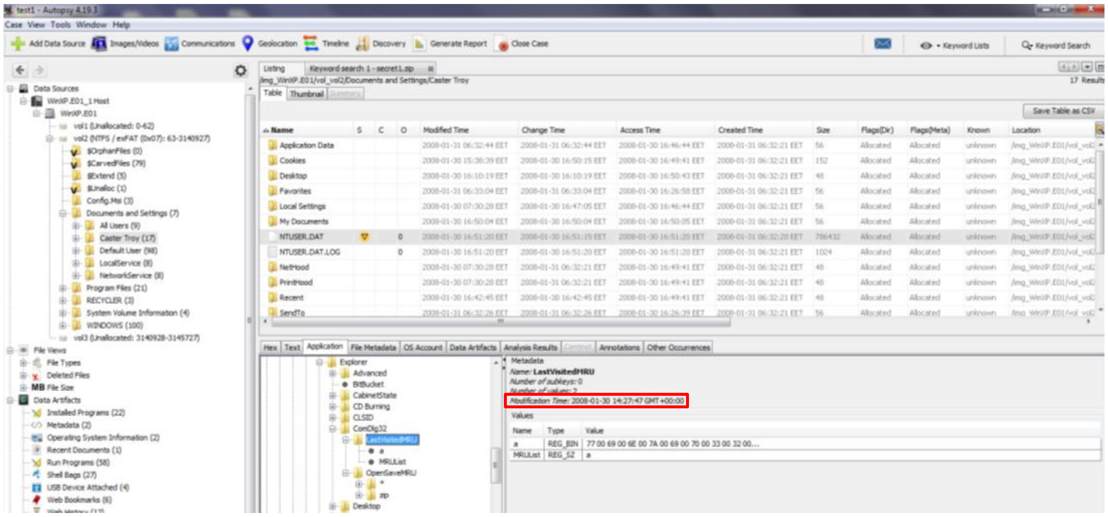


Metadata
Name: a
Type: REG_SZ
Value
E:\secret3.zip

Metadata
Name: b
Type: REG_SZ
Value
E:\secret4.zip

Metadata
Name: c
Type: REG_SZ
Value
E:\secret5.zip

2. LastVisitedMRU – Modification time: 2008-01-30 14:27:47 GMT +00:00



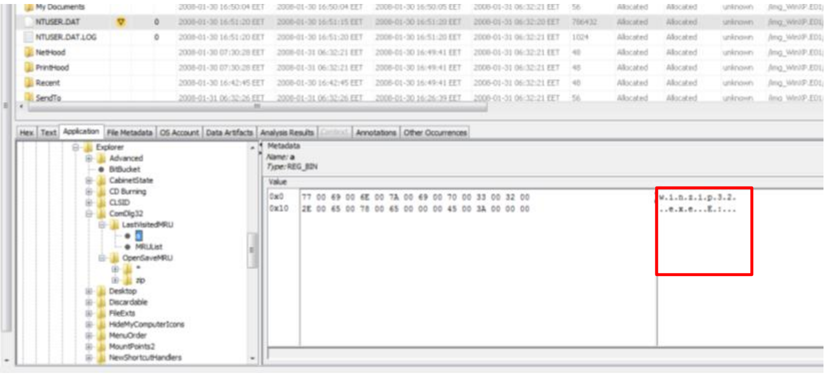
Metadata
Name: **LastVisitedMRU**
Number of subkeys: 0
Number of values: 2
Modification Time: 2008-01-30 14:27:47 GMT +00:00

Values

Name	Type	Value
a	REG_BIN	77 00 69 00 6E 00 7A 00 69 00 70 00 33 00 32 00...
MRUList	REG_SZ	a

Screenshot 3 LastVisitedMRU

- This key tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key



My Documents			2008-01-30 16:50:04 EET	2008-01-30 16:50:04 EET	2008-01-30 16:50:05 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/
NTUSER.DAT	▽	0	2008-01-30 16:51:20 EET	2008-01-30 16:51:15 EET	2008-01-30 16:51:20 EET	2008-01-31 06:32:20 EET	786432	Allocated	Allocated	unknown	/img_WinXP.E01/
NTUSER.DAT.LOG		0	2008-01-30 16:51:20 EET	2008-01-30 16:51:20 EET	2008-01-30 16:51:20 EET	2008-01-31 06:32:21 EET	1024	Allocated	Allocated	unknown	/img_WinXP.E01/
NetHood			2008-01-30 07:30:28 EET	2008-01-31 06:32:21 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/
PrintHood			2008-01-30 07:30:28 EET	2008-01-31 06:32:21 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/
Recent			2008-01-30 16:42:45 EET	2008-01-30 16:42:45 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/
SendTo			2008-01-31 06:32:26 EET	2008-01-31 06:32:26 EET	2008-01-30 16:26:39 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/

Metadata
Name: a
Type: REG_BIN

Value

```
0x0    77 00 69 00 6E 00 7A 00 69 00 70 00 33 00 32 00    w.i.n.z.i.p.3.2.
0x10   2E 00 65 00 78 00 65 00 00 00 45 00 3A 00 00 00    ..e.x.e...E.:...
```

Screenshot 4 LastVisitedMRU Value

ANALYSIS

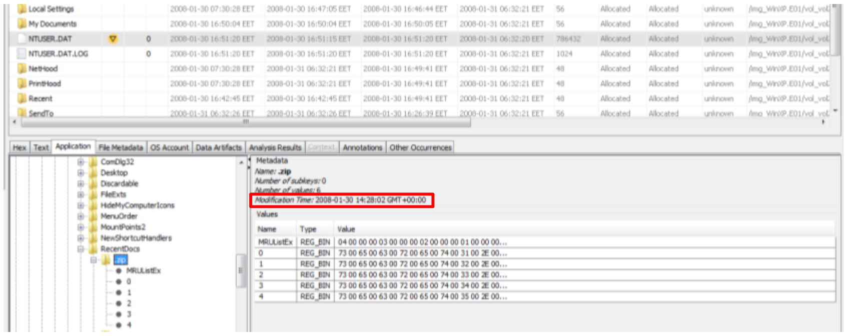
The WinZip application was used by Troy the same time he accessed secret3.zip, secret4.zip, and secret5.zip. This indicates that these files were compressed using the software, WinZip.

2 – RECENT DOCS

Location: Software/Microsoft/Windows/CurrentVersion/Explorer/RecentDocs

By investigating this directory, I found out that there are 2 sub-folders:

1. .zip – modification time: 2008-01-30 14:28:02 GMT +00:00



Local Settings			2008-01-30 07:30:28 EET	2008-01-30 16:47:05 EET	2008-01-30 16:46:44 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol
My Documents			2008-01-30 16:50:04 EET	2008-01-30 16:50:04 EET	2008-01-30 16:50:05 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol
NTUSER.DAT	▽	0	2008-01-30 16:51:20 EET	2008-01-30 16:51:15 EET	2008-01-30 16:51:20 EET	2008-01-31 06:32:20 EET	786432	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol
NTUSER.DAT.LOG		0	2008-01-30 16:51:20 EET	2008-01-30 16:51:20 EET	2008-01-30 16:51:20 EET	2008-01-31 06:32:21 EET	1024	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol
NetHood			2008-01-30 07:30:28 EET	2008-01-31 06:32:21 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol
PrintHood			2008-01-30 07:30:28 EET	2008-01-31 06:32:21 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol
Recent			2008-01-30 16:42:45 EET	2008-01-30 16:42:45 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol
SendTo			2008-01-31 06:32:26 EET	2008-01-31 06:32:26 EET	2008-01-30 16:26:39 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol

Metadata
Name: .zip
Number of subkeys: 0
Number of values: 6
Modification Time: 2008-01-30 14:28:02 GMT+00:00

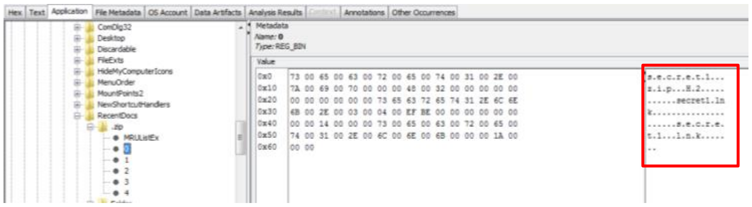
Values

Name	Type	Value
MRUListEx	REG_BIN	04 00 00 00 03 00 00 00 02 00 00 00 01 00 00 00...
0	REG_BIN	73 00 65 00 63 00 72 00 65 00 74 00 31 00 2E 00...
1	REG_BIN	73 00 65 00 63 00 72 00 65 00 74 00 32 00 2E 00...
2	REG_BIN	73 00 65 00 63 00 72 00 65 00 74 00 33 00 2E 00...
3	REG_BIN	73 00 65 00 63 00 72 00 65 00 74 00 34 00 2E 00...
4	REG_BIN	73 00 65 00 63 00 72 00 65 00 74 00 35 00 2E 00...

Screenshot 5 .zip

- This folder contains 6 values – MRUListEx, 0, 1, 2, 3, 4. The screenshots shows that secret1.zip, secret2.zip, secret3.zip, secret4.zip, secret5.zip were recently modified.

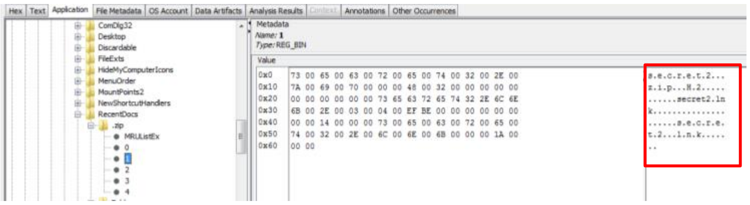
Screenshot 6 .zip values



Metadata
Name: **0**
Type: REG_BIN

Value

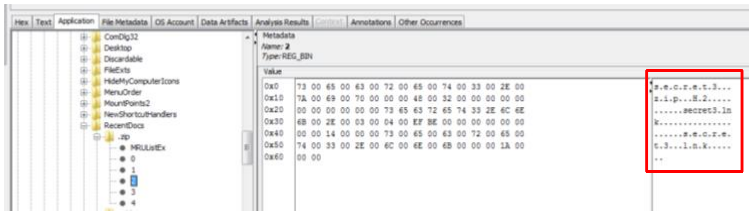
```
0x0    73 00 65 00 63 00 72 00 65 00 74 00 31 00 2E 00    s.e.c.r.e.t.1...
0x10   7A 00 69 00 70 00 00 00 48 00 32 00 00 00 00 00    z.i.p...H.2.....
0x20   00 00 00 00 00 00 73 65 63 72 65 74 31 2E 6C 6E    ......secret1.ln
0x30   6B 00 2E 00 03 00 04 00 EF BE 00 00 00 00 00 00    k...............
0x40   00 00 14 00 00 00 73 00 65 00 63 00 72 00 65 00    ......s.e.c.r.e.
0x50   74 00 31 00 2E 00 6C 00 6E 00 6B 00 00 00 1A 00    t.1...l.n.k.....
0x60   00 00                                              ..
```



Metadata
Name: **1**
Type: REG_BIN

Value

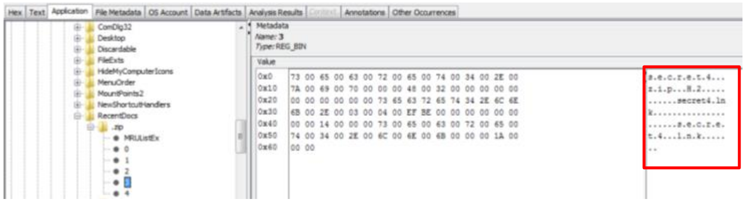
```
0x0    73 00 65 00 63 00 72 00 65 00 74 00 32 00 2E 00    s.e.c.r.e.t.2...
0x10   7A 00 69 00 70 00 00 00 48 00 32 00 00 00 00 00    z.i.p...H.2.....
0x20   00 00 00 00 00 00 73 65 63 72 65 74 32 2E 6C 6E    ......secret2.ln
0x30   6B 00 2E 00 03 00 04 00 EF BE 00 00 00 00 00 00    k...............
0x40   00 00 14 00 00 00 73 00 65 00 63 00 72 00 65 00    ......s.e.c.r.e.
0x50   74 00 32 00 2E 00 6C 00 6E 00 6B 00 00 00 1A 00    t.2...l.n.k.....
0x60   00 00                                              ..
```



Metadata
Name: **2**
Type: REG_BIN

Value

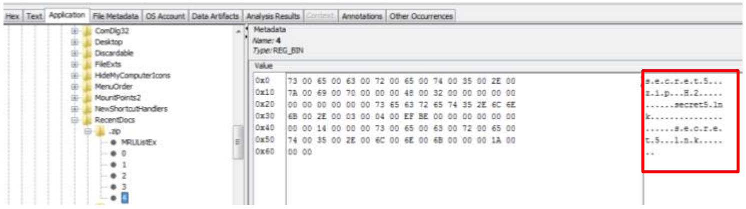
```
0x0    73 00 65 00 63 00 72 00 65 00 74 00 33 00 2E 00    s.e.c.r.e.t.3...
0x10   7A 00 69 00 70 00 00 00 48 00 32 00 00 00 00 00    z.i.p...H.2.....
0x20   00 00 00 00 00 00 73 65 63 72 65 74 33 2E 6C 6E    ......secret3.ln
0x30   6B 00 2E 00 03 00 04 00 EF BE 00 00 00 00 00 00    k...............
0x40   00 00 14 00 00 00 73 00 65 00 63 00 72 00 65 00    ......s.e.c.r.e.
0x50   74 00 33 00 2E 00 6C 00 6E 00 6B 00 00 00 1A 00    t.3...l.n.k.....
0x60   00 00                                              ..
```



Metadata
Name: **3**
Type: REG_BIN

Value

```
0x0    73 00 65 00 63 00 72 00 65 00 74 00 34 00 2E 00    s.e.c.r.e.t.4...
0x10   7A 00 69 00 70 00 00 00 48 00 32 00 00 00 00 00    z.i.p...H.2.....
0x20   00 00 00 00 00 00 73 65 63 72 65 74 34 2E 6C 6E    ......secret4.ln
0x30   6B 00 2E 00 03 00 04 00 EF BE 00 00 00 00 00 00    k...............
0x40   00 00 14 00 00 00 73 00 65 00 63 00 72 00 65 00    ......s.e.c.r.e.
0x50   74 00 34 00 2E 00 6C 00 6E 00 6B 00 00 00 1A 00    t.4...l.n.k.....
0x60   00 00                                              ..
```

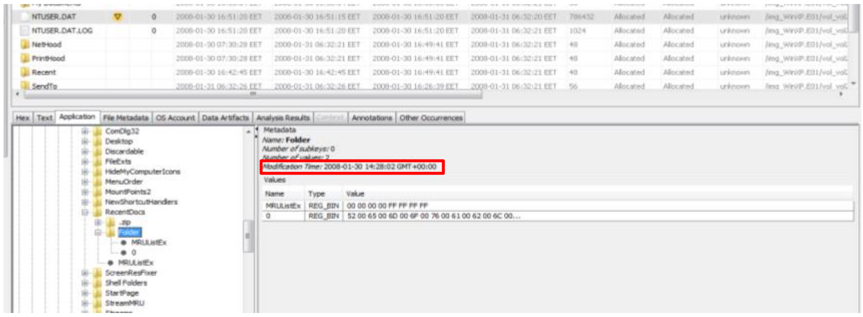


Metadata
Name: **4**
Type: REG_BIN

Value

```
0x0    73 00 65 00 63 00 72 00 65 00 74 00 35 00 2E 00    s.e.c.r.e.t.5...
0x10   7A 00 69 00 70 00 00 00 48 00 32 00 00 00 00 00    z.i.p...H.2.....
0x20   00 00 00 00 00 00 73 65 63 72 65 74 35 2E 6C 6E    ......secret5.ln
0x30   6B 00 2E 00 03 00 04 00 EF BE 00 00 00 00 00 00    k...............
0x40   00 00 14 00 00 00 73 00 65 00 63 00 72 00 65 00    ......s.e.c.r.e.
0x50   74 00 35 00 2E 00 6C 00 6E 00 6B 00 00 00 1A 00    t.5...l.n.k.....
0x60   00 00                                              ..
```

2. Folder – modification time: 2008-01-30 14:28:02 GMT +00:00



NTUSER.DAT	0	2008-01-30 16:51:20 EET	2008-01-30 16:51:15 EET	2008-01-30 16:51:20 EET	2008-01-31 06:32:20 EET	786432	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol
NTUSER.DAT.LOG	0	2008-01-30 16:51:20 EET	2008-01-30 16:51:20 EET	2008-01-30 16:51:20 EET	2008-01-31 06:32:21 EET	1024	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol
NetHood		2008-01-30 07:30:28 EET	2008-01-31 06:32:21 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol
PrintHood		2008-01-30 07:30:28 EET	2008-01-31 06:32:21 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol
Recent		2008-01-30 16:42:45 EET	2008-01-30 16:42:45 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol
SendTo		2008-01-31 06:32:26 EET	2008-01-31 06:32:26 EET	2008-01-30 16:26:39 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol

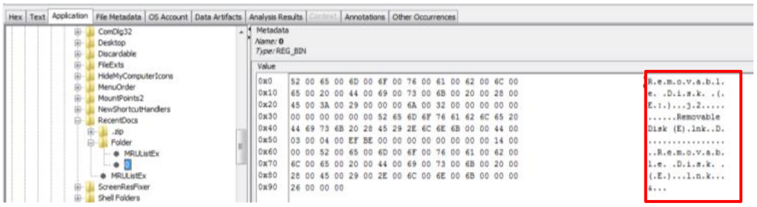
Metadata
Name: **Folder**
Number of subkeys: 0
Number of values: 2
Modification Time: 2008-01-30 14:28:02 GMT+00:00

Values

Name	Type	Value
MRUListEx	REG_BIN	00 00 00 00 FF FF FF FF
0	REG_BIN	52 00 65 00 6D 00 6F 00 76 00 61 00 62 00 6C 00...

Screenshot 7 Folder

- This folder contains 2 values – MRUListEx and 0. The screenshot shows that a removable disk was modified.



Metadata
Name: **0**
Type: REG_BIN

Value

```
0x0   52 00 65 00 6D 00 6F 00 76 00 61 00 62 00 6C 00   R.e.m.o.v.a.b.l.
0x10  65 00 20 00 44 00 69 00 73 00 6B 00 20 00 28 00   e. .D.i.s.k. .(.
0x20  45 00 3A 00 29 00 00 00 6A 00 32 00 00 00 00 00   E.:.)...j.2.....
0x30  00 00 00 00 00 00 52 65 6D 6F 76 61 62 6C 65 20   ......Removable 
0x40  44 69 73 6B 20 28 45 29 2E 6C 6E 6B 00 00 44 00   Disk (E).lnk..D.
0x50  03 00 04 00 EF BE 00 00 00 00 00 00 00 00 14 00   ................
0x60  00 00 52 00 65 00 6D 00 6F 00 76 00 61 00 62 00   ..R.e.m.o.v.a.b.
0x70  6C 00 65 00 20 00 44 00 69 00 73 00 6B 00 20 00   l.e. .D.i.s.k. .
0x80  28 00 45 00 29 00 2E 00 6C 00 6E 00 6B 00 00 00   (.E.)...l.n.k...
0x90  26 00 00 00                                       &...
```

Screenshot 8 Folder Values

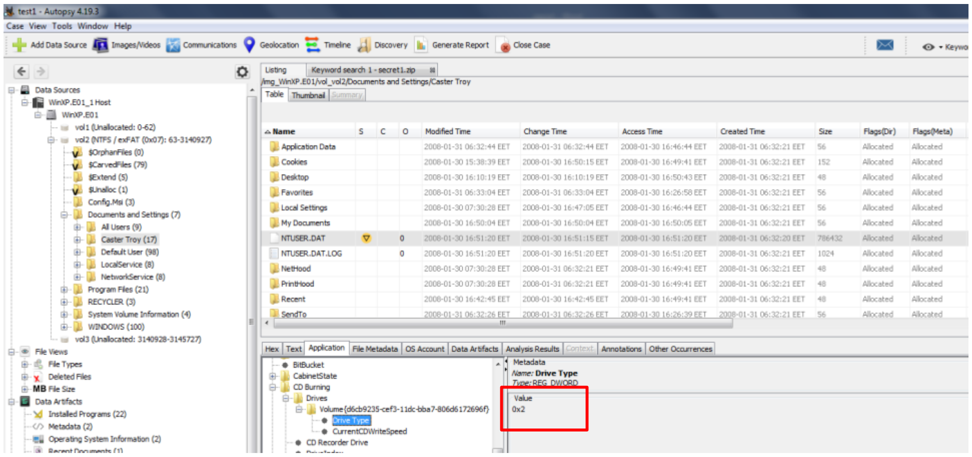
ANALYSIS

The above evidence shows that Troy accessed 5 secret zip files from a different drive, E:\. This drive can be an external drive attached to the device. So far, all findings link to each other making the suspect more doubtful.

3 – DRIVES

<u>Location:</u> Software/Microsoft/Windows/CurrentVersion/ CDburning/Drives

By investigation this directory, I found 1 volume with a value of (0x2), which means that this is a removable disk (refer to table):



/img_WinXP.E01/vol_vol2/Documents and Settings/Caster Troy

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
Application Data				2008-01-31 06:32:44 EET	2008-01-31 06:32:44 EET	2008-01-30 16:46:44 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated
Cookies				2008-01-30 15:38:39 EET	2008-01-30 16:50:15 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	152	Allocated	Allocated
Desktop				2008-01-30 16:10:19 EET	2008-01-30 16:10:19 EET	2008-01-30 16:50:43 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated
Favorites				2008-01-31 06:33:04 EET	2008-01-31 06:33:04 EET	2008-01-30 16:26:58 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated
Local Settings				2008-01-30 07:30:28 EET	2008-01-30 16:47:05 EET	2008-01-30 16:46:44 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated
My Documents				2008-01-30 16:50:04 EET	2008-01-30 16:50:04 EET	2008-01-30 16:50:05 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated
NTUSER.DAT	▽		0	2008-01-30 16:51:20 EET	2008-01-30 16:51:15 EET	2008-01-30 16:51:20 EET	2008-01-31 06:32:20 EET	786432	Allocated	Allocated
NTUSER.DAT.LOG			0	2008-01-30 16:51:20 EET	2008-01-30 16:51:20 EET	2008-01-30 16:51:20 EET	2008-01-31 06:32:21 EET	1024	Allocated	Allocated
NetHood				2008-01-30 07:30:28 EET	2008-01-31 06:32:21 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated
PrintHood				2008-01-30 07:30:28 EET	2008-01-31 06:32:21 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated
Recent				2008-01-30 16:42:45 EET	2008-01-30 16:42:45 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated
SendTo				2008-01-31 06:32:26 EET	2008-01-31 06:32:26 EET	2008-01-30 16:26:39 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated

Metadata
Name: **Drive Type**
Type: REG_DWORD

Value
0x2

Screenshot 9 0x2 value

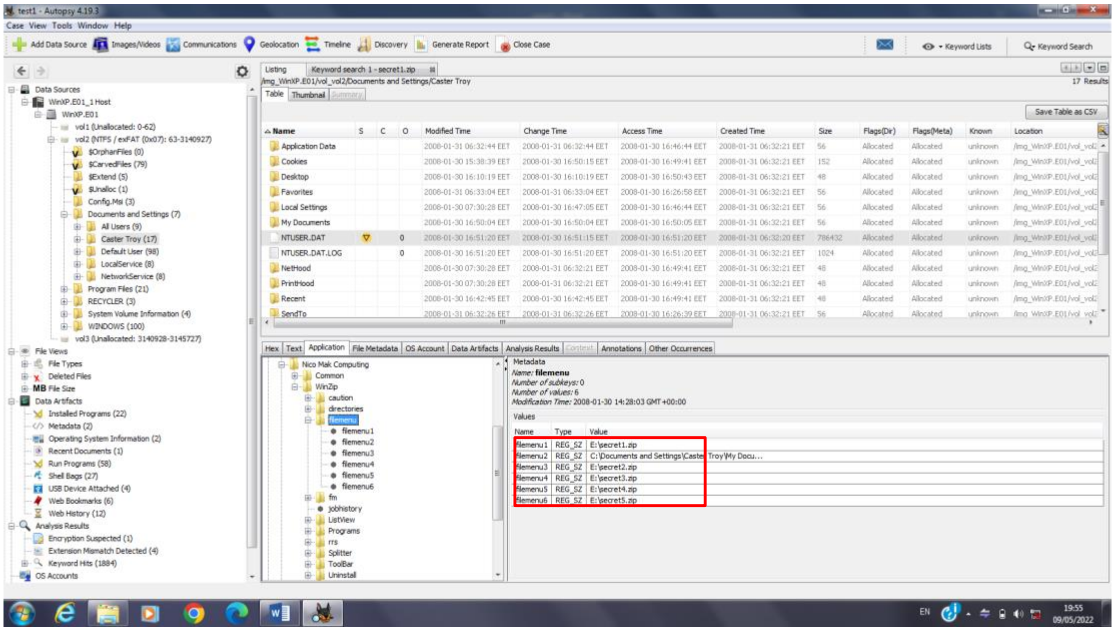
Table 6 Drive Value

Value	Meaning
0 (0 x 0)	Unknown
1 (0 x 2)	No Root directory
2 (0 x 2)	Removable disk
3 (0 x 3)	Local disk
4 (0 x 4)	Network drive
5 (0 x 5)	Compact disk
6 (0 x 6)	RAM disk

4 – WINZIP

Location: Software/NicoMakComputing /Winzip/filemenu

As shown screenshot 12, all secret files were accessed from E:\. This means that Troy accessed the files from another drive than the local one.



/img_WinXP.E01/vol_vol2/Documents and Settings/Caster Troy

17 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Application Data				2008-01-31 06:32:44 EET	2008-01-31 06:32:44 EET	2008-01-30 16:46:44 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
Cookies				2008-01-30 15:38:39 EET	2008-01-30 16:50:15 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	152	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
Desktop				2008-01-30 16:10:19 EET	2008-01-30 16:10:19 EET	2008-01-30 16:50:43 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
Favorites				2008-01-31 06:33:04 EET	2008-01-31 06:33:04 EET	2008-01-30 16:26:58 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
Local Settings				2008-01-30 07:30:28 EET	2008-01-30 16:47:05 EET	2008-01-30 16:46:44 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
My Documents				2008-01-30 16:50:04 EET	2008-01-30 16:50:04 EET	2008-01-30 16:50:05 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
NTUSER.DAT	▽		0	2008-01-30 16:51:20 EET	2008-01-30 16:51:15 EET	2008-01-30 16:51:20 EET	2008-01-31 06:32:20 EET	786432	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
NTUSER.DAT.LOG			0	2008-01-30 16:51:20 EET	2008-01-30 16:51:20 EET	2008-01-30 16:51:20 EET	2008-01-31 06:32:21 EET	1024	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
NetHood				2008-01-30 07:30:28 EET	2008-01-31 06:32:21 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
PrintHood				2008-01-30 07:30:28 EET	2008-01-31 06:32:21 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
Recent				2008-01-30 16:42:45 EET	2008-01-30 16:42:45 EET	2008-01-30 16:49:41 EET	2008-01-31 06:32:21 EET	48	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2
SendTo				2008-01-31 06:32:26 EET	2008-01-31 06:32:26 EET	2008-01-30 16:26:39 EET	2008-01-31 06:32:21 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2

Metadata

Name: **filemenu**
Number of subkeys: 0
Number of values: 6
Modification Time: 2008-01-30 14:28:03 GMT +00:00

Values

Name	Type	Value
filemenu1	REG_SZ	E:\secret1.zip
filemenu2	REG_SZ	C:\Documents and Settings\Caster Troy\My Docu...
filemenu3	REG_SZ	E:\secret2.zip
filemenu4	REG_SZ	E:\secret3.zip
filemenu5	REG_SZ	E:\secret4.zip
filemenu6	REG_SZ	E:\secret5.zip

Screenshot 10 Winzip filemenu

The values within this subkey will show what ZIP files were created using WinZIP. As you can see, there was only 5 ZIP files that Troy created using WinZIP.

EVIDENCE CLASS 3

EXHIBIT C

Table 7 shows information about "system". This file contains very important information that will be discussed below.

Table 7 system

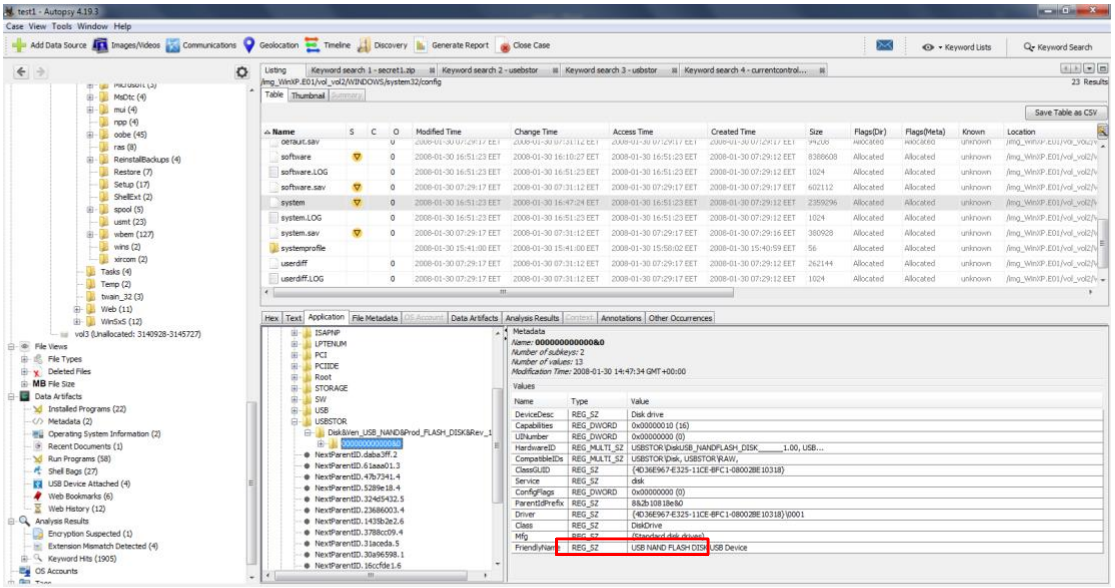
Item	WinXP.E01
File Name	System
Path	/Img_WinXP.E01/vol_vol2/WINDOWS/system32/config/system/
Hash Value	MD5: 693f9a21b6552ae94ff6f2f7c8fee0fb SHA-256: e507a8369ba73b46fb4ce2f42924b75c0c6dc30d4f03328e4e9b01b88e9a8062

Created time	2008-01-30 07:29:12 EET
Accessed time	2008-01-30 16:51:23 EET
Modified time	2008-01-30 16:51:23 EET

1 – USBSTOR

Location: ControlSet/Enum/USBSTOR

The USBSTOR key keeps a list of all USB storage devices that have ever been plugged into the system. It shows the USB device name, vendor name (manufacturer name), etc. As shown in screenshot 13, the name of the USB is "USB NAND FLASH DISK USB", which is the one probably used to transfer the documents on.



/img_WinXP.E01/vol_vol2/WINDOWS/system32/config

23 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
software	▽		0	2008-01-30 16:51:23 EET	2008-01-30 16:10:27 EET	2008-01-30 16:51:23 EET	2008-01-30 07:29:12 EET	8388608	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2/\
software.LOG			0	2008-01-30 16:51:23 EET	2008-01-30 16:51:23 EET	2008-01-30 16:51:23 EET	2008-01-30 07:29:12 EET	1024	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2/\
software.sav	▽		0	2008-01-30 07:29:17 EET	2008-01-30 07:31:12 EET	2008-01-30 07:29:17 EET	2008-01-30 07:29:17 EET	602112	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2/\
system	▽		0	2008-01-30 16:51:23 EET	2008-01-30 16:47:24 EET	2008-01-30 16:51:23 EET	2008-01-30 07:29:12 EET	2359296	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2/\
system.LOG			0	2008-01-30 16:51:23 EET	2008-01-30 16:51:23 EET	2008-01-30 16:51:23 EET	2008-01-30 07:29:12 EET	1024	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2/\
system.sav	▽		0	2008-01-30 07:29:17 EET	2008-01-30 07:31:12 EET	2008-01-30 07:29:17 EET	2008-01-30 07:29:16 EET	380928	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2/\
systemprofile				2008-01-30 15:41:00 EET	2008-01-30 15:41:00 EET	2008-01-30 15:58:02 EET	2008-01-30 15:40:59 EET	56	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2/\
userdiff			0	2008-01-30 07:29:17 EET	2008-01-30 07:31:12 EET	2008-01-30 07:29:17 EET	2008-01-30 07:29:12 EET	262144	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2/\
userdiff.LOG			0	2008-01-30 07:29:17 EET	2008-01-30 07:31:12 EET	2008-01-30 07:29:17 EET	2008-01-30 07:29:12 EET	1024	Allocated	Allocated	unknown	/img_WinXP.E01/vol_vol2/\

Metadata

Name: **000000000000&0**
Number of subkeys: 2
Number of values: 13
Modification Time: 2008-01-30 14:47:34 GMT +00:00

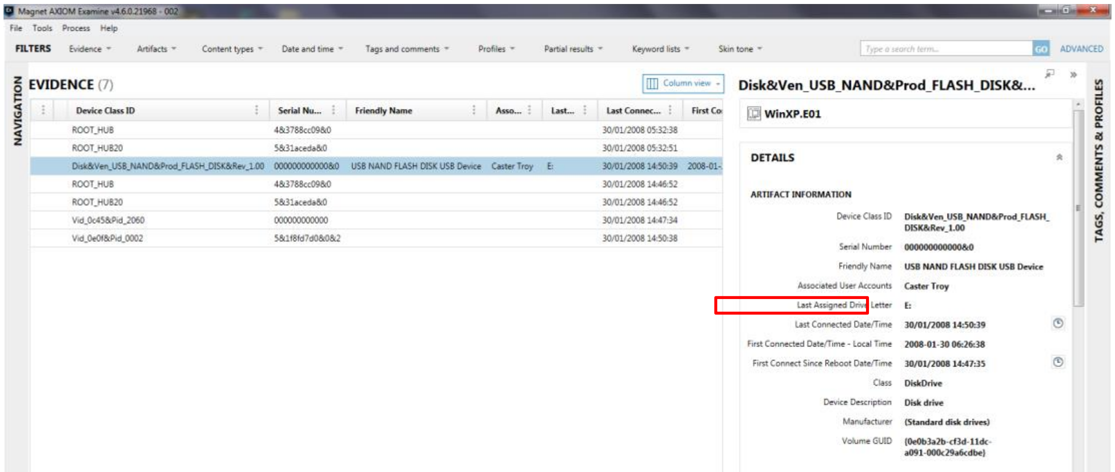
Values

Name	Type	Value
DeviceDesc	REG_SZ	Disk drive
Capabilities	REG_DWORD	0x00000010 (16)
UINumber	REG_DWORD	0x00000000 (0)
HardwareID	REG_MULTI_SZ	USBSTOR\DiskUSB_NANDFLASH_DISK______1.00, USB...
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk, USBSTOR\RAW,
ClassGUID	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}
Service	REG_SZ	disk
ConfigFlags	REG_DWORD	0x00000000 (0)
ParentIdPrefix	REG_SZ	8&2b10818e&0
Driver	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}\0001
Class	REG_SZ	DiskDrive
Mfg	REG_SZ	(Standard disk drives)
FriendlyName	REG_SZ	USB NAND FLASH DISK USB Device

Screenshot 11 USBSTOR

EXHIBIT D

In Axiom, more details were given on the same USB, as shown in screenshot 14. It shows that the Last assigned drive letter was E:. As previously mentioned, that the secret zip files were also assigned to the letter E: which proves that Troy did in fact copy these documents.



EVIDENCE (7)

Device Class ID	Serial Nu...	Friendly Name	Asso...	Last...	Last Connec...	First Co
ROOT_HUB	4&3788cc09&0				30/01/2008 05:32:38	
ROOT_HUB20	5&31aceda&0				30/01/2008 05:32:51	
Disk&Ven_USB_NAND&Prod_FLASH_DISK&Rev_1.00	000000000000&0	USB NAND FLASH DISK USB Device	Caster Troy	E:	30/01/2008 14:50:39	2008-01-
ROOT_HUB	4&3788cc09&0				30/01/2008 14:46:52	
ROOT_HUB20	5&31aceda&0				30/01/2008 14:46:52	
Vid_0c45&Pid_2060	000000000000				30/01/2008 14:47:34	
Vid_0e0f&Pid_0002	5&1f8fd7d0&0&2				30/01/2008 14:50:38	

Disk&Ven_USB_NAND&Prod_FLASH_DISK&...

WinXP.E01

DETAILS

ARTIFACT INFORMATION

Device Class ID	Disk&Ven_USB_NAND&Prod_FLASH_DISK&Rev_1.00
Serial Number	000000000000&0
Friendly Name	USB NAND FLASH DISK USB Device
Associated User Accounts	Caster Troy
Last Assigned Drive Letter	E:
Last Connected Date/Time	30/01/2008 14:50:39
First Connected Date/Time - Local Time	2008-01-30 06:26:38
First Connect Since Reboot Date/Time	30/01/2008 14:47:35
Class	DiskDrive
Device Description	Disk drive
Manufacturer	(Standard disk drives)
Volume GUID	{0e0b3a2b-cf3d-11dc-a091-000c29a6cdbe}

Screenshot 12 USB Axiom

EVIDENCE CLASS 4

In this section, we'll look at the evidence found in Mobile.zip. Numerous confusing details that I noticed include:

- The time gap is tremendously huge. The actions happened in the year 2008 in WinXP.E01. However, in Mobile.zip it happened in the year 2017.
- The suspicious text messages that will be discussed later are incoming to the device, meaning that it was send to the suspect not from the suspect.

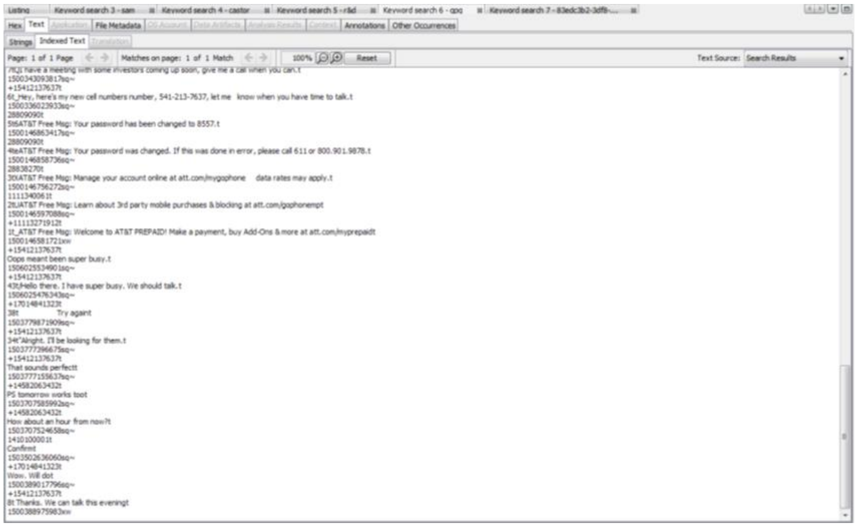
EXHIBIT D

Table 8 shows information about "smsBackup". This file contains very important information that will be discussed below.

Table 8 smsBackup

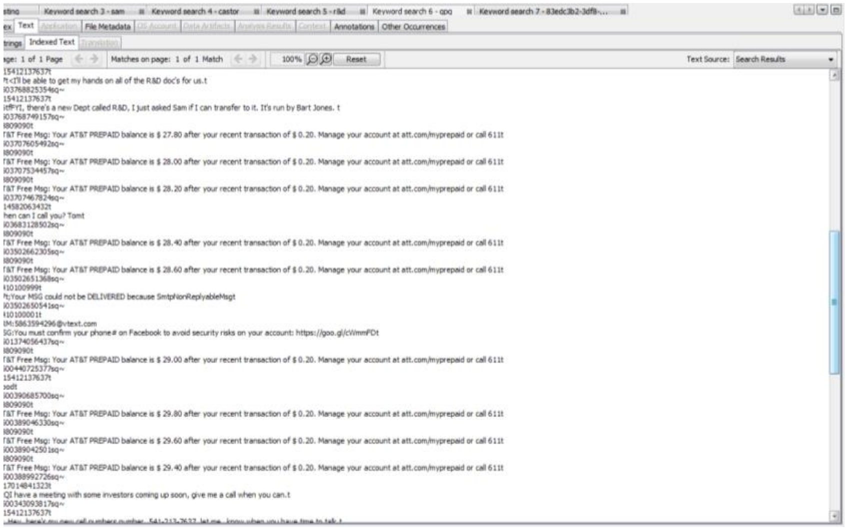
Item	Mobile.zip
File Name	smsBackup
Path	/LogicalFileSet1/logical files/apps/com.android.mms/f/smsBackup
Hash Value	MD5: e0f4bf6a55df71ca5504573e0b16317a SHA-256: fd634a421290f3c5ea7154e03437fed2dad71b1976282e46944d6e29ed6a7259

The following screenshots show all incoming and outgoing messages on the phone between the insider and the outsider. Those text messages are explained in detail in the coming section.



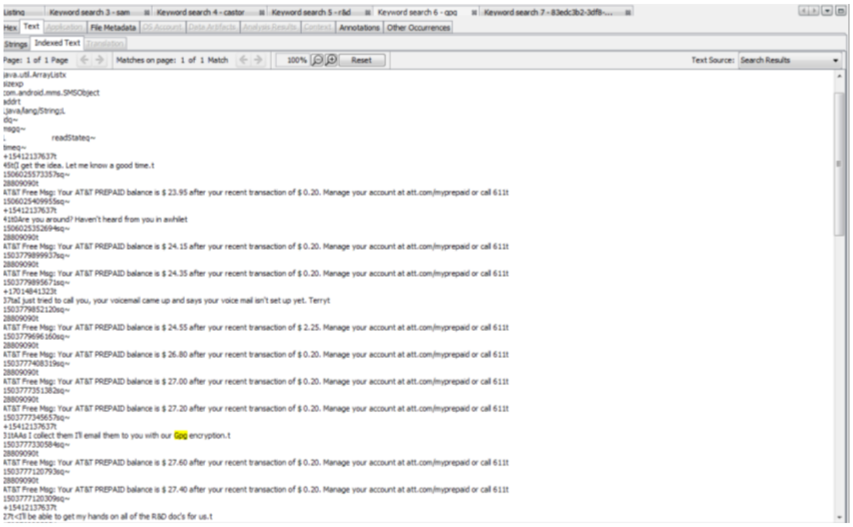
```
7tQI have a meeting with some investors coming up soon, give me a call when you can.t
1500343093817sq~
+15412137637t
6t_Hey, here's my new cell numbers number, 541-213-7637, let me   know when you have time to talk.t
1500336023933sq~
28809090t
5t6AT&T Free Msg: Your password has been changed to 8557.t
1500146863417sq~
28809090t
4teAT&T Free Msg: Your password was changed. If this was done in error, please call 611 or 800.901.9878.t
1500146858736sq~
28838270t
3tXAT&T Free Msg: Manage your account online at att.com/mygophone     data rates may apply.t
1500146756272sq~
1111340061t
2tUAT&T Free Msg: Learn about 3rd party mobile purchases & blocking at att.com/gophonempt
1500146597088sq~
+11113271912t
1t_AT&T Free Msg: Welcome to AT&T PREPAID! Make a payment, buy Add-Ons & more at att.com/myprepaidt
1500146581721xw
+15412137637t
Oops meant been super busy.t
1506025534901sq~
+15412137637t
43t/Hello there. I have super busy. We should talk.t
1506025476343sq~
+17014841323t
38t                Try againt
1503779871909sq~
+15412137637t
34t"Alright. I'll be looking for them.t
1503777296675sq~
+15412137637t
That sounds perfectt
1503777155637sq~
+14582063432t
PS tomorrow works toot
1503707585992sq~
+14582063432t
How about an hour from now?t
1503707524658sq~
14101000001t
Confirmt
1503502636060sq~
+17014841323t
Wow. Will dot
1500389017796sq~
+15412137637t
8t Thanks. We can talk this eveningt
1500388975983xw
```

Screenshot 13 smsBackup1



```
15412137637t
?t<I'll be able to get my hands on all of the R&D doc's for us.t
503768825354sq~
15412137637t
ItfFYI, there's a new Dept called R&D, I just asked Sam if I can transfer to it. It's run by Bart Jones. t
503768749157sq~
8809090t
T&T Free Msg: Your AT&T PREPAID balance is $ 27.80 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
503707605492sq~
8809090t
T&T Free Msg: Your AT&T PREPAID balance is $ 28.00 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
503707534457sq~
8809090t
T&T Free Msg: Your AT&T PREPAID balance is $ 28.20 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
503707467824sq~
14582063432t
hen can I call you? Tomt
503683128502sq~
8809090t
T&T Free Msg: Your AT&T PREPAID balance is $ 28.40 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
503502662305sq~
8809090t
T&T Free Msg: Your AT&T PREPAID balance is $ 28.60 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
503502651368sq~
410100999t
?t;Your MSG could not be DELIVERED because SmtpNonReplyableMsgt
503502650541sq~
410100001t
tM:5863594296@vtext.com
SG:You must confirm your phone# on Facebook to avoid security risks on your account: https://goo.gl/cWmmFDt
501374056437sq~
8809090t
T&T Free Msg: Your AT&T PREPAID balance is $ 29.00 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
500440725377sq~
15412137637t
oodt
500390685700sq~
8809090t
T&T Free Msg: Your AT&T PREPAID balance is $ 29.80 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
500389046330sq~
8809090t
T&T Free Msg: Your AT&T PREPAID balance is $ 29.60 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
500389042501sq~
8809090t
T&T Free Msg: Your AT&T PREPAID balance is $ 29.40 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
500388992726sq~
17014841323t
QI have a meeting with some investors coming up soon, give me a call when you can.t
500343093817sq~
15412137637t
_Hey, here's my new cell numbers number, 541-213-7637, let me   know when you have time to talk.t
```

Screenshot 14 smsBackup2



```
java.util.ArrayListx
sizexp
com.android.mms.SMSObject
addrt
Ljava/lang/String;L
dq~
msgq~
L         readStateq~
timeq~
+15412137637t
45t(I get the idea. Let me know a good time.t
1506025573357sq~
28809090t
AT&T Free Msg: Your AT&T PREPAID balance is $ 23.95 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
1506025409955sq~
+15412137637t
41t0Are you around? Haven't heard from you in awhilet
1506025352694sq~
28809090t
AT&T Free Msg: Your AT&T PREPAID balance is $ 24.15 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
1503779899937sq~
28809090t
AT&T Free Msg: Your AT&T PREPAID balance is $ 24.35 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
1503779895671sq~
+17014841323t
37taI just tried to call you, your voicemail came up and says your voice mail isn't set up yet. Terryt
1503779852120sq~
28809090t
AT&T Free Msg: Your AT&T PREPAID balance is $ 24.55 after your recent transaction of $ 2.25. Manage your account at att.com/myprepaid or call 611t
1503779696160sq~
28809090t
AT&T Free Msg: Your AT&T PREPAID balance is $ 26.80 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
1503777408319sq~
28809090t
AT&T Free Msg: Your AT&T PREPAID balance is $ 27.00 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
1503777351382sq~
28809090t
AT&T Free Msg: Your AT&T PREPAID balance is $ 27.20 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
1503777345657sq~
+15412137637t
31tAAs I collect them I'll email them to you with our Gpg encryption.t
1503777330584sq~
28809090t
AT&T Free Msg: Your AT&T PREPAID balance is $ 27.60 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
1503777120793sq~
28809090t
AT&T Free Msg: Your AT&T PREPAID balance is $ 27.40 after your recent transaction of $ 0.20. Manage your account at att.com/myprepaid or call 611t
1503777120309sq~
+15412137637t
27t<I'll be able to get my hands on all of the R&D doc's for us.t
```

Screenshot 15 smsBackup3

EVIDENCE CLASS 5

EXHIBIT E

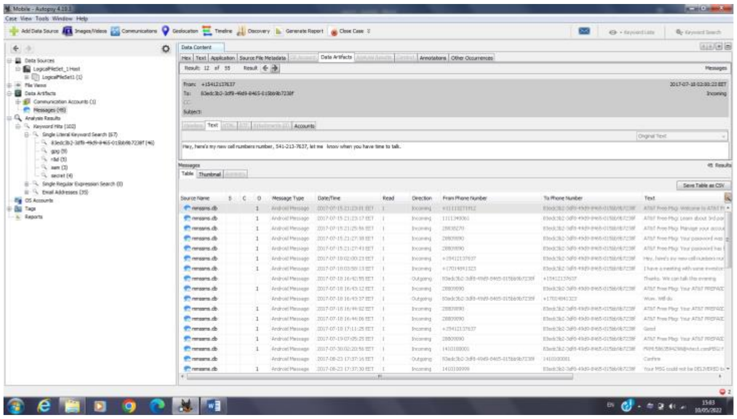
Table 18 shows information about the file "Message Artifacts". This file contains very crucial information including incoming/outgoing messages that were on the employee's device.

Item	Mobile.zip
File Name	Message Artifacts
Path	/LogicalFileSet1/logical files/apps/com.android.providers.telephony/db/mmssms.db
Hash Value	MD5: 67f7380755d7912624b46d9ba4831a56 SHA-256: c0ea5967b1996ac5f1a827b2d4f1b2ac9744f77ab09d5c775efc3818f929a13f

Screenshot 16 Message Artifacts

To obtain all these important SMS messages and its data including – date and time, who sent it, who was it sent to, I executed the following steps:

1. I tagged all message types.



Result: 12 of 55 Result

Messages

From: +15412137637 2017-07-18 02:00:23 EET

To: 83edc3b2-3df8-49d9-8465-015bb9b7238f Incoming

CC:

Subject:

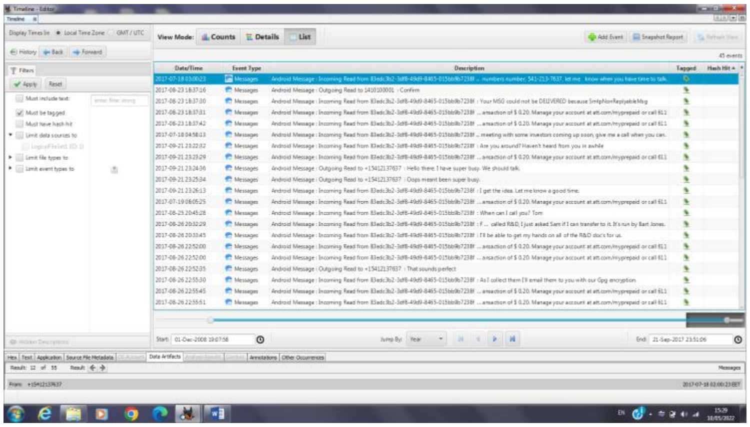
Hey, here's my new cell numbers number, 541-213-7637, let me know when you have time to talk.

Messages 45 Results

Source Name	S	C	O	Message Type	Date/Time	Read	Direction	From Phone Number	To Phone Number	Text
mmssms.db			1	Android Message	2017-07-15 21:23:01 EET	1	Incoming	+31113271912	83edc3b2-3df8-49d9-8465-015bb9b7238f	AT&T Free Msg: Welcome to AT&T Pr
mmssms.db			1	Android Message	2017-07-15 21:23:17 EET	1	Incoming	1111340061	83edc3b2-3df8-49d9-8465-015bb9b7238f	AT&T Free Msg: Learn about 3rd par
mmssms.db			1	Android Message	2017-07-15 21:25:56 EET	1	Incoming	28838270	83edc3b2-3df8-49d9-8465-015bb9b7238f	AT&T Free Msg: Manage your accou
mmssms.db			1	Android Message	2017-07-15 21:27:38 EET	1	Incoming	28809890	83edc3b2-3df8-49d9-8465-015bb9b7238f	AT&T Free Msg: Your password was
mmssms.db			1	Android Message	2017-07-15 21:27:43 EET	1	Incoming	28809890	83edc3b2-3df8-49d9-8465-015bb9b7238f	AT&T Free Msg: Your password has
mmssms.db			1	Android Message	2017-07-18 02:00:23 EET	1	Incoming	+15412137637	83edc3b2-3df8-49d9-8465-015bb9b7238f	Hey, here's my new cell numbers nu
mmssms.db			1	Android Message	2017-07-18 03:58:13 EET	1	Incoming	+17014941323	83edc3b2-3df8-49d9-8465-015bb9b7238f	I have a meeting with some investor
mmssms.db				Android Message	2017-07-18 16:42:55 EET	1	Outgoing	83edc3b2-3df8-49d9-8465-015bb9b7238f	+15412137637	Thanks. We can talk this evening
mmssms.db			1	Android Message	2017-07-18 16:43:12 EET	1	Incoming	28809890	83edc3b2-3df8-49d9-8465-015bb9b7238f	AT&T Free Msg: Your AT&T PREPAID
mmssms.db				Android Message	2017-07-18 16:43:37 EET	1	Outgoing	83edc3b2-3df8-49d9-8465-015bb9b7238f	+17014941323	Wow. Will do
mmssms.db			1	Android Message	2017-07-18 16:44:02 EET	1	Incoming	28809890	83edc3b2-3df8-49d9-8465-015bb9b7238f	AT&T Free Msg: Your AT&T PREPAID
mmssms.db			1	Android Message	2017-07-18 16:44:06 EET	1	Incoming	28809890	83edc3b2-3df8-49d9-8465-015bb9b7238f	AT&T Free Msg: Your AT&T PREPAID
mmssms.db			1	Android Message	2017-07-18 17:11:25 EET	1	Incoming	+15412137637	83edc3b2-3df8-49d9-8465-015bb9b7238f	Good
mmssms.db			1	Android Message	2017-07-19 07:05:25 EET	1	Incoming	28809890	83edc3b2-3df8-49d9-8465-015bb9b7238f	AT&T Free Msg: Your AT&T PREPAID
mmssms.db			1	Android Message	2017-07-30 02:20:56 EET	1	Incoming	1410100001	83edc3b2-3df8-49d9-8465-015bb9b7238f	FRM:5863594298@vtext.com?BS:?
mmssms.db				Android Message	2017-08-23 17:37:16 EET	1	Outgoing	83edc3b2-3df8-49d9-8465-015bb9b7238f	1410100001	Confirm
mmssms.db			1	Android Message	2017-08-23 17:37:30 EET	1	Incoming	1410100999	83edc3b2-3df8-49d9-8465-015bb9b7238f	Your MSG could not be DELIVERED b

Screenshot 17 Message tags

2. I then created a timeline and filtered out all untagged docs.



☐ Must include text: enter filter string

☑ Must be tagged

☐ Must have hash hit

45 events

Date/Time	Event Type	Description	Tagged	Hash Hit
2017-07-18 03:00:23	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f ... numbers number, 541-213-7637, let me know when you have time to talk.	✓	
2017-08-23 18:37:16	Messages	Android Message : Outgoing Read to 1410100001 : Confirm	✓	
2017-08-23 18:37:30	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : Your MSG could not be DELIVERED because SmtpNonReplyableMsg	✓	
2017-08-23 18:37:31	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f ...ansaction of $ 0.20. Manage your account at att.com/myprepaid or call 611	✓	
2017-08-23 18:37:42	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f ...ansaction of $ 0.20. Manage your account at att.com/myprepaid or call 611	✓	
2017-07-18 04:58:13	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f ... meeting with some investors coming up soon, give me a call when you can.	✓	
2017-09-21 23:22:32	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : Are you around? Haven't heard from you in awhile	✓	
2017-09-21 23:23:29	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f ...ansaction of $ 0.20. Manage your account at att.com/myprepaid or call 611	✓	
2017-09-21 23:24:36	Messages	Android Message : Outgoing Read to +15412137637 : Hello there. I have super busy. We should talk.	✓	
2017-09-21 23:25:34	Messages	Android Message : Outgoing Read to +15412137637 : Oops meant been super busy.	✓	
2017-09-21 23:26:13	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : I get the idea. Let me know a good time.	✓	
2017-07-19 08:05:25	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f ...ansaction of $ 0.20. Manage your account at att.com/myprepaid or call 611	✓	
2017-08-23 20:45:28	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : When can I call you? Tom	✓	
2017-08-26 20:32:29	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : F... called R&D, I just asked Sam if I can transfer to it. It's run by Bart Jones.	✓	
2017-08-26 20:33:45	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : I'll be able to get my hands on all of the R&D doc's for us.	✓	
2017-08-26 22:52:00	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f ...ansaction of $ 0.20. Manage your account at att.com/myprepaid or call 611	✓	
2017-08-26 22:52:00	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f ...ansaction of $ 0.20. Manage your account at att.com/myprepaid or call 611	✓	
2017-08-26 22:52:35	Messages	Android Message : Outgoing Read to +15412137637 : That sounds perfect	✓	
2017-08-26 22:55:30	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : As I collect them I'll email them to you with our Gpg encryption.	✓	
2017-08-26 22:55:45	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f ...ansaction of $ 0.20. Manage your account at att.com/myprepaid or call 611	✓	
2017-08-26 22:55:51	Messages	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f ...ansaction of $ 0.20. Manage your account at att.com/myprepaid or call 611	✓	

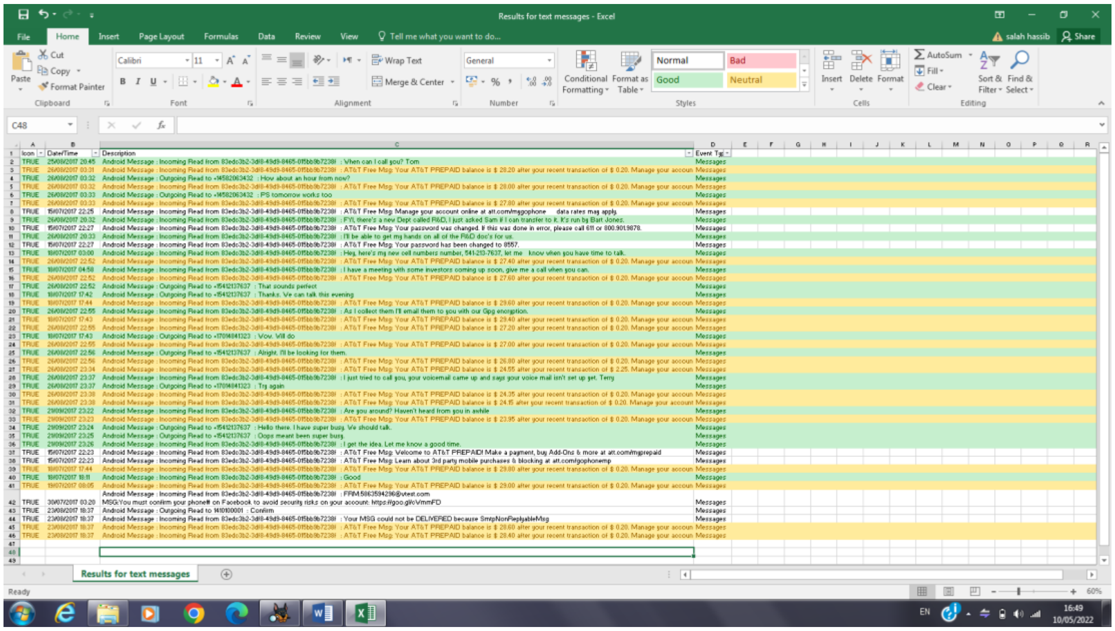
Start: 01-Dec-2008 19:07:58 End: 21-Sep-2017 23:51:06

Result: 12 of 55 Result Messages

From: +15412137637 2017-07-18 02:00:23 EET

Screenshot 18 Message timeline

3. After that, I extracted and saved the result in an excel sheet. To ease the process, I highlighted all text messages from individuals by green and all text messages from telecommunication companies by yellow.



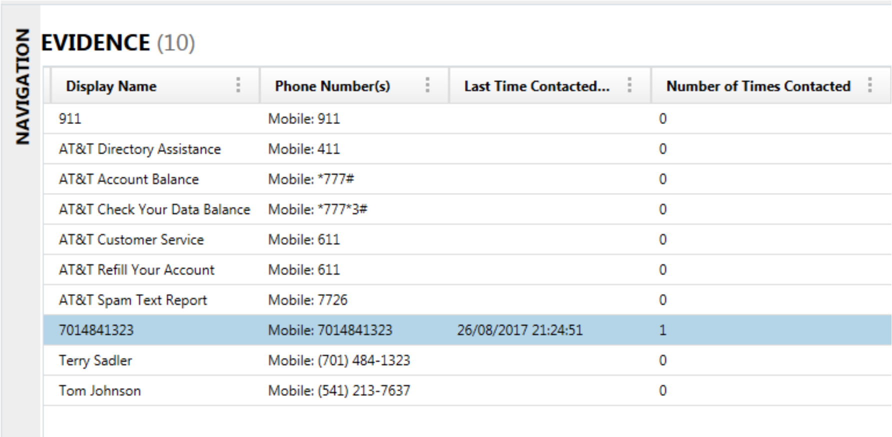
	Icon	Date/Time	Description	Event Tg
2	TRUE	25/08/2017 20:45	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : When can I call you? Tom	Messages
3	TRUE	26/08/2017 03:31	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 28.20 after your recent transaction of $ 0.20. Manage your accoun	Messages
4	TRUE	26/08/2017 03:32	Android Message : Outgoing Read to +14582063432 : How about an hour from now?	Messages
5	TRUE	26/08/2017 03:32	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 28.00 after your recent transaction of $ 0.20. Manage your accoun	Messages
6	TRUE	26/08/2017 03:33	Android Message : Outgoing Read to +14582063432 : PS tomorrow works too	Messages
7	TRUE	26/08/2017 03:33	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 27.80 after your recent transaction of $ 0.20. Manage your accoun	Messages
8	TRUE	15/07/2017 22:25	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Manage your account online at att.com/mygophone data rates may apply.	Messages
9	TRUE	26/08/2017 20:32	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : FYI, there's a new Dept called R&D, I just asked Sam if I can transfer to it. It's run by Bart Jones.	Messages
10	TRUE	15/07/2017 22:27	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your password was changed. If this was done in error, please call 611 or 800.901.9878.	Messages
11	TRUE	26/08/2017 20:33	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : I'll be able to get my hands on all of the R&D doc's for us.	Messages
12	TRUE	15/07/2017 22:27	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your password has been changed to 8557.	Messages
13	TRUE	18/07/2017 03:00	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : Hey, here's my new cell numbers number, 541-213-7637, let me know when you have time to talk.	Messages
14	TRUE	26/08/2017 22:52	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 27.40 after your recent transaction of $ 0.20. Manage your accoun	Messages
15	TRUE	18/07/2017 04:58	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : I have a meeting with some investors coming up soon, give me a call when you can.	Messages
16	TRUE	26/08/2017 22:52	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 27.60 after your recent transaction of $ 0.20. Manage your accoun	Messages
17	TRUE	26/08/2017 22:52	Android Message : Outgoing Read to +15412137637 : That sounds perfect	Messages
18	TRUE	18/07/2017 17:42	Android Message : Outgoing Read to +15412137637 : Thanks. We can talk this evening	Messages
19	TRUE	18/07/2017 17:44	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 29.60 after your recent transaction of $ 0.20. Manage your accoun	Messages
20	TRUE	26/08/2017 22:55	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : As I collect them I'll email them to you with our Gpg encryption.	Messages
21	TRUE	18/07/2017 17:43	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 29.40 after your recent transaction of $ 0.20. Manage your accoun	Messages
22	TRUE	26/08/2017 22:55	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 27.20 after your recent transaction of $ 0.20. Manage your accoun	Messages
23	TRUE	18/07/2017 17:43	Android Message : Outgoing Read to +17014841323 : Wow. Will do	Messages
24	TRUE	26/08/2017 22:55	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 27.00 after your recent transaction of $ 0.20. Manage your accoun	Messages
25	TRUE	26/08/2017 22:56	Android Message : Outgoing Read to +15412137637 : Alright. I'll be looking for them.	Messages
26	TRUE	26/08/2017 22:56	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 26.80 after your recent transaction of $ 0.20. Manage your accoun	Messages
27	TRUE	26/08/2017 23:34	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 24.55 after your recent transaction of $ 2.25. Manage your accoun	Messages
28	TRUE	26/08/2017 23:37	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : I just tried to call you, your voicemail came up and says your voice mail isn't set up yet. Terry	Messages
29	TRUE	26/08/2017 23:37	Android Message : Outgoing Read to +17014841323 : Try again	Messages
30	TRUE	26/08/2017 23:38	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 24.35 after your recent transaction of $ 0.20. Manage your accoun	Messages
31	TRUE	26/08/2017 23:38	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 24.15 after your recent transaction of $ 0.20. Manage your account	Messages
32	TRUE	21/09/2017 23:22	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : Are you around? Haven't heard from you in awhile	Messages
33	TRUE	21/09/2017 23:23	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 23.95 after your recent transaction of $ 0.20. Manage your accoun	Messages
34	TRUE	21/09/2017 23:24	Android Message : Outgoing Read to +15412137637 : Hello there. I have super busy. We should talk.	Messages
35	TRUE	21/09/2017 23:25	Android Message : Outgoing Read to +15412137637 : Oops meant been super busy.	Messages
36	TRUE	21/09/2017 23:26	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : I get the idea. Let me know a good time.	Messages
37	TRUE	15/07/2017 22:23	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Welcome to AT&T PREPAID! Make a payment, buy Add-Ons & more at att.com/myprepaid	Messages
38	TRUE	15/07/2017 22:23	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Learn about 3rd party mobile purchases & blocking at att.com/gophonemp	Messages
39	TRUE	18/07/2017 17:44	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 29.80 after your recent transaction of $ 0.20. Manage your accoun	Messages
40	TRUE	18/07/2017 18:11	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : Good	Messages
41	TRUE	19/07/2017 08:05	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 29.00 after your recent transaction of $ 0.20. Manage your accoun	Messages
42	TRUE	30/07/2017 03:20	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : FRM:5863594296@vtest.com MSG:You must confirm your phone# on Facebook to avoid security risks on your account: https://goo.gl/xVmmFD	Messages
43	TRUE	23/08/2017 18:37	Android Message : Outgoing Read to 1410100001 : Confirm	Messages
44	TRUE	23/08/2017 18:37	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : Your MSG could not be DELIVERED because SmtpNonReplyableMsg	Messages
45	TRUE	23/08/2017 18:37	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 28.60 after your recent transaction of $ 0.20. Manage your accoun	Messages
46	TRUE	23/08/2017 18:37	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : AT&T Free Msg: Your AT&T PREPAID balance is $ 28.40 after your recent transaction of $ 0.20. Manage your accoun	Messages

Screenshot 19 Messages Excel

1 – TEXT MESSAGES

As the screenshot below illustrates the employee had someone on the outside. He was planning to get the R&D (research and development) documents by asking Sam to transfer to this particular department. Once, he is able to get these documents, he will encrypt them using Gpg and then email them to the outsider. This outsider is probably working for a competitive company.

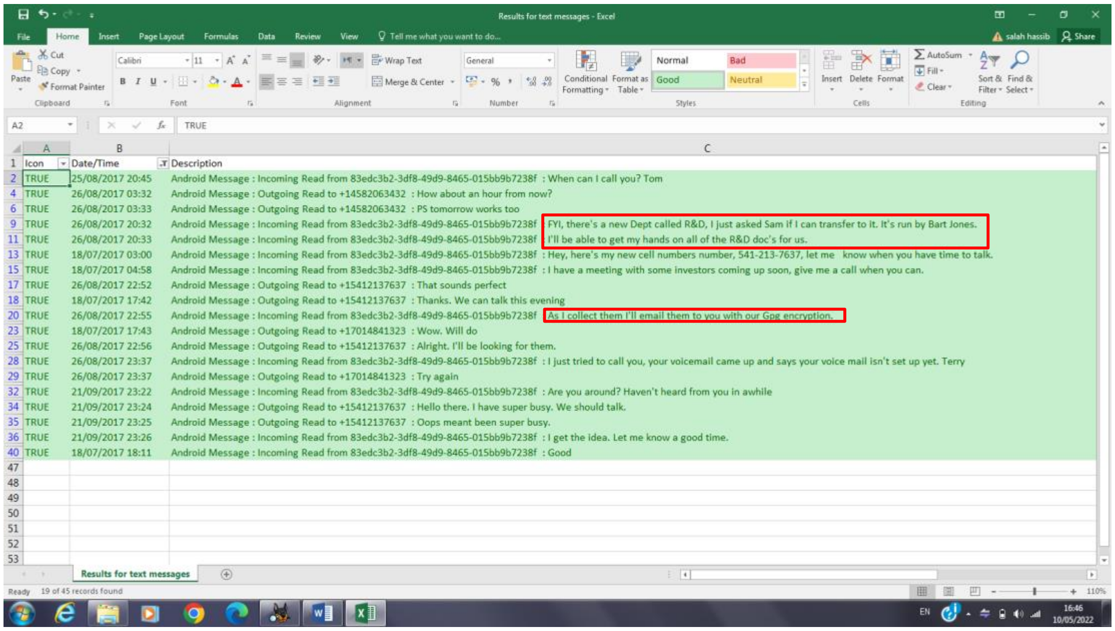
Since Autopsy could not get the contacts on the mobile, I used Axiom to get the contacts showed in screenshot 22.



EVIDENCE (10)

Display Name	Phone Number(s)	Last Time Contacted...	Number of Times Contacted
911	Mobile: 911		0
AT&T Directory Assistance	Mobile: 411		0
AT&T Account Balance	Mobile: *777#		0
AT&T Check Your Data Balance	Mobile: *777*3#		0
AT&T Customer Service	Mobile: 611		0
AT&T Refill Your Account	Mobile: 611		0
AT&T Spam Text Report	Mobile: 7726		0
7014841323	Mobile: 7014841323	26/08/2017 21:24:51	1
Terry Sadler	Mobile: (701) 484-1323		0
Tom Johnson	Mobile: (541) 213-7637		0

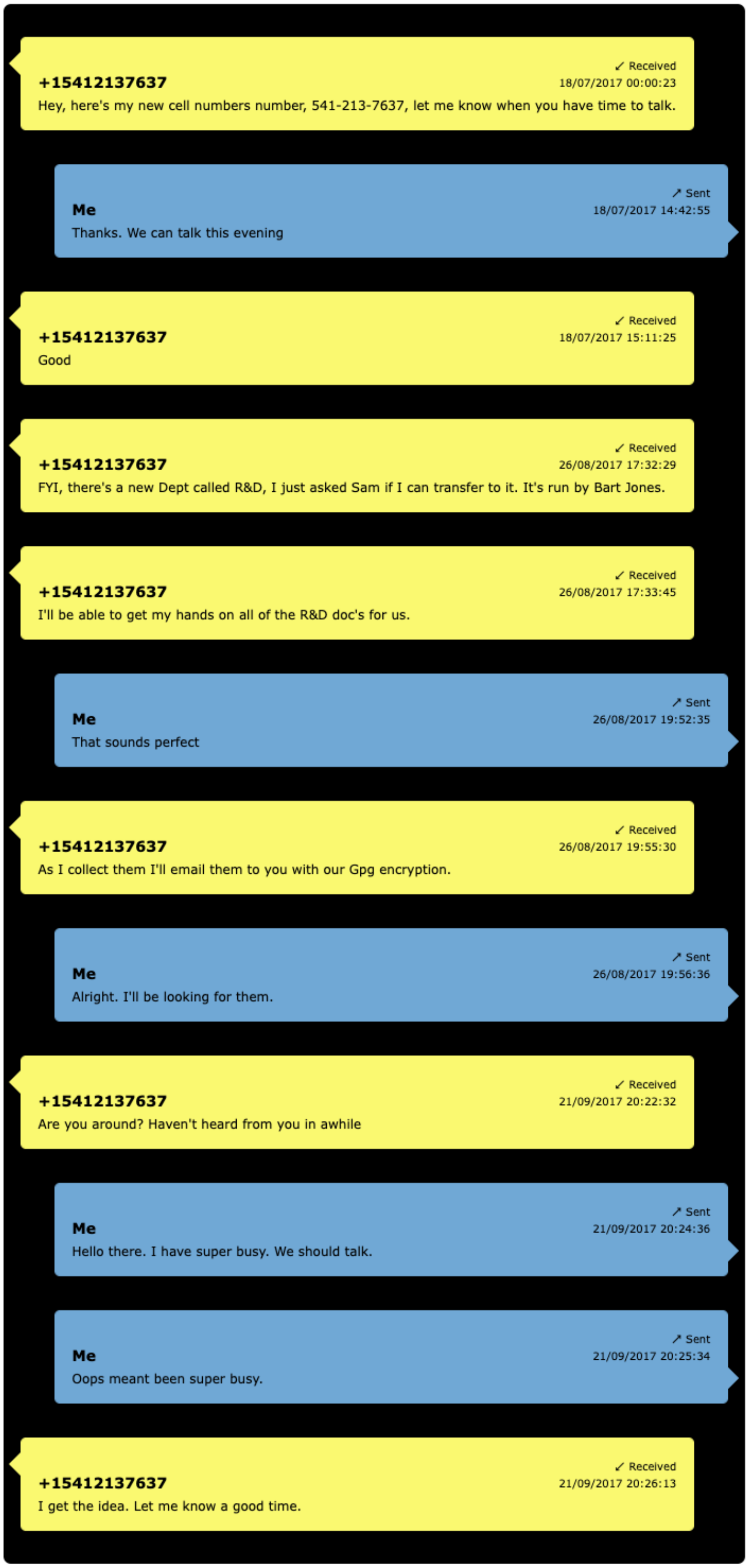
Screenshot 20 Contacts



	A	B	C
1	Icon	Date/Time	Description
2	TRUE	25/08/2017 20:45	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : When can I call you? Tom
4	TRUE	26/08/2017 03:32	Android Message : Outgoing Read to +14582063432 : How about an hour from now?
6	TRUE	26/08/2017 03:33	Android Message : Outgoing Read to +14582063432 : PS tomorrow works too
9	TRUE	26/08/2017 20:32	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : FYI, there's a new Dept called R&D, I just asked Sam if I can transfer to it. It's run by Bart Jones.
11	TRUE	26/08/2017 20:33	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : I'll be able to get my hands on all of the R&D doc's for us.
13	TRUE	18/07/2017 03:00	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : Hey, here's my new cell numbers number, 541-213-7637, let me know when you have time to talk.
15	TRUE	18/07/2017 04:58	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : I have a meeting with some investors coming up soon, give me a call when you can.
17	TRUE	26/08/2017 22:52	Android Message : Outgoing Read to +15412137637 : That sounds perfect
18	TRUE	18/07/2017 17:42	Android Message : Outgoing Read to +15412137637 : Thanks. We can talk this evening
20	TRUE	26/08/2017 22:55	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : As I collect them I'll email them to you with our Gpg encryption.
23	TRUE	18/07/2017 17:43	Android Message : Outgoing Read to +17014841323 : Wow. Will do
25	TRUE	26/08/2017 22:56	Android Message : Outgoing Read to +15412137637 : Alright. I'll be looking for them.
28	TRUE	26/08/2017 23:37	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : I just tried to call you, your voicemail came up and says your voice mail isn't set up yet. Terry
29	TRUE	26/08/2017 23:37	Android Message : Outgoing Read to +17014841323 : Try again
32	TRUE	21/09/2017 23:22	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : Are you around? Haven't heard from you in awhile
34	TRUE	21/09/2017 23:24	Android Message : Outgoing Read to +15412137637 : Hello there. I have super busy. We should talk.
35	TRUE	21/09/2017 23:25	Android Message : Outgoing Read to +15412137637 : Oops meant been super busy.
36	TRUE	21/09/2017 23:26	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : I get the idea. Let me know a good time.
40	TRUE	18/07/2017 18:11	Android Message : Incoming Read from 83edc3b2-3df8-49d9-8465-015bb9b7238f : Good

Screenshot 21 Filtered Messages

As shown in screenshots 23 & 24, the number associated with the suspicious messages is Tom Johnson. For a better view and understanding, refer to screenshot.



+15412137637 ✓ Received 18/07/2017 00:00:23
Hey, here's my new cell numbers number, 541-213-7637, let me know when you have time to talk.

Me ↗ Sent 18/07/2017 14:42:55
Thanks. We can talk this evening

+15412137637 ✓ Received 18/07/2017 15:11:25
Good

+15412137637 ✓ Received 26/08/2017 17:32:29
FYI, there's a new Dept called R&D, I just asked Sam if I can transfer to it. It's run by Bart Jones.

+15412137637 ✓ Received 26/08/2017 17:33:45
I'll be able to get my hands on all of the R&D doc's for us.

Me ↗ Sent 26/08/2017 19:52:35
That sounds perfect

+15412137637 ✓ Received 26/08/2017 19:55:30
As I collect them I'll email them to you with our Gpg encryption.

Me ↗ Sent 26/08/2017 19:56:36
Alright. I'll be looking for them.

+15412137637 ✓ Received 21/09/2017 20:22:32
Are you around? Haven't heard from you in awhile

Me ↗ Sent 21/09/2017 20:24:36
Hello there. I have super busy. We should talk.

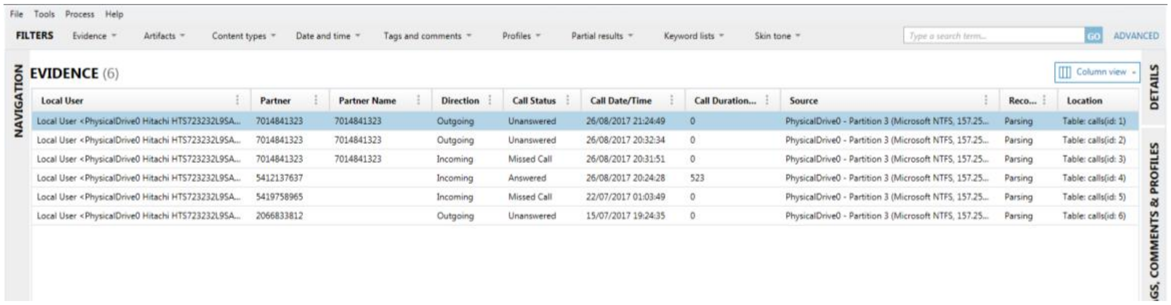
Me ↗ Sent 21/09/2017 20:25:34
Oops meant been super busy.

+15412137637 ✓ Received 21/09/2017 20:26:13
I get the idea. Let me know a good time.

Screenshot 22 Axiom Messages

2 – CALLS

As screenshot 25illustrates the employee had several calls between them, which shows that both parties, the insider and the outsider, are a part of this fraud plan. Since Autopsy could not get the call logs on the mobile, I used Axiom to get the call logs showed below in the screenshot.



EVIDENCE (6)

Local User	Partner	Partner Name	Direction	Call Status	Call Date/Time	Call Duration...	Source	Reco...	Location
Local User <PhysicalDrive0 Hitachi HTS723232L9SA...	7014841323	7014841323	Outgoing	Unanswered	26/08/2017 21:24:49	0	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 157.25...	Parsing	Table: calls(id: 1)
Local User <PhysicalDrive0 Hitachi HTS723232L9SA...	7014841323	7014841323	Outgoing	Unanswered	26/08/2017 20:32:34	0	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 157.25...	Parsing	Table: calls(id: 2)
Local User <PhysicalDrive0 Hitachi HTS723232L9SA...	7014841323	7014841323	Incoming	Missed Call	26/08/2017 20:31:51	0	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 157.25...	Parsing	Table: calls(id: 3)
Local User <PhysicalDrive0 Hitachi HTS723232L9SA...	5412137637		Incoming	Answered	26/08/2017 20:24:28	523	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 157.25...	Parsing	Table: calls(id: 4)
Local User <PhysicalDrive0 Hitachi HTS723232L9SA...	5419758965		Incoming	Missed Call	22/07/2017 01:03:49	0	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 157.25...	Parsing	Table: calls(id: 5)
Local User <PhysicalDrive0 Hitachi HTS723232L9SA...	2066833812		Outgoing	Unanswered	15/07/2017 19:24:35	0	PhysicalDrive0 - Partition 3 (Microsoft NTFS, 157.25...	Parsing	Table: calls(id: 6)

Screenshot 23 Call Logs

ANALYSIS

The evidence found in the Mobile.zip illustrates that the suspect did not only transfer the documents to an external drive (as seen previously), but also was in contact with someone outside the company and was planning to send the sensitive information out to outsiders through an encryption call GPG, which stands for "**Gnu Privacy Guard**." It is a re-write or upgrade of PGP. It does not use the IDEA encryption algorithm. This is to make it completely free. It uses the NIST AES, Advanced Encryption Standard. All the algorithm data is stored and documented publicly by OpenPGP Alliance (Kaushik, 2012).

CONCLUSION

The theory I concluded after performing this thorough examination is that Castor Troy is the employee that abruptly left the company and he was involved and complicit in accessing, copying, and transferring sensitive information. He performed this by using WinZip to compress the sensitive files from documents on his machine and copying them to a thumb drive and later emailed them, using GPG encryption, to an external individual (most likely working for a competitive company).

The power of forensic tools such as Autopsy and Axiom is tremendous. It's quite amazing all the data stored in a device can be recovered by a Forensics expert. That's the reason everyone should be carefull with their responsible data and avoid illegal actions at all times.

REFERENCES

Chad Tilbury. (2010, April 2). *Viviana Ross*. SANS Digital Forensics and Incident Response Blog | OpenSaveMRU and LastVisitedMRU | SANS Institute. Retrieved May 12, 2022, from https://www.sans.org/blog/opensavemru-and-lastvisitedmru/

Damon S. (2013, December 6). *Intellectual property theft: Analysis of the victim's devices*. Intellectual Property Theft: Analyzing The "Victim" Organization's Devices. Retrieved May 12, 2022, from https://www.vestigeltd.com/thought-leadership/intellectual-property-theft-analyzing-the-victim-organization-s-devices/

Kaushik, N. (2012, April 9). *Difference between PGP and GPG*. Difference Between Similar Terms and Objects. Retrieved May 13, 2022, from http://www.differencebetween.net/technology/software-technology/difference-between-pgp-and-gpg/#:~:text=%E2%80%9CGPG%E2%80%9D%20stands%20for%20%E2%80%9CGnu,documented%20publicly%20by%20OpenPGP%20Alliance.

Opsitnick, T. M., Anguilano, J. M., & Tucker, T. B. (2021, August 2). *Using computer forensics to investigate employee data theft*. Gertsburg Licata. Retrieved May 12, 2022, from https://www.gertsburglicata.com/blog/computer-forensics-to-investigate-employee-data-theft/

Phillips, N., & Enfinger, S. (2009). *Guide to computer forensics and investigations*. Delmar.

Pixley, L., Elwell, C., & Poirier, J. ((2019, May).). *Cal Poly: Learn by doing*. California Cybersecurity Institute. Retrieved May 12, 2022, from https://cci.calpoly.edu/

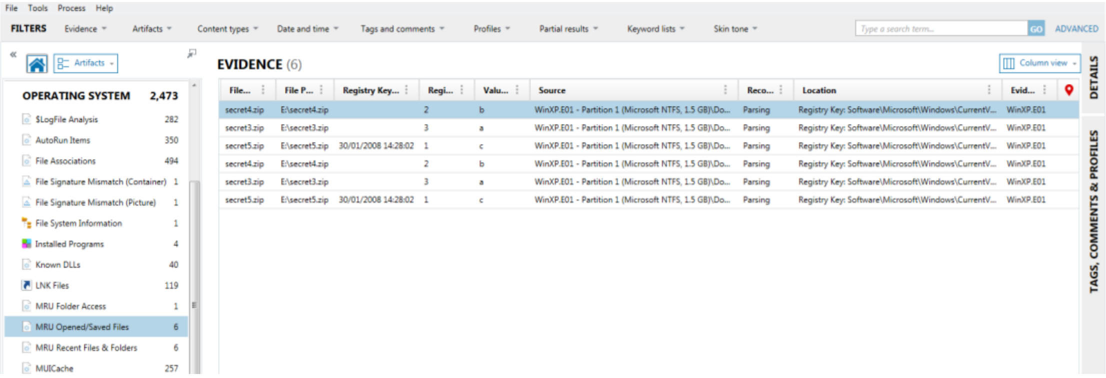
Shlomo, E. (2019, April 2). *Windows Forensics Analysis (Evidence)*. Eshlomo. Retrieved May 12, 2022, from https://www.eshlomo.us/windows-forensics-analysis-evidence/

Win32_volume class (windows). (Windows) | Microsoft Docs. (2015, August 31). Retrieved May 12, 2022, from https://docs.microsoft.com/en-us/previous-versions/windows/desktop/legacy/aa394515(v=vs.85)

Window registry. Window Registry - an overview | ScienceDirect Topics. (2017). Retrieved May 12, 2022, from https://www.sciencedirect.com/topics/computer-science/window-registry

APPENDICES

The following screenshots are MRU Opened Files and MRU Recent Files accessed from Axiom.

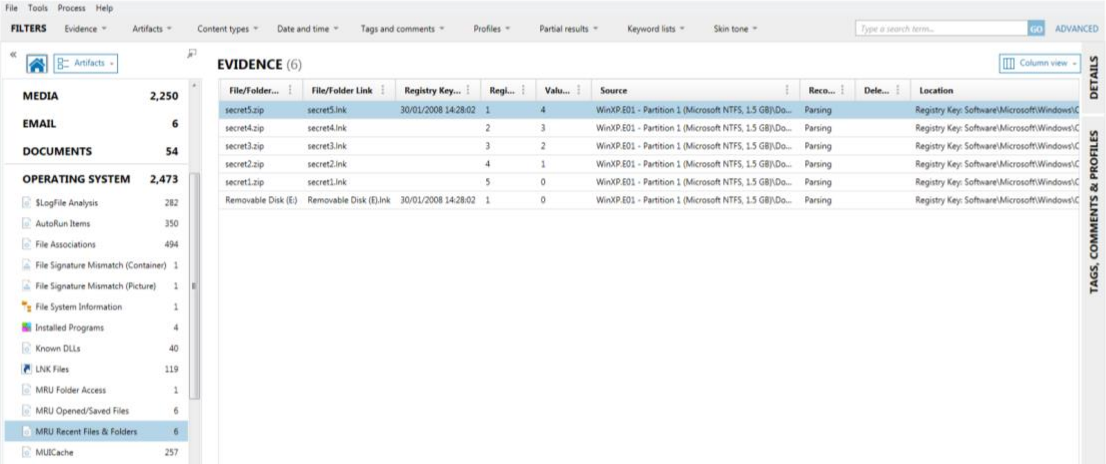

File Tools Process Help
FILTERS Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone
Type a search term... GO ADVANCED
Artifacts
Column view
DETAILS
TAGS, COMMENTS & PROFILES

OPERATING SYSTEM	2,473
$LogFile Analysis	282
AutoRun Items	350
File Associations	494
File Signature Mismatch (Container)	1
File Signature Mismatch (Picture)	1
File System Information	1
Installed Programs	4
Known DLLs	40
LNK Files	119
MRU Folder Access	1
MRU Opened/Saved Files	6
MRU Recent Files & Folders	6
MUICache	257

EVIDENCE (6)

File...	File P...	Registry Key...	Regi...	Valu...	Source	Reco...	Location	Evid...
secret4.zip	E:\secret4.zip		2	b	WinXP.E01 - Partition 1 (Microsoft NTFS, 1.5 GB)\Do...	Parsing	Registry Key: Software\Microsoft\Windows\CurrentV...	WinXP.E01
secret3.zip	E:\secret3.zip		3	a	WinXP.E01 - Partition 1 (Microsoft NTFS, 1.5 GB)\Do...	Parsing	Registry Key: Software\Microsoft\Windows\CurrentV...	WinXP.E01
secret5.zip	E:\secret5.zip	30/01/2008 14:28:02	1	c	WinXP.E01 - Partition 1 (Microsoft NTFS, 1.5 GB)\Do...	Parsing	Registry Key: Software\Microsoft\Windows\CurrentV...	WinXP.E01
secret4.zip	E:\secret4.zip		2	b	WinXP.E01 - Partition 1 (Microsoft NTFS, 1.5 GB)\Do...	Parsing	Registry Key: Software\Microsoft\Windows\CurrentV...	WinXP.E01
secret3.zip	E:\secret3.zip		3	a	WinXP.E01 - Partition 1 (Microsoft NTFS, 1.5 GB)\Do...	Parsing	Registry Key: Software\Microsoft\Windows\CurrentV...	WinXP.E01
secret5.zip	E:\secret5.zip	30/01/2008 14:28:02	1	c	WinXP.E01 - Partition 1 (Microsoft NTFS, 1.5 GB)\Do...	Parsing	Registry Key: Software\Microsoft\Windows\CurrentV...	WinXP.E01

Screenshot 24 Axiom MRUOpened


File Tools Process Help
FILTERS Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone
Type a search term... GO ADVANCED
Artifacts
Column view
DETAILS
TAGS, COMMENTS & PROFILES

MEDIA	2,250
EMAIL	6
DOCUMENTS	54
OPERATING SYSTEM	2,473
$LogFile Analysis	282
AutoRun Items	350
File Associations	494
File Signature Mismatch (Container)	1
File Signature Mismatch (Picture)	1
File System Information	1
Installed Programs	4
Known DLLs	40
LNK Files	119
MRU Folder Access	1
MRU Opened/Saved Files	6
MRU Recent Files & Folders	6
MUICache	257

EVIDENCE (6)

File/Folder...	File/Folder Link	Registry Key...	Regi...	Valu...	Source	Reco...	Dele...	Location
secret5.zip	secret5.lnk	30/01/2008 14:28:02	1	4	WinXP.E01 - Partition 1 (Microsoft NTFS, 1.5 GB)\Do...	Parsing		Registry Key: Software\Microsoft\Windows\C
secret4.zip	secret4.lnk		2	3	WinXP.E01 - Partition 1 (Microsoft NTFS, 1.5 GB)\Do...	Parsing		Registry Key: Software\Microsoft\Windows\C
secret3.zip	secret3.lnk		3	2	WinXP.E01 - Partition 1 (Microsoft NTFS, 1.5 GB)\Do...	Parsing		Registry Key: Software\Microsoft\Windows\C
secret2.zip	secret2.lnk		4	1	WinXP.E01 - Partition 1 (Microsoft NTFS, 1.5 GB)\Do...	Parsing		Registry Key: Software\Microsoft\Windows\C
secret1.zip	secret1.lnk		5	0	WinXP.E01 - Partition 1 (Microsoft NTFS, 1.5 GB)\Do...	Parsing		Registry Key: Software\Microsoft\Windows\C
Removable Disk (E:)	Removable Disk (E).lnk	30/01/2008 14:28:02	1	0	WinXP.E01 - Partition 1 (Microsoft NTFS, 1.5 GB)\Do...	Parsing		Registry Key: Software\Microsoft\Windows\C

Screenshot 25 Axiom MRU Recent Files

FORENSICS REPORT GENERATED BY FORENSIC TOOLS

I generated reports with the two tools I used. Kindly find, in the submission link, 2 .rar files attached – Axiom-reports.rar & Autopsy-reports.rar.