SCHOOL OF ARCHITECTURE, COMPUTING & ENGINEERING

MSc Information Security & Digital Forensics

Course assignment CN7019 – Digital Forensics

SUPERVISOR

Dr. LIAMBAS CHRISTOS

EDITING

MANIOS ATHANASIOS

U2020737

BANDIS CHRISTOS

U2121211

INSTITUTION

METROPOLITAN COLLEGE CAMPUS

AMAROUSIOU

May, 2023

Table of Contents

1. Case Summary

1.1. Case Information

Case name	Greg Schardt's (Mr. Evil) Case
Competent body	University of East London (UEL) - Metropolitan College
Researchers' Names	Manios Athanasios Bandis Christos
Researchers' Emails	amanios19b@amcstudent.edu.gr cbantis20b@amcstudent.edu.gr
Date of recovery of evidence	20/09/2021
Exhibits	1 Dell laptop 1 PCMCIA wireless network card 1 external 802.11b frequency antenna
Model / Serial number (laptop)	Latitude CPi / #VLQLW
Report writing date	22/05/2023

Table 1 - Case information

1.2. Overview of the case

On 20/9/2021, a Dell laptop with serial number #VLQLW was found abandoned, along with a PCMCIA wireless network card and an external 802.11b antenna. It is suspected that this laptop has been used in illegal electronic activities, although it cannot be linked to a suspect, whose first name is Gregory.

There is the unspecified information that Gregory -possibly- uses the nickname "Mr. Evil" or "Mr. Bad". Some of his accomplices confessed during the interrogation process that he intended to park his car outside of locations that would be within range of wireless access points, such as Starbucks and other T-Mobile hotspots. His goal was to intercept packets of Internet traffic to intercept usernames and passwords, as well as credit card numbers.

1.3. Taking over the case

Two "disk image" files named "4Dell Latitude CPi.E01" and "4Dell Latitude CPi.E02" were downloaded, respectively, which constitute the virtual copy of the

evidence on which the test was performed. The unique digital fingerprints (hash values) of the above files were also provided (Table 2).

Virtual disk name	Hash Value
4Dell Latitude CPi.E01	943243e71eda7481fee7b83f06698993
4Dell Latitude CPi.E02	4931253cc91dffdef5867c3dfbd99516

Table 2 - The hash values of the virtual disks

Then, the hash values of the virtual disks were matched with the given hash values. More specifically, by typing the command “certutil -hashfile (filename) md5” in “cmd” the hash value of the user-defined file is calculated. Therefore, based on the values in the image below and the table above, it is verified that the virtual disk files are true and accurate copies of the crime scene.

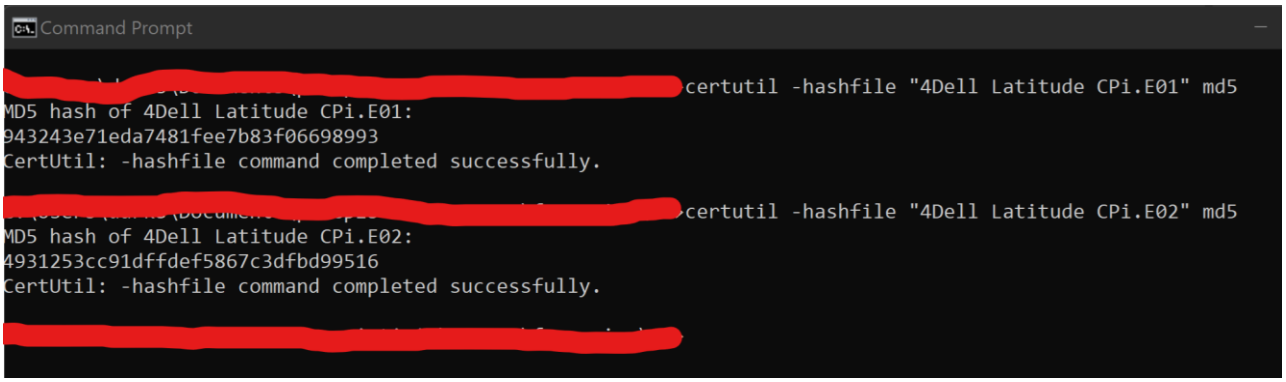

Figure 1 - Verifying the hashes of virtual disks

During the process that will be followed, from receiving the evidence to storing it in a safe place, all ACPO practices will be used, as no competent (or not) person will modify the data on the virtual disk and the processes that will take place will be recorded and maintained.

For easier reading and understanding of the content, in the rest of the report the path “/img_4Dell Latitude CPi.E01/vol_vol2/” will be replaced with “C:/”.

2. Important files

2.1. Application shortcuts in the “Tools” folder of “Desktop”

Name	123 WASP.lnk
Physical size	1024 bytes
Logical size	628 bytes
Date of creation	2004-08-20 18:13:08 EEST
Date of modification	2004-08-20 18:13:08 EEST
Date of access	2004-08-20 18:24:40 EEST

Path	C:/Documents and Settings/Mr. Evil/Desktop/Tools/123 WASP.lnk
Name	Agent.lnk
Physical size	650 bytes
Logical size	650 bytes
Date of creation	2004-08-20 18:08:19 EEST
Date of modification	2004-08-20 18:08:19 EEST
Date of access	2004-08-20 18:55:34 EEST
Path	C:/Documents and Settings/Mr. Evil/Desktop/Tools/Agent.lnk
Name	Cain v2.5.lnk
Physical size	1536 bytes
Logical size	1496 bytes
Date of creation	2004-08-20 18:06:01 EEST
Date of modification	2004-08-20 18:06:01 EEST
Date of access	2004-08-20 18:34:52 EEST
Path	C:/Documents and Settings/Mr. Evil/Desktop/Tools/Agent.lnk/Documents and Settings/Mr. Evil/Desktop/Tools/Cain v2.5.lnk
Name	CuteFTP.lnk
Physical size	1024 bytes
Logical size	827 bytes
Date of creation	2004-08-20 18:09:02 EEST
Date of modification	2004-08-20 18:09:02 EEST
Date of access	2004-08-20 18:11:12 EEST
Path	C:/Documents and Settings/Mr. Evil/Desktop/Tools/CuteFTP.lnk
Name	CuteHTML.lnk
Physical size	1024 bytes
Logical size	932 bytes
Date of creation	2004-08-20 18:09:04 EEST
Date of modification	2004-08-20 18:09:04 EEST
Date of access	2004-08-20 18:24:40 EEST
Path	C:/Documents and Settings/Mr. Evil/Desktop/Tools/CuteHTML.lnk
Name	Ethereal.lnk
Physical size	700 bytes
Logical size	700 bytes
Date of creation	2004-08-27 18:29:44 EEST
Date of modification	2004-08-27 18:29:44 EEST
Date of access	2004-08-27 18:34:54 EEST
Path	C:/Documents and Settings/Mr. Evil/Desktop/Tools/Ethereal.lnk
Name	Faber Toys.lnk
Physical size	1024 bytes
Logical size	706 bytes
Date of creation	2004-08-20 18:07:24 EEST
Date of modification	2004-08-20 18:07:24 EEST
Date of access	2004-08-25 18:27:30 EEST

Path	C:/Documents and Settings/Mr. Evil/Desktop/Tools/Faber Toys.lnk
Name	Look@Host.lnk
Physical size	2048 bytes
Logical size	1562 bytes
Date of creation	2004-08-25 18:56:11 EEST
Date of modification	2004-08-25 18:56:11 EEST
Date of access	2004-08-27 18:18:04 EEST
Path	C:/Documents and Settings/Mr. Evil/Desktop/Tools/Look@Host.lnk
Name	Look@LAN.lnk
Physical size	2048 bytes
Logical size	1555 bytes
Date of creation	2004-08-25 18:56:11 EEST
Date of modification	2004-08-25 18:56:11 EEST
Date of access	2004-08-27 18:18:04 EEST
Path	C:/Documents and Settings/Mr. Evil/Desktop/Tools/Look@LAN.lnk
Name	mIRC.lnk
Physical size	638 bytes
Logical size	638 bytes
Date of creation	2004-08-20 18:10:04 EEST
Date of modification	2004-08-20 18:09:56 EEST
Date of access	2004-08-25 19:20:24 EEST
Path	C:/Documents and Settings/Mr. Evil/Desktop/Tools/mIRC.lnk
Name	Network Stumbler.lnk
Physical size	1024 bytes
Logical size	753 bytes
Date of creation	2004-08-27 18:12:17 EEST
Date of modification	2004-08-27 18:12:17 EEST
Date of access	2004-08-27 18:12:43 EEST
Path	C:/Documents and Settings/Mr. Evil/Desktop/Tools/Network Stumbler.lnk
Name	Shortcut to whois.lnk
Physical size	1024 bytes
Logical size	638 bytes
Date of creation	2004-08-20 18:11:19 EEST
Date of modification	2004-08-20 18:11:19 EEST
Date of access	2004-08-26 18:13:56 EEST
Path	C:/Documents and Settings/Mr. Evil/Desktop/Tools/Shortcut to whois.lnk

Table 3 - Application shortcuts in the "Tools" folder of "Desktop"

2.2. Malware in the “My Documents” folder for use on various Operating Systems (NT, Unix)

Name	ARCHIVE
Size	1.97 MB
Date of creation	2004-08-20 18:18:07 EEST
Date of modification	2004-08-20 18:18:09 EEST
Date of access	2004-08-20 18:18:09 EEST
Path	C:/My Documents/ARCHIVE
Name	COMMANDS
Size	3.08 MB
Date of creation	2004-08-20 18:18:12 EEST
Date of modification	2004-08-20 18:18:16 EEST
Date of access	2004-08-20 18:18:16 EEST
Path	C:/My Documents/COMMANDS
Name	DICTIONARIES
Size	37.6 MB
Date of creation	2004-08-20 18:18:16 EEST
Date of modification	2004-08-20 18:18:41 EEST
Date of access	2004-08-20 18:18:41 EEST
Path	C:/My Documents/DICTIONARIES
Name	ENUMERATION
Size	20.7 MB
Date of creation	2004-08-20 18:18:41 EEST
Date of modification	2004-08-20 18:18:41 EEST
Date of access	2004-08-20 18:18:41 EEST
Path	C:/My Documents/ENUMERATION
Name	EXPLOITATION
Size	46.7 MB
Date of creation	2004-08-20 18:19:09 EEST
Date of modification	2004-08-20 18:19:12 EEST
Date of access	2004-08-20 18:19:12 EEST
Path	C:/My Documents/EXPLOITATION
Name	FOOTPRINTING
Size	90.2 MB
Date of creation	2004-08-20 18:19:49 EEST
Date of modification	2004-08-20 18:19:49 EEST
Date of access	2004-08-20 18:19:49 EEST
Path	C:/My Documents/FOOTPRINTING
Name	MISCELLANEOUS
Size	1.3 MB
Date of creation	2004-08-20 18:21:04 EEST
Date of modification	2004-08-20 18:21:04 EEST
Date of access	2004-08-20 18:21:04 EEST
Path	C:/My Documents/MISCELLANEOUS
Name	NOVELL
Size	2.91 MB
Date of creation	2004-08-20 18:21:05 EEST

Date of modification	2004-08-20 18:21:08 EEST
Date of access	2004-08-20 18:21:08 EEST
Path	C:/My Documents/NOVELL

Table 4 - Malware in the "My Documents" folder

3. Results of digital evidence analysis

3.1. Identification of any software directly linked to cybercrime

3.1.1 Within the folder "C:/Program Files" the following software were found (Figure 2):

- **123Wasp (Version 2.01)** - Tool to retrieve the passwords of accounts connected to a computer, which are stored in the file with the extension ".pwl" in the path "C:/Windows" (It is addressed to the versions of Windows 95, Windows 98 and Windows ME, as these files are found only in these versions - in newer versions they have been removed).
- **Anonymizer Bar 2.0** - Tool to hide the IP address for the purpose of anonymous web browsing, offering anonymous proxy servers.
- **Cain & Abel (Version 2.5)** - Password recovery tool that allows recovery of various types of passwords through network sniffing and decryption of encrypted passwords using methods such as "Dictionary", "Brute-force" and "Cryptanalysis".
- **Ethereal (Version 0.10.6)** - Network sniffing and network traffic analyzer.
- **Look@LAN (Version 2.50)** - Network monitoring tool.
- **Network Stumbler (Version 0.4.0)** - Tool that allows detecting wireless local area networks (WLAN) using 802.11a/b/g**.** Often used for "WarDriving" and targeting of directional antennas for long distance WLAN connections.

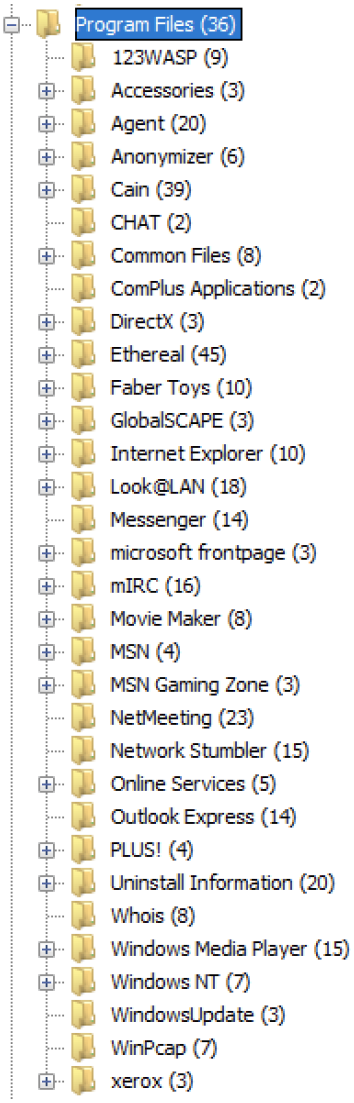

Figure 2 - The contents of the "C:/Program Files" folder

3.1.2 Within the "C:/My Documents" folder, the following auxiliary malicious toolkits were detected (Figure 3). These include sniffers, brute-force crackers, port scanners and exploits, which are categorized according to their purpose and the operating system they target:

- **ARCHIVE**
- **COMMANDS**
- **DICTIONARIES**
- **ENUMERATION**
- **EXPLOITATION**
- **FOOTPRINTING**
- **MISCELLANEOUS**

- **NOVELL**

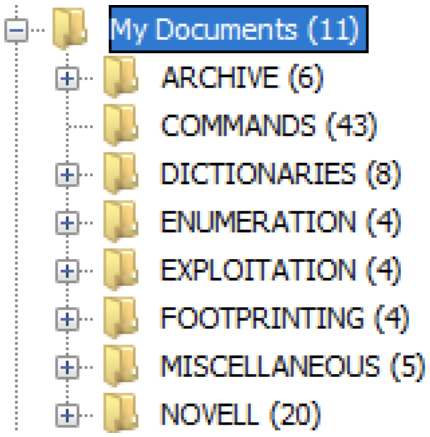

Figure 3 - The contents of the "C:/My Documents" folder

3.2. Locating evidence of the use of the above software

3.2.1. Going to the "C:/Program Files" folder and checking the creation and last access dates, the following conclusions can be drawn:

Name	Date of creation	Date of last access	Conclusion
123Wasp	2004-08-20 18:13:08 EEST	2004-08-20 18:13:08 EEST	He was never executed
Anonymizer (Folder)	2004-08-20 18:05:06 EEST	2004-08-27 18:32:07 EEST	Executed seven (7) days after installation
Anonymizer (AnonymizerBar.dll)	2002-07-12 03:31:30 EEST	2004-08-20 18:05:09 EEST	This library file appears to have been created two (2) years before the software was installed, indicating a possible software update
Cain & Abel	2004-08-20 18:05:58 EEST	2004-08-27 18:14:45 EEST	Executed seven (7) days after installation
Ethereal	2004-08-13 05:15:35 EEST	2004-08-27 18:34:54 EEST	Executed fourteen (14) days after installation
Look@LAN	2004-02-18 01:35:21 EEST	2004-08-26 17:58:49 EEST	Executed one hundred and ninety (190) days after installation
Network Stumbler	2004-04-21 10:16:58 EEST	2004-08-27 18:12:37 EEST	Executed one hundred and twenty-eight (128) days after installation

Table 5 - Evidence of the use of malware

3.2.2. Checking the Windows “prefetch” files in “C:/Windows/Prefetch”. A prefetch file is created whenever software is executed for the first time and contains data that the operating system uses to increase its performance. In the “Data Artifacts” generated by the scan of the virtual disk by the “Autopsy” tool (https://www.autopsy.com/), the “Run Programs” tab is located, which contains the set of prefetch files, providing various information, such as the number of runs for each of them (Figure 4).

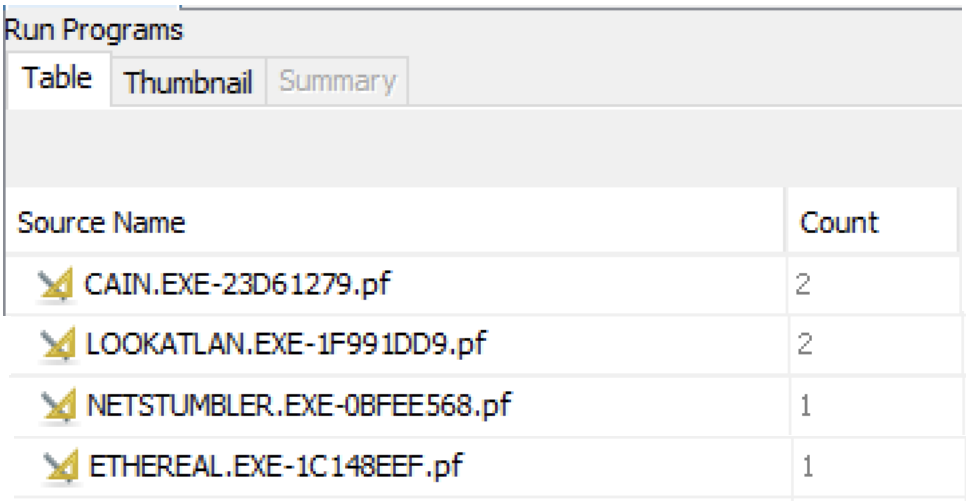

Figure 4 - The “Run Programs” tab of the “Autopsy” tool

3.2.3. Extracting the file “NTUSER.DAT” via the “Autopsy” tool from the folder “C:/Documents and Setting/Mr. Evil” and importing it into the application “UserAssist v2.6.0.0” (https://blog.didierstevens.com/programs/userassist/). Within the file, the path “NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist” contains the encrypted, with ROT-13[1], keys that display information about the execution of the software on the operating system. The number of executions of the malicious software on the virtual disk is shown below (Figure 5).

[1] Algorithm for replacing characters by 13 positions.

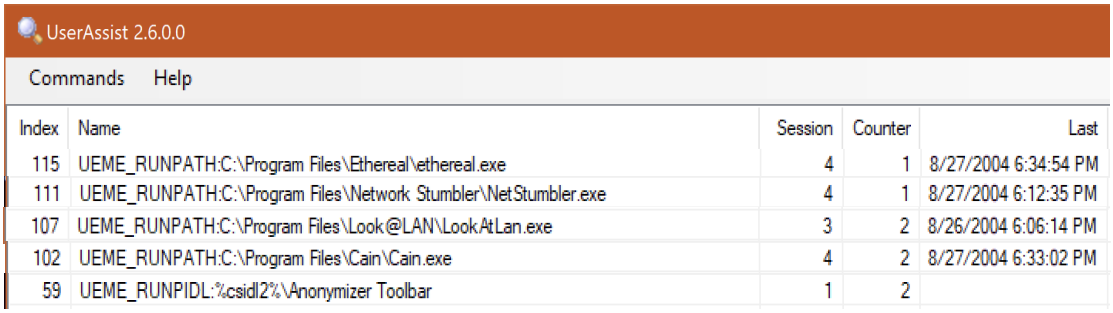

Figure 5 - The number of executions of malware on the virtual disk

It is worth mentioning that no "prefetch" file has been created for the "Anonymizer Toolbar" tool, as it is executed within the web browser.

3.3. Locating any data that may have been generated by using the above software

Name	Path	Application	Description
interception	C:\Documents and Settings\Mr. Evil\interception	Ethereal	Contains the results of the interception process
recent	C:/Documents and Settings/Mr. Evil/Application Data/Ethereal/recent	Ethereal	Generated every time the application is closed and contains the most recent settings

Table 6 - Data generated by using malware

3.4. Identification of any data that may have been intercepted

Since the "Ethereal" tool is used to perform eavesdropping, an investigation was carried out on its generated files. In the "recent" file, located in the path "C:/Documents and Settings/Mr. Evil/Application Data/Ethereal/Ethereal/recent", that stores the most recent settings, the path of the file containing information about the most recent interception was found (Figure 6).

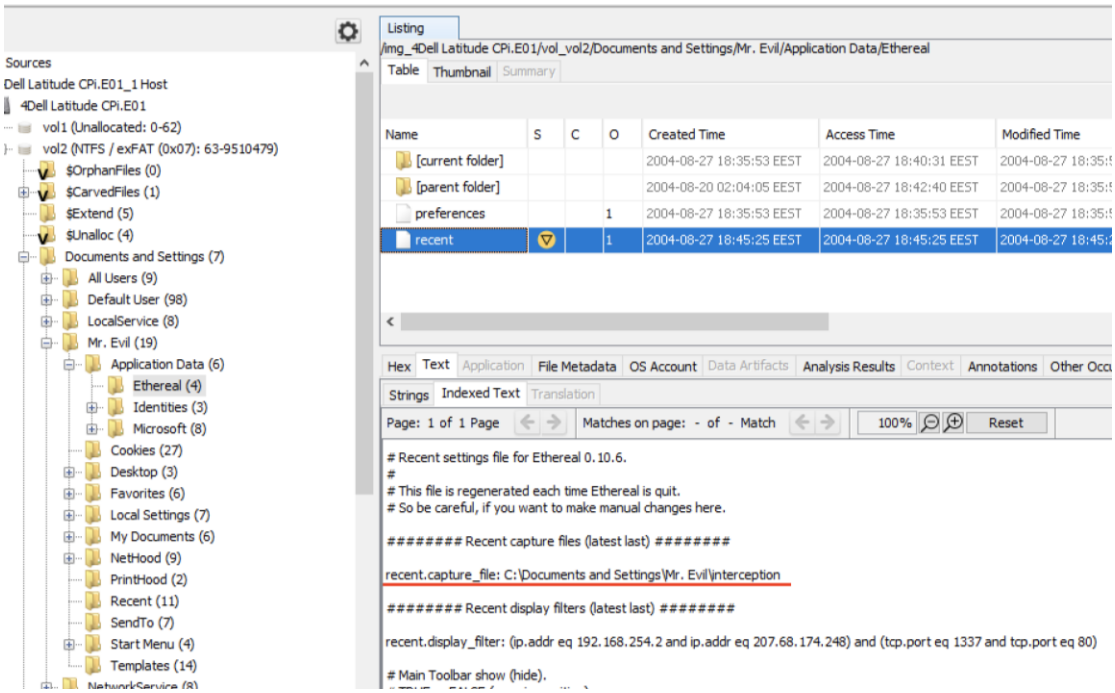

Figure 6 - The information about the most recent interception from the "recent" file

Within the "interception" file the intercepted data is displayed. It appears that the victim was browsing the internet via a "Pocket PC", with "Windows CE - Version 4.20" as the operating system, an "Intel(R) PXA255" processor and a screen resolution of 240x320px with 16bit color depth (Figure 7). The websites visited during the interception process were "mobile.msn.com" (Figure 8) and "MSN Hotmail" (Figure 9).

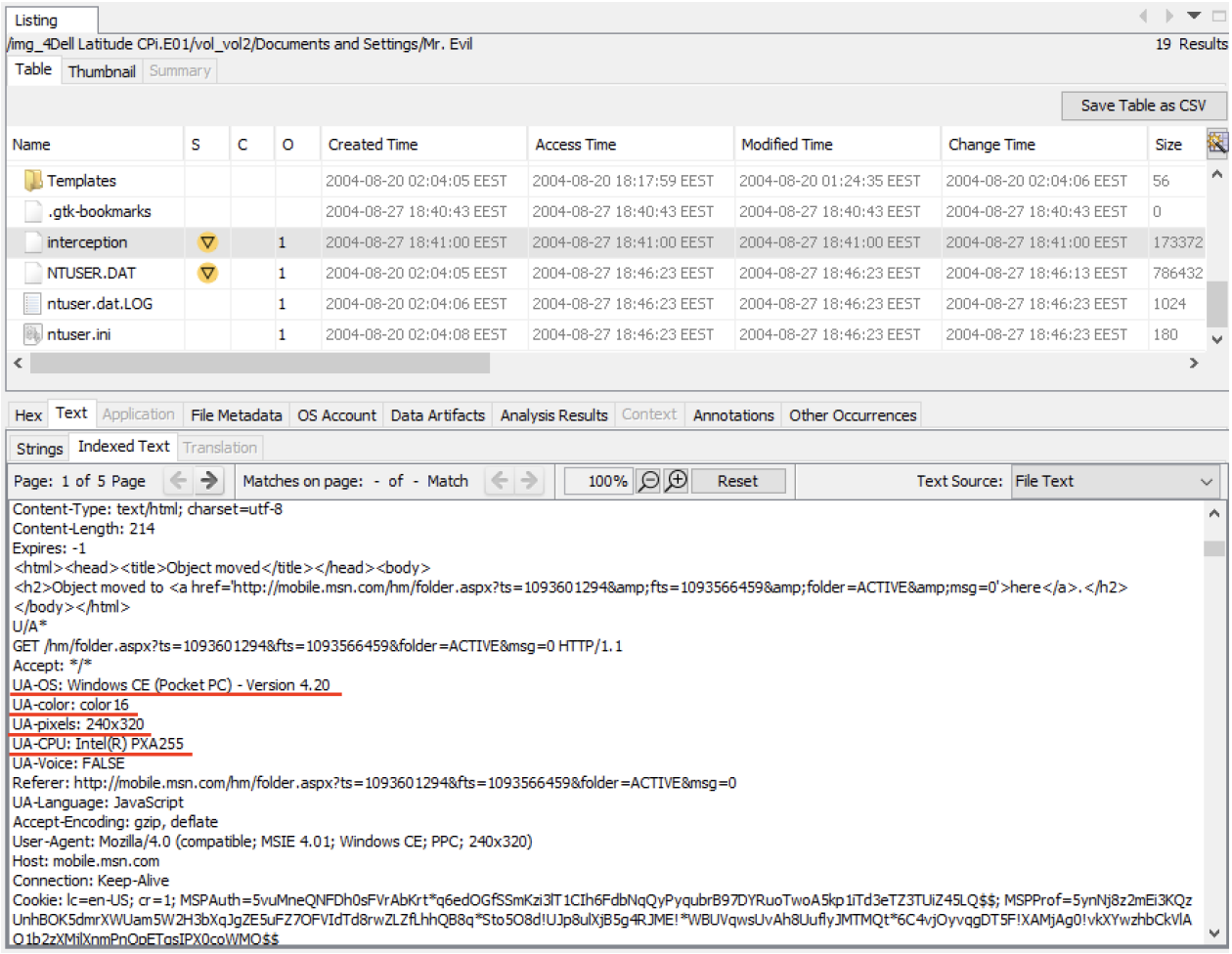

Figure 7 - Information about the victim's device

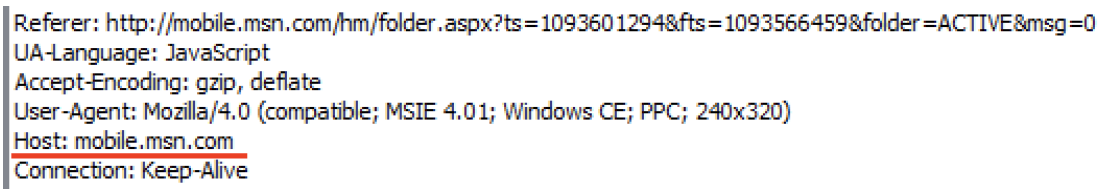

Figure 8 - The website "mobile.msn.com" visited by the victim

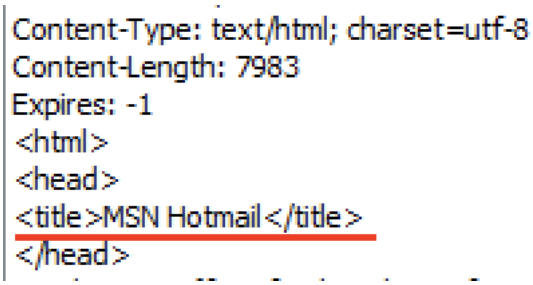

Figure 9 - The "MSN Hotmail" website visited by the victim

The above claims are verified by the content of the "packets.pcap" file generated by the "Bulk_Extractor" application (pre-installed on the "Kali Linux" operating system) (Figure 10). This file contains the network traffic at a given time, which in this case is the time of the aforementioned interception.

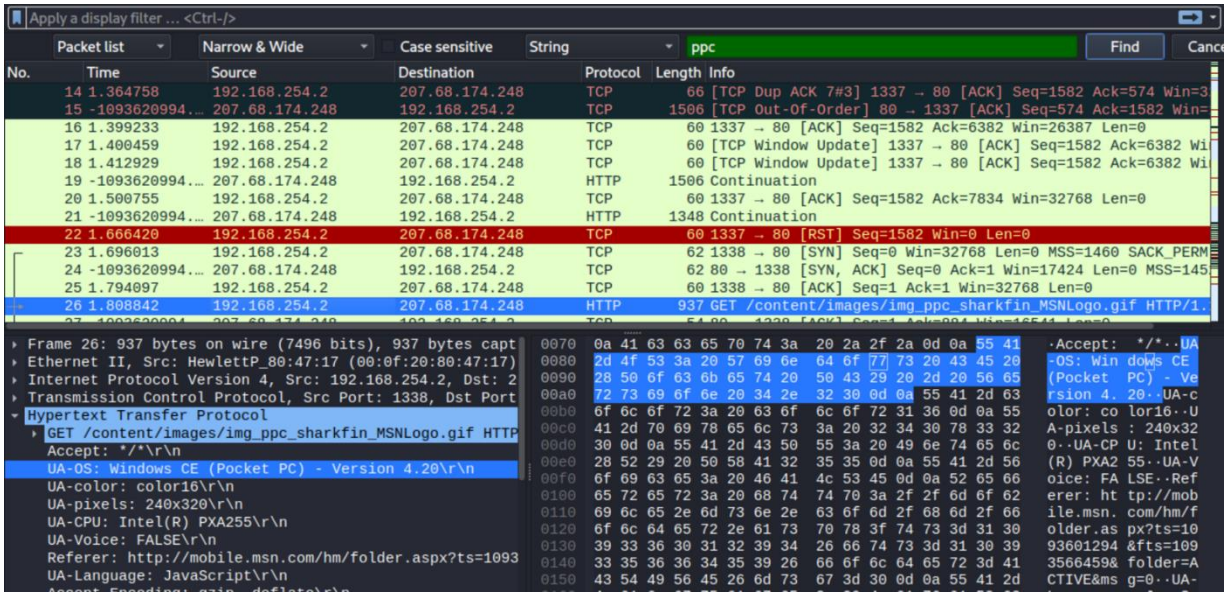

Figure 10 - The content of the "packets.pcap" file produced by the "Bulk_Extractor" application

3.5. Detection of the installation date of the operating system

A search of the system files revealed that the original operating system of the computer was "Windows 98", which was subsequently updated to "Windows XP Professional". More specifically, according to the creation date of the "Program Files" folder, which is created when the operating system is installed, it is concluded that "Windows 98" was installed on 2004-08-18 19:31:52 EEST (Figure 11).

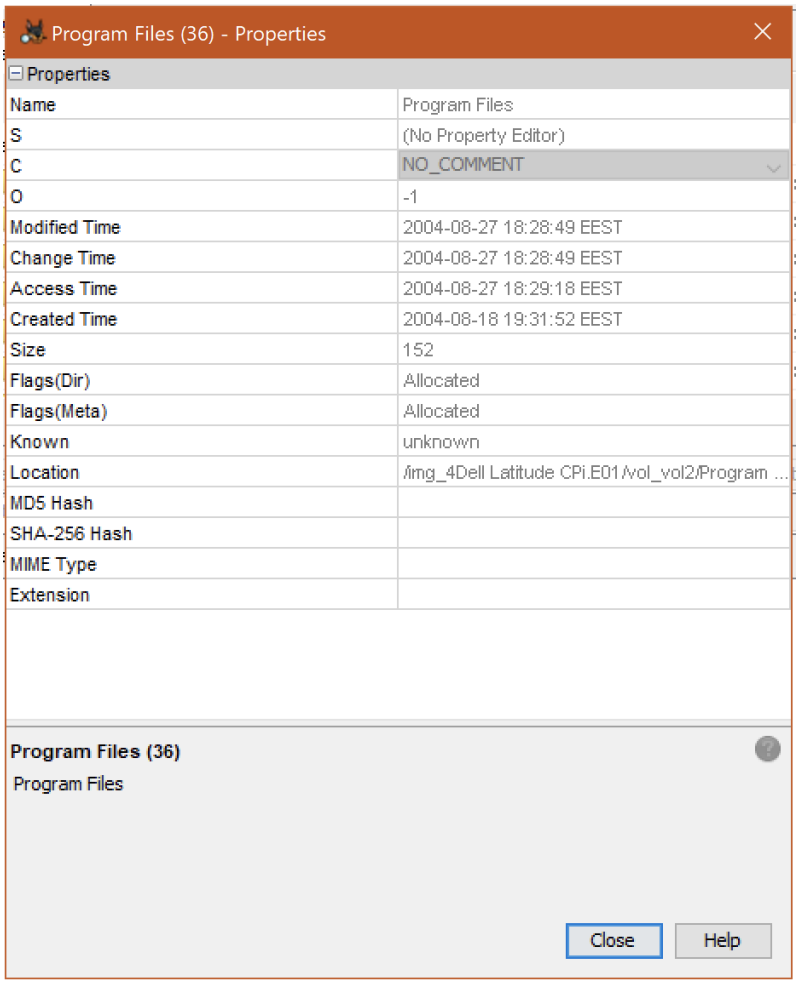

Figure 11 - Properties of the "Program Files" folder

Then, the update to “Windows XP Professional” was started, according to the date of creation of the file “boot.ini”[2] located at “root” of “C:/”, on 2004-08-19 19:47:33 EEST (Figure 12) and completed, according to the value of the “InstallDate” subkey of “Registry”, located at “C:/Windows/system32/config/software\Microsoft\Windows NT\CurrentVersion”, on 2004-08-20 01:48:27 EEST (Figure 13).

[2] A file containing the startup settings for computers with operating systems up to Windows XP

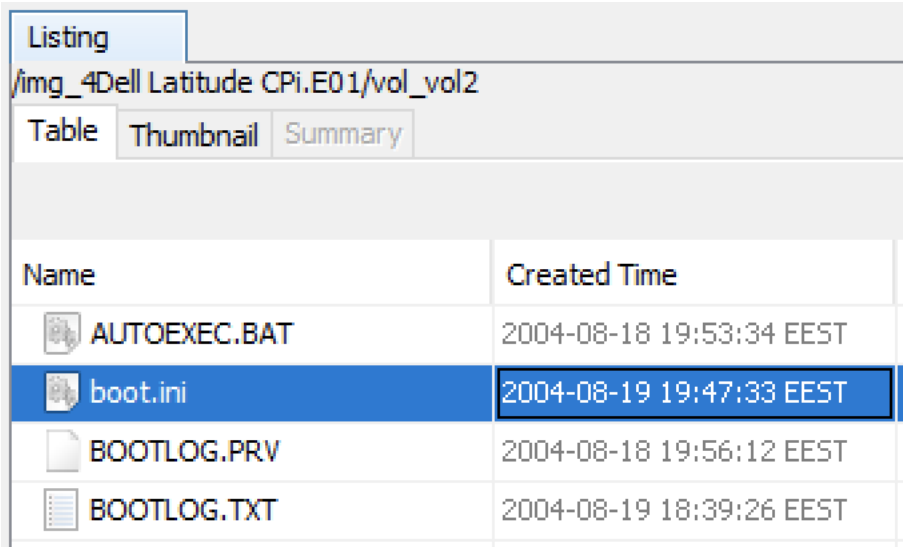

Figure 12 - The creation date of the "boot.ini" file

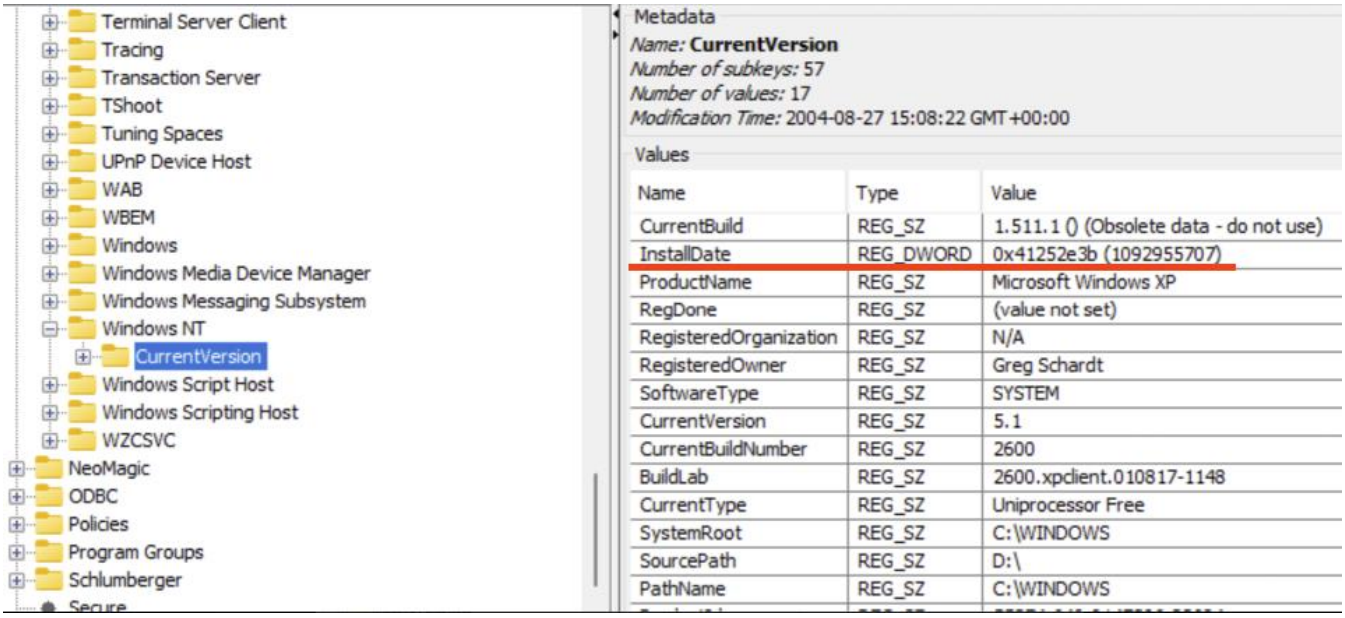

Figure 13 - The value of the "InstallDate" "key" of the Registry

It is worth pointing out that the value of the “InstallDate” key is displayed in “Unix hex timestamp” format, so it needs to be converted to the local time zone, which was done with the help of the tool: https://www.epochconverter.com/.

3.6. Identification of the operating system used

According to the value of the “ProductName” subkey of the “Registry”, located in the path “C:/Windows/system32/config/software\Microsoft\Windows

NT\CurrentVersion", the operating system found to be used on the evidence-computer is "Windows XP" (Figure 14). Also, due to the absence of the "CSDVersion" subkey, it follows that no "Service Pack" has been installed.

Values

Name	Type	Value
CurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)
InstallDate	REG_DWORD	0x41252e3b (1092955707)
ProductName	REG_SZ	Microsoft Windows XP
RegDone	REG_SZ	(value not set)
RegisteredOrganization	REG_SZ	N/A
RegisteredOwner	REG_SZ	Greg Schardt
SoftwareType	REG_SZ	SYSTEM
CurrentVersion	REG_SZ	5.1
CurrentBuildNumber	REG_SZ	2600
BuildLab	REG_SZ	2600.xpclient.010817-1148
CurrentType	REG_SZ	Uniprocessor Free
SystemRoot	REG_SZ	C:\WINDOWS
SourcePath	REG_SZ	D:\
PathName	REG_SZ	C:\WINDOWS
ProductId	REG_SZ	55274-640-0147306-23684
DigitalProductId	REG_BIN	A4 00 00 00 03 00 00 00 35 35 32 37 34 2D 36 34...
LicenseInfo	REG_BIN	34 54 AE DC C7 2E 3D E5 8B 15 06 1A 8C 74 A6 55...

Figure 14 - The operating system of the evidence-computer

Furthermore, based on the contents of the "boot.ini" file located in the "root" of "C:/", which contains the boot options for computers with operating system up to "Windows XP" (since "Vista" and later it has been replaced by "Boot Configuration Data - BCD"), the full name of the operating system version is "Windows XP Professional" (Figure 15).

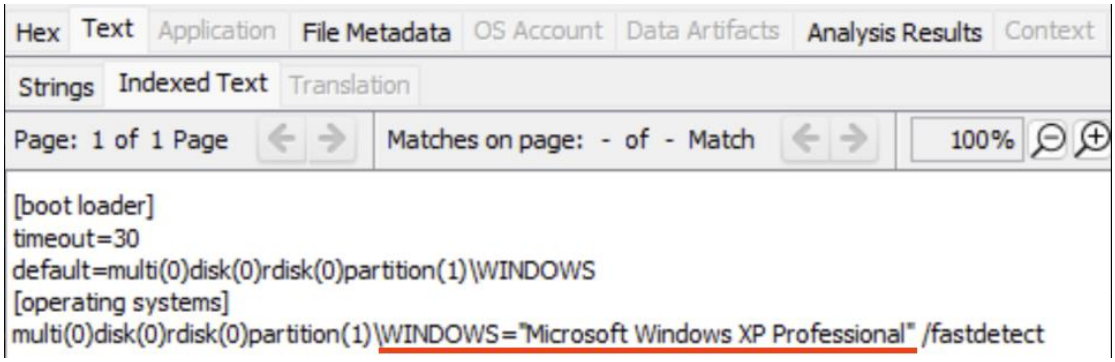

Figure 15 - The full name of the operating system version of the evidence-computer

3.7. Locating the computer's account name

The analysis of the Registry file “SAM”, which contains information about all existing user accounts and is located in the path “C:/Windows/system32/config/SAM”, results in the discovery of the subkey “Users”, which contains five (5) subkeys corresponding to the user accounts of the computer. Within each subkey there are two values “F” and “V” and more specifically, in the second of these, the user's name appears. In the present case, the user's account is associated with the subkey “000003EB” and his name is “Mr. Evil” (Figure 16), which is confirmed by the content of the subkey “Names”, located within the same subkey and associated with the names of the system user accounts (Figure 17).

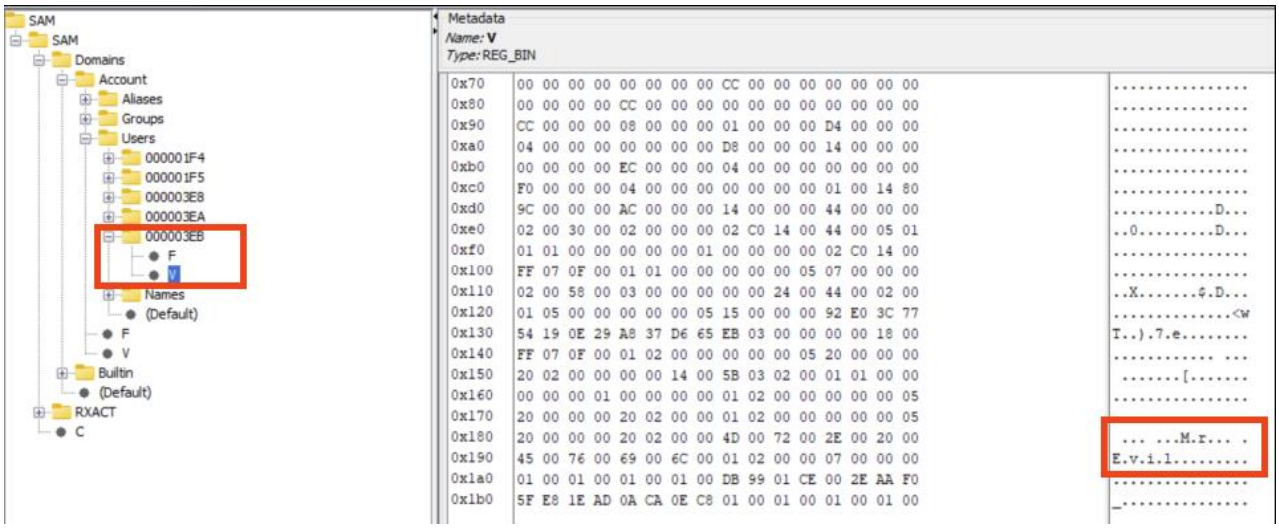

Figure 16 - The subkey "000003EB" of the Registry file "SAM"

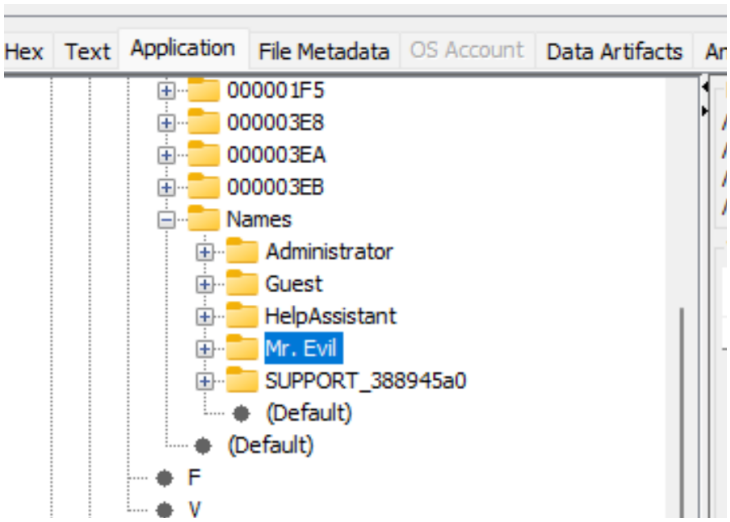

Figure 17 - The "Names" subkey of the Registry "SAM" file

3.8. Confirmation or denial of the suspicion that the computer was previously moved to another geographical area

3.8.1 The first consideration in the analysis of the suspect's location was to examine the IP addresses with which he interacted. Based on the https://www.geolocation.com/ tool, these addresses corresponded to the following areas:

- **New York** (207.68.174.248 - C:/Documents and Settings/Mr. Evil/Application Data/Ethereal/recent)
- **Sunnyvale - California** (64.68.82.189 - C:/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/JIRVJY9X/search[2])
- **Plano - Texas** (216.62.23.121 - C:/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BON0/whatismyip[1])
- **Hong Kong - China** (207.46.130.100 - C:/WINDOWS/system32/config/SysEvent.Evt)
- **RTM - Washington** (65.54.54.179.230 - C:/pagefile.sys)

3.8.2 Next, the Registry files were examined with the help of the "Registry Explorer" tool (https://ericzimmerman.github.io/#!index.md). In the "system" file (C:/WINDOWS/system32/config/system) some crossed out and unassigned values were found (Figure 18), which contained the following IP addresses, which according to the https://www.geolocation.com/ tool corresponded to the following areas:

- **Houston - Texas** (151.164.11.201)
- **Richardson - Texas** (151.164.1.8)

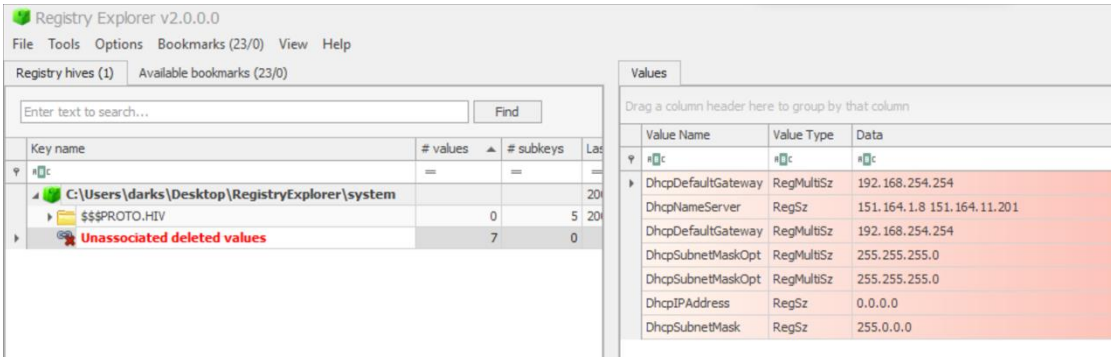

Figure 18 - The deleted and unassigned values of the Registry file "system"

3.8.3 During the browsing of the file system of the tester, the file “hiberfil.sys” (C:/hiberfil.sys) (Figure 19) was found, indicating that the suspect had the “Hibernation” mode enabled.

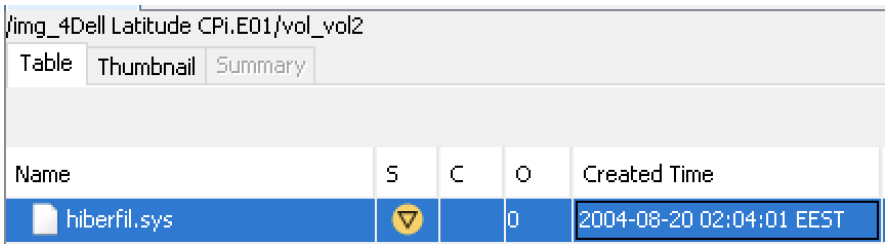

Figure 19 - The file "hiberfil.sys"

The following procedure was followed to read the above file:

1. The Volatility 2 tool (https://github.com/volatilityfoundation/volatility/wiki/Installation) was downloaded and installed on a Kali Linux operating system.
2. The file “hiberfil.sys” was converted to “raw memory dump” format using the “vol.py imagecopy -f hiberfil.sys -O winxp.img” command.
3. The network connections that were active at the time the “Hibernation” mode was implemented (Figure 20) were searched using the “vol.py -f winxp.img --profile=WinXPSP2x86 connscan” command.

Offset(P)	Local Address	Remote Address	Pid
0x002aa298	192.168.1.111:1183	130.94.133.187:80	1156
0x0108edd8	0.0.0.0:0	0.0.0.0:0	2157104624
0x010b1350	192.168.1.111:1184	209.185.12.42:80	1156
0x01833e68	192.168.1.111:1182	130.94.133.187:80	1156
0x05241420	192.168.1.111:1148	67.114.52.28:80	1524
0x05d26678	192.168.1.111:1175	204.193.136.54:6667	1564
0x06baa540	112.0.0.0:46079	0.0.0.0:45264	4289366312
0x07122820	0.0.0.0:0	0.0.0.0:0	4289091640
0x07847628	192.168.1.111:1179	67.15.24.20:80	1156

Figure 20 - The network connections that were active at the time the "Hibernation" mode was implemented

Using the https://www.geolocation.com/ tool, these addresses correspond to the following areas:

- **Redmond - Washington** (130.94.133.187, 67.114.52.28)
- **Phoenix - Arizona** (209.185.12.42)
- **Swanny - Georgia** (204.193.136.54**)**

- **San Jose - California** (64.15.24.20)

3.8.4 Despite the various IPs that the suspect interacted with, there does not appear to be conclusive evidence to confirm the suspicion that the computer had previously been moved to another geographical area. This is verified firstly, by the date of the last entry of the "TimeZoneInformation" key (C:/Windows/System32/config/system\ControlSet001\Control\TimeZoneInformation) which is 2004-08-19, i.e. the date when the installation of the operating system started (Figure 21) and then, by the "NTP" (Network Time Protocol) content of the "Type" value in the path "C:/Windows/System32/config/system\ControlSet001\Services/W32Time/Parameters " (Figure 22), which means that the system time was automatically synchronized via the Internet. It is worth noting that, according to the "TimeZoneInformation" key mentioned above, the system's time zone was set to "Central Standard Time" (UTC -6), i.e. it was part of the timezone "US & Canada" (Figure 23). Therefore, since no change was made to the computer's time zone since the time of the operating system installation, no move to another geographical area was performed.

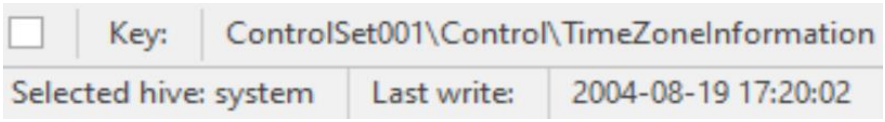

Figure 21 - The date of the last record of the "TimeZoneInformation" key

Value Name	Value Type	Data
ServiceMain	RegSz	SvchostEntry_W32Time
ServiceDll	RegExpandSz	C:\WINDOWS\System32\w32time.dll
NtpServer	RegSz	time.windows.com,0x1
Type	RegSz	NTP

Figure 22 - The "NTP" content of the "Type" value

Value Name	Value Data
Bias	360
StandardName	Central Standard Time
StandardBias	0
StandardStart	Month 10, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
DaylightName	Central Daylight Time
DaylightBias	-60
DaylightStart	Month 4, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
ActiveTimeBias	300

Figure 23 - The Time Zone of the system

3.9. Identification of additional users who had access to the computer

After analyzing the "C:/Document and Settings" folder, it was found that the only user account created is named "Mr. Evil" (Figure 24), however, there is a possibility that there are more user accounts whose profile folders have not been created. This may be due to instances of remote access via "Remote Desktop Protocol - RDP" using the default "port" 3389. Due to this, a more thorough search of the "Registry" was required, and more specifically, the file "C:/Windows/system32/config/SAM", which contains information about existing user accounts. The result of the investigation is that there are five (5) user accounts registered with the following names: Administrator, Guest, HelpAssistant, Mr. Evil, SUPPORT_388945a0. By importing the "SAM" file into a registry viewer, specifically the "AccessData Registry Viewer" (https://www.exterro.com/ftk-product-downloads/registry-viewer-2-0-0) for further analysis, it was concluded that the only user using the computer was "Mr. Evil", as none of the other accounts had ever logged in. A further finding from the analysis was that the user "Mr. Evil" had logged in fifteen (15) times, with the last one taking place on 2004-08-27 18:08:23 EEST (15:08:23 UTC) (Figure 25).

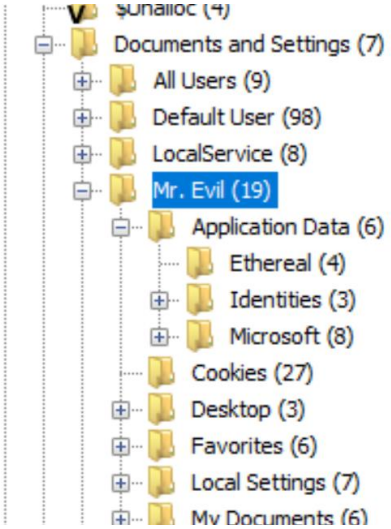

Figure 24 - The contents of the "C:/Document and Settings" folder

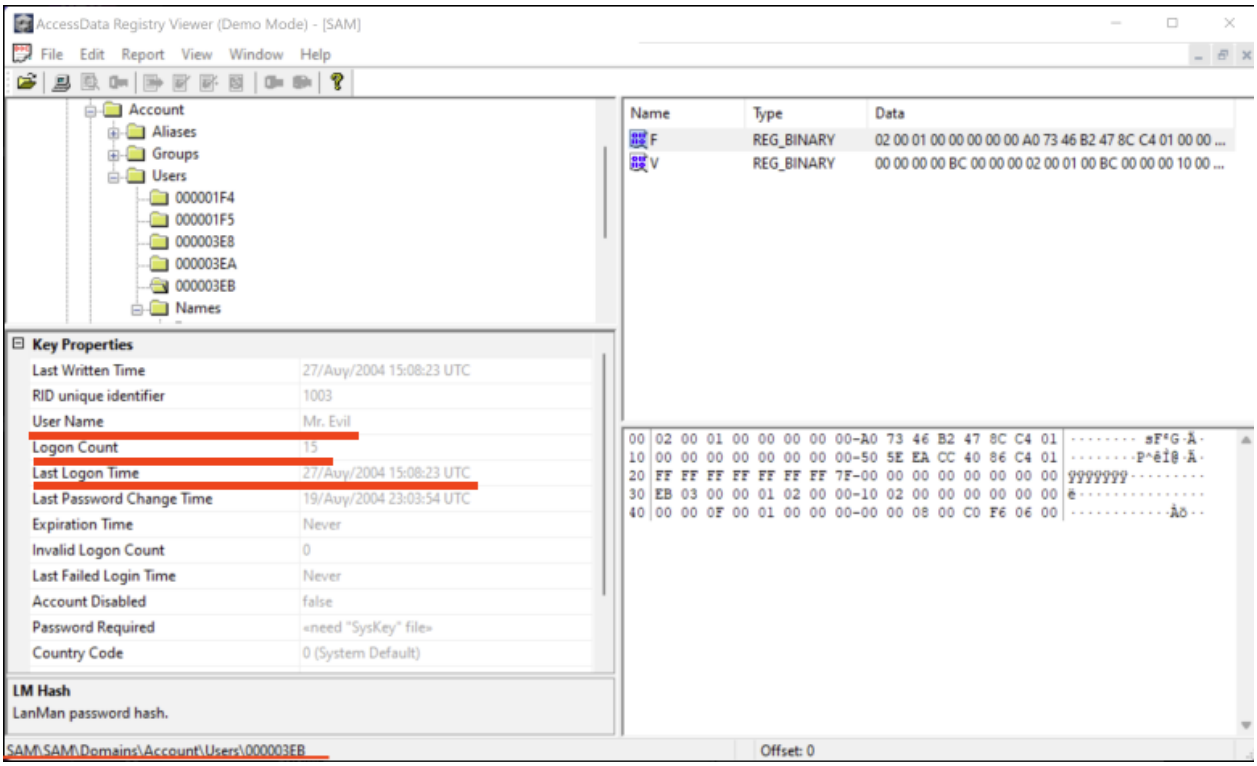

Figure 25 - Information about the user account "Mr. Evil"

During the investigation, the subkey “RegisteredOwner” was found in the path “C:/Windows/System32/config/software\Microsoft\Windows NT\Current Version\Winlogon”, indicating that the owner of the computer is named “Greg Schardt” (Figure 26), which verifies the suspicion that the first name of the suspect associated with the computer is “Gregory” and therefore uses the alias “Mr. Evil”.

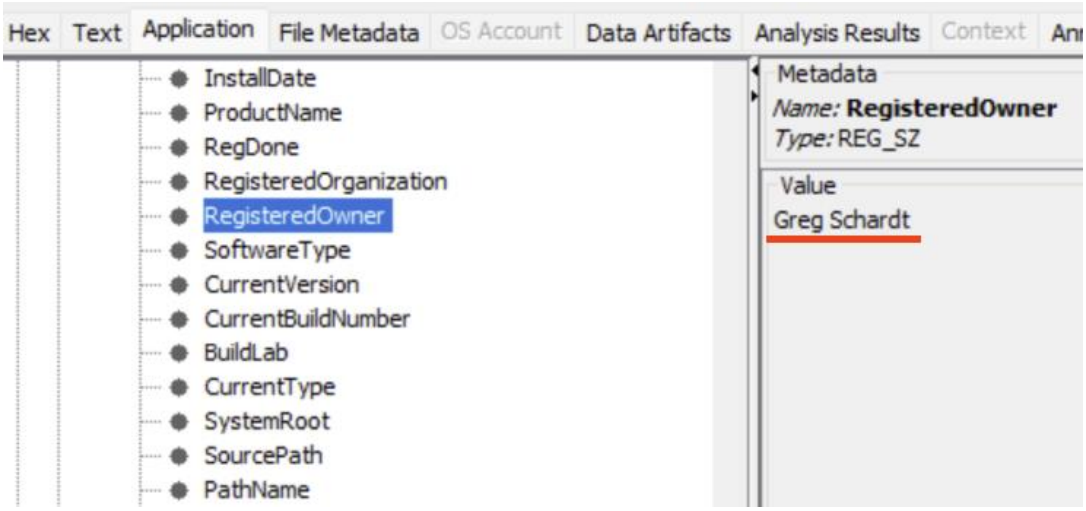

Figure 26 - The name of the computer owner

Since it turned out that Greg Schardt is the owner of the system and uses the only active account on the system (Mr. Evil), it is very likely that this account is also the system administrator, i.e. belongs to the "Local Administrators Group". The first step in proving this claim is to find the hex value representing the administrators group, which, according to "Microsoft" (https://learn.microsoft.com/en-us/dotnet/api/system.security.principal.windowsprincipal.isinrole?view=net-7.0), is "0x220". The next step is to search by the unique ID number of "Mr. Evil", i.e. "000003EB", in the path "SAM\SAM\Domains\Builtin\Aliases\Members\", in order to find the value containing (20 02 00 00 00) (full path "SAM\SAM\Domains\Builtin\Aliases\Members\S-1-5-21-2000478354-688789844-1708537768\000003EB". It is then necessary to find the version of the processor, as this makes it possible to read the above key. According to the value of the key "PROCESSOR_IDENTIFIER" located in the path "C:/Windows/System32/config/system\ControlSet001\Control\Session Manager\Environment" (Figure 27), the processor is "Intel" with "x86" architecture. Knowing that "Intel" processors with "x86" architecture use the "Little-endian" rule (convention) to sort the data transferred from the Register to the Memory (https://levelup.gitconnected.com/little-endian-vs-big-endian-eb2a2c3a9135), the above value "20 02 00 00" is read from right to left, therefore it is converted to "0x00000220", which is the same as "0x220" which "Microsoft" defines as Administrator. So, the account "Mr. Evil" is also system administrator.

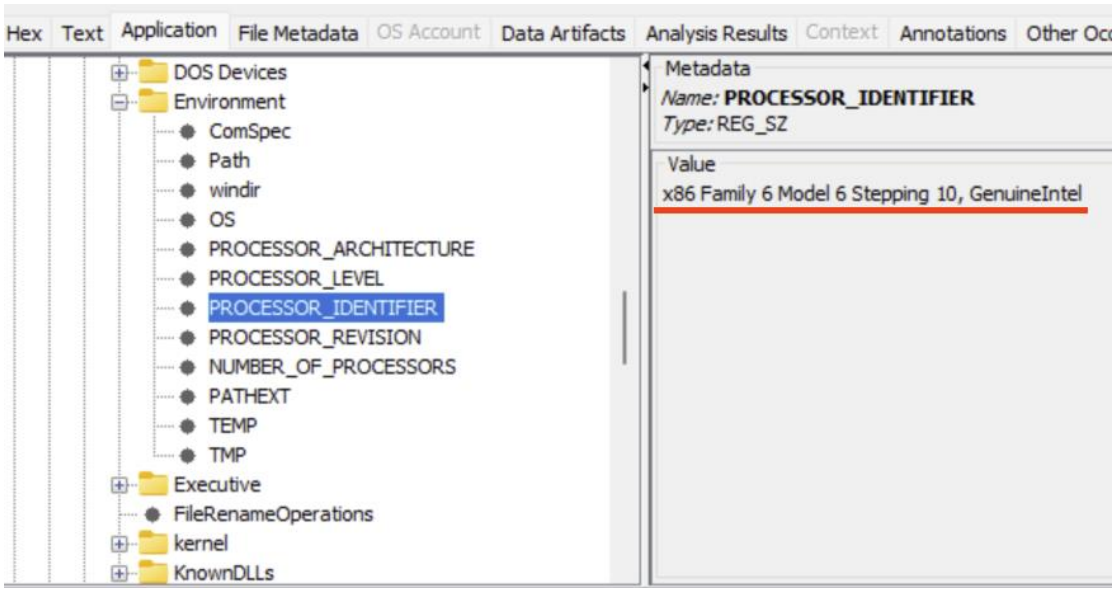

Figure 27 - Information about the system processor

3.10. Identification of the manufacturer of the network card used for the illegal activities

To find the network cards connected to the computer, the path "C:/Windows//System32/config/software\Microsoft\Windows NT\CurrentVersion\NetworkCards" was followed, in which there were two subkeys corresponding to two different network cards (Figures 28 and 29).

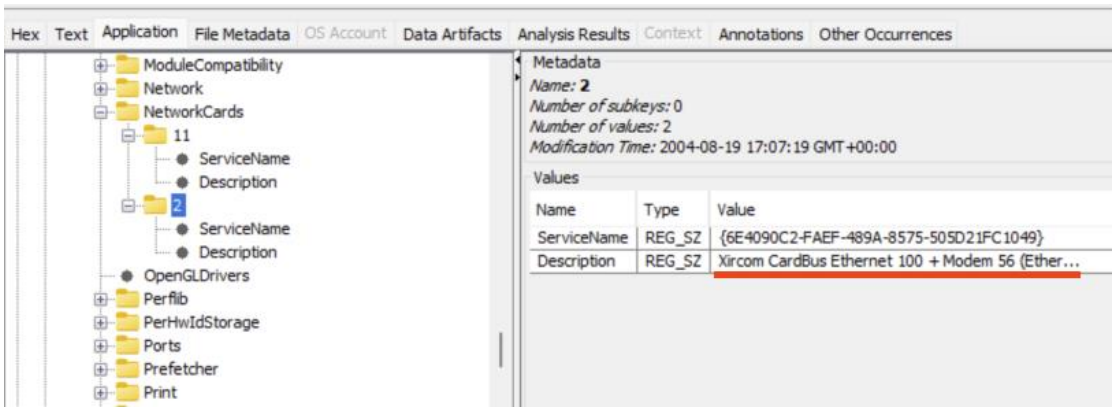

Figure 28 - The "Xircom" network card

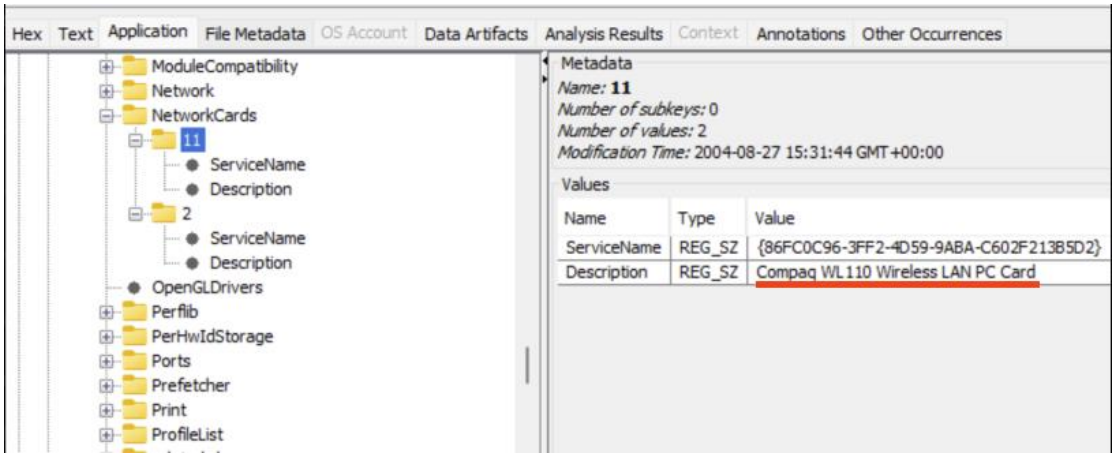

Figure 29 - The "Compaq" network card

In order to identify the network card used for the illegal activities, a search was carried out in the files of the “Look@LAN” tool, which is used to analyze network traffic. More specifically, the file “irunin.ini” located in the path “C:/Program Files/Look@LAN/irunin.ini” contains data such as the username (%LANUSER%), the IP address (%LANIP%) and the MAC address of the network card used (%LANNIC%) (Figure 30). By searching for the MAC address in the database of the https://www.adminsub.net/ tool, it was found to correspond to the manufacturer “XIRCOM” (Figure 31).

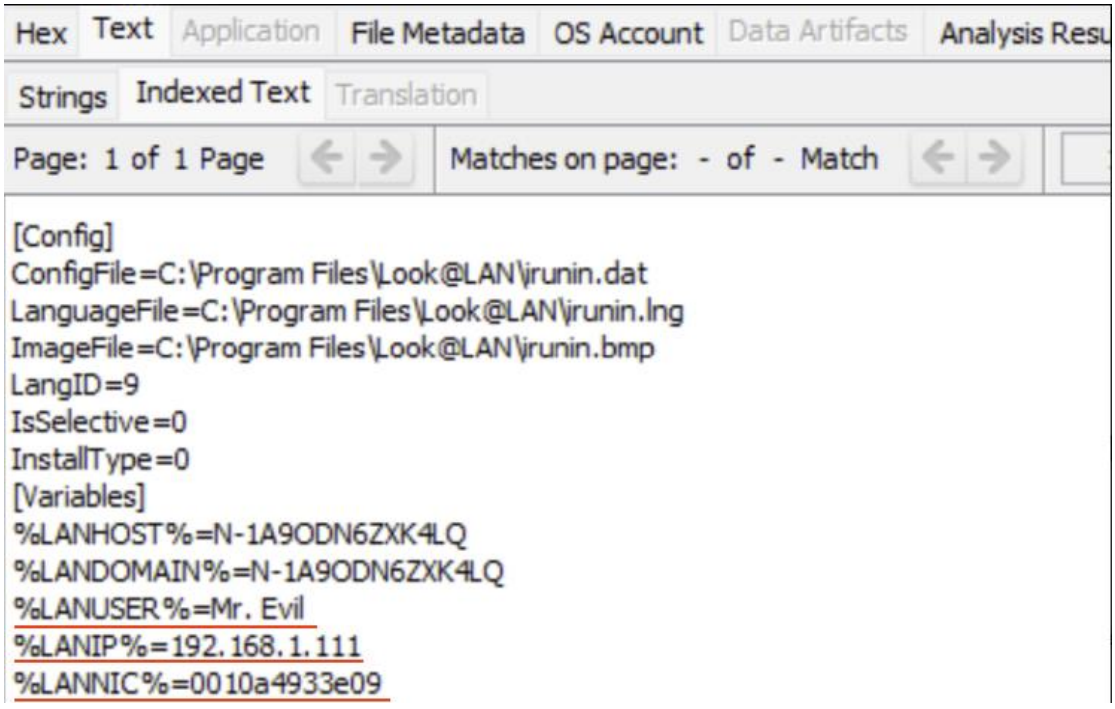

Figure 30 - The contents of the file "irunin.ini"

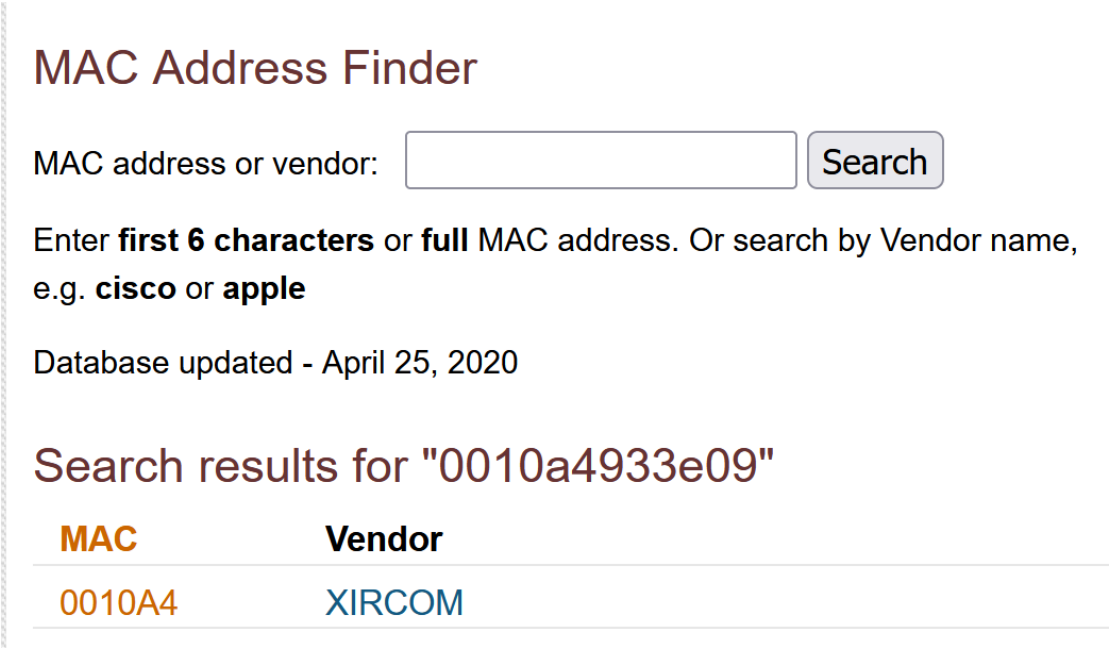

Figure 31 - Search by MAC address in the "https://www.adminsub.net/" tool

3.11. Verification or denial of the testimony of his accomplices in order to bring additional criminal proceedings

According to the confessions of the defendant's accomplices, that he had intended to park his car outside of places that would be within the range of wireless access points, such as Starbucks and other hotspots of T-Mobile, in order to intercept packets of internet traffic, a search was conducted in the content of the virtual disk using keywords such as: “T-Mobile” and “Starbucks”. The results of the search using the keyword “T-Mobile” showed that the suspect was interested in the telecommunications company, as he had visited a website that mentioned its business activities, which included working with other companies to provide them with technological solutions, such as the “hotspot” (Figure 32).

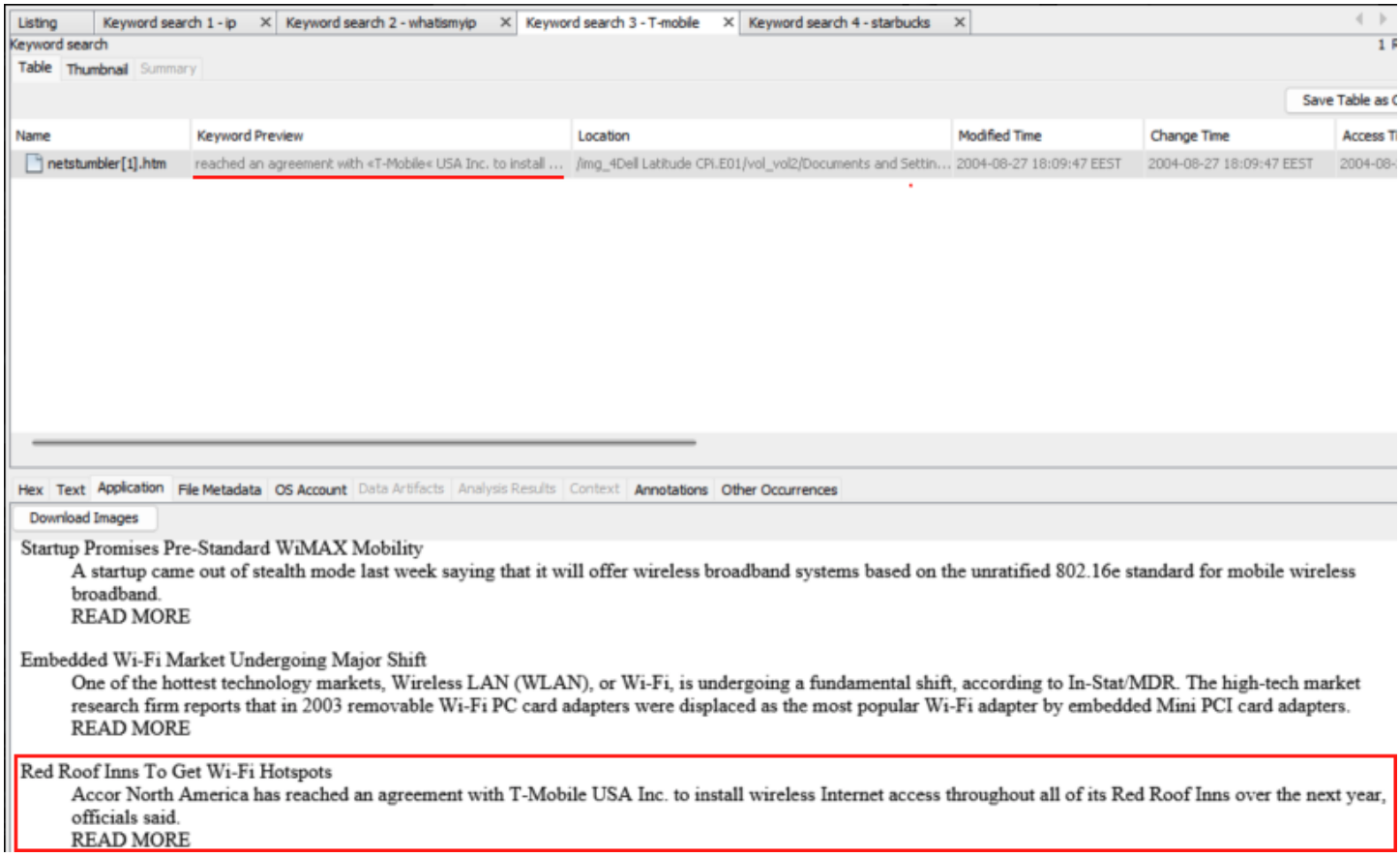

Figure 32 - Website trace reporting T-Mobile's business moves

Regarding the keyword “Starbucks”, a trace of a visit to a website related to “Wardriving” was found, which demonstrates the suspect's interest in this type of attack (Figure 33).

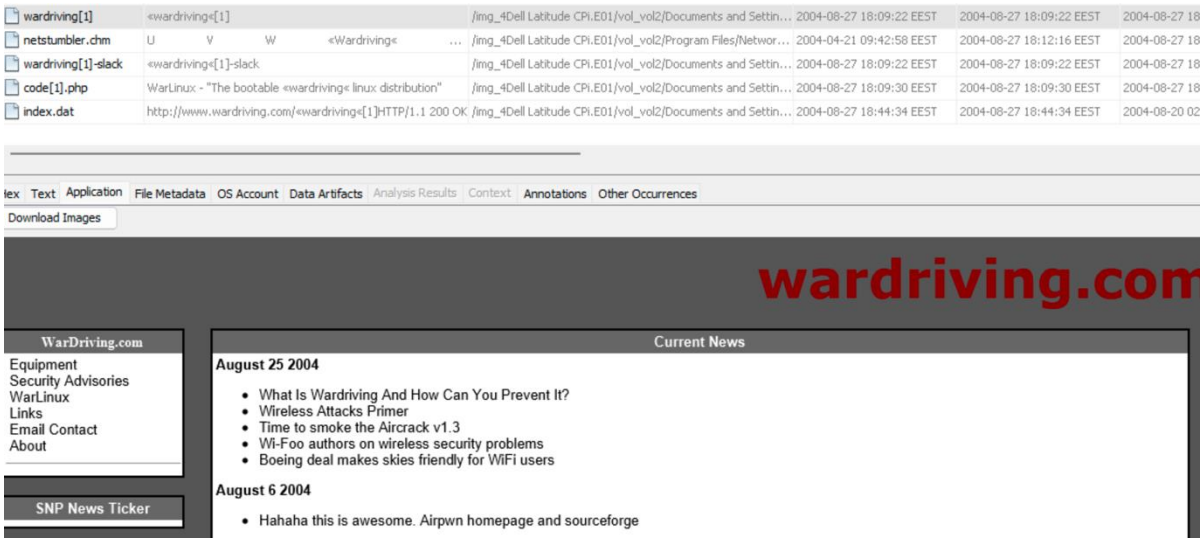

Figure 33 - Website trace of a website related to "Wardriving"

The files generated by using the only interception tool (Ethereal) installed on the computer were also examined (C:/Documents and Setting/Mr. Evil/Application Data/Ethereal & C:/Program Files/Ethereal). The result of the examination was the finding of the evidence that the default setting of the network card was to be used in "Promiscuous Mode" (network card mode, whereby all network packets are forwarded to the central processing unit - CPU and is mainly used for network packet interception), when running "Ethereal" (Figure 34).

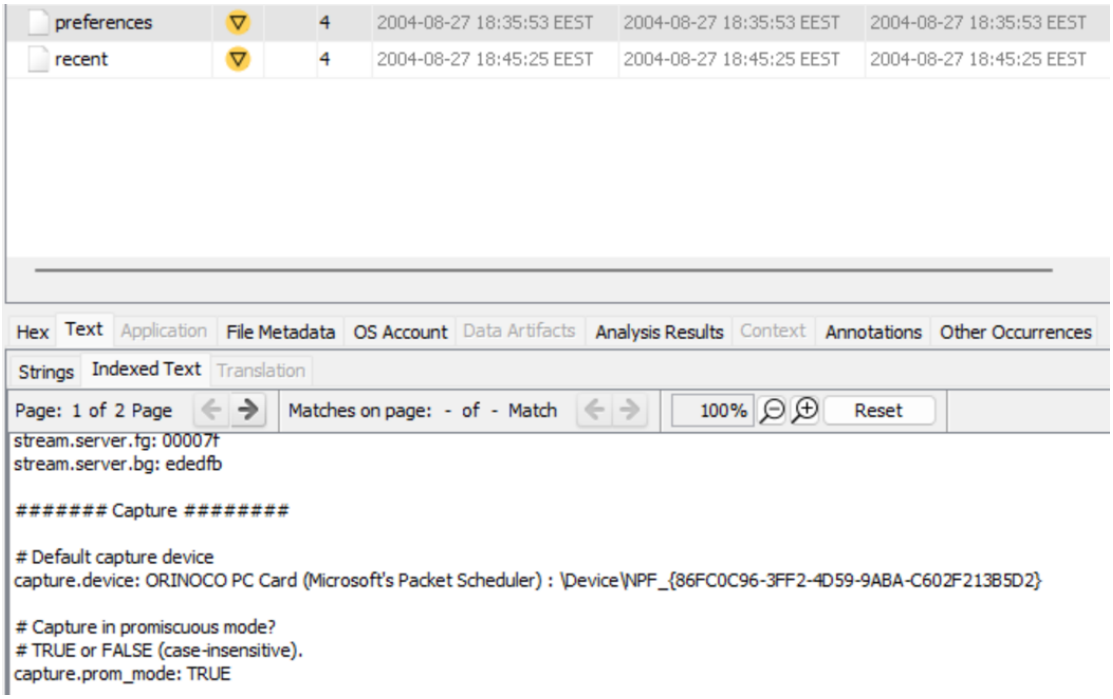

Figure 34 - Proof that the network card was operating in "Promiscuous Mode"

Next, the IP addresses to which the user connected to in order to use the interception tool were analyzed. Remaining in the same subfolder, the "recent" file was identified, which is created each time the application is shut down and contains the last filter applied during the data interception process. In this file, a target IP address (207.68.174.248) was found on ports "1337" and "80" (Figure 35).

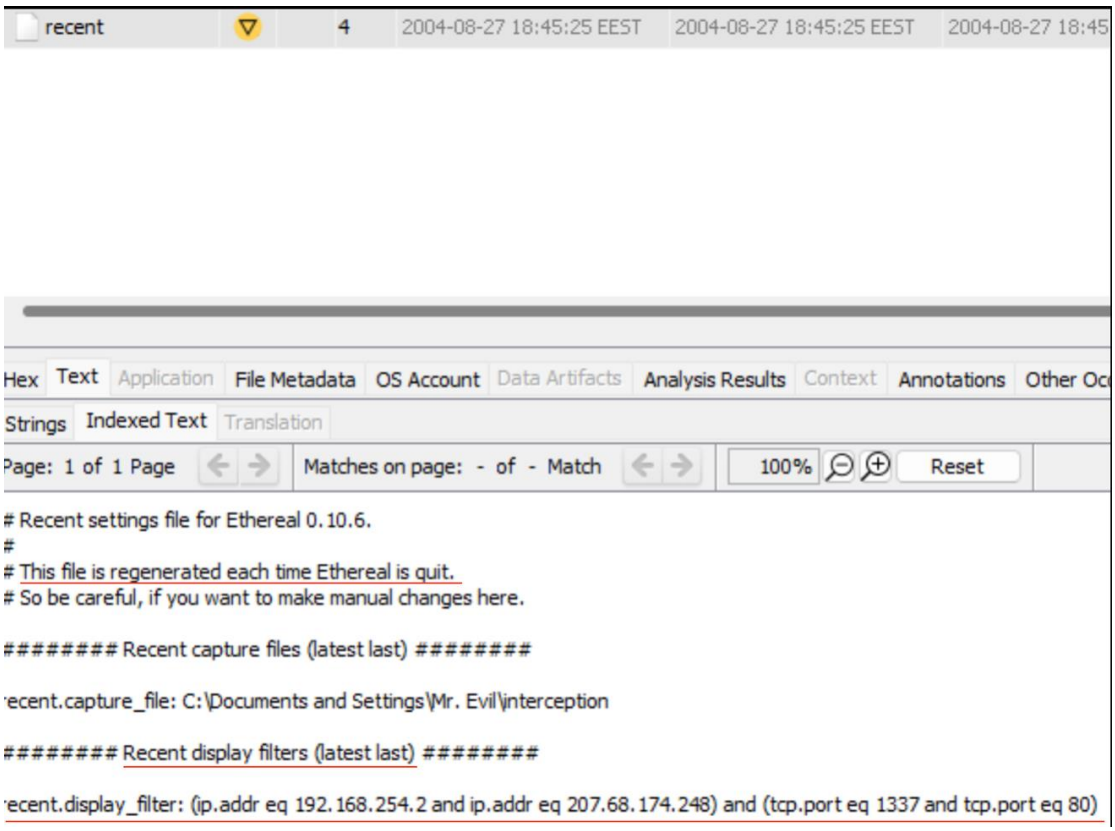

Figure 35 - The filter applied during the last data interception process

The target address was then further investigated using the https://www.geolocation.com/ tool, where entering the address displays relevant information such as approximate location and coordinates (Figure 36).

Country United States of America	**Region** New York	**City** New York City
ZIP or Postal Code 10116	**Latitude** 40.712252	**Longitude** -74.005408
ISP Microsoft Corporation	**Domain Name** microsoft.com [WHOIS] [Check Mail Server]	**Usage Type** DCH
Weather View Weather	**Time Zone** America/New_York	**Local Time** 2023-05-15T10:47:39-04:00
Address Type Unicast	**Category** Business Software	**District** -
AS Number 8075	**AS Name** Microsoft Corporation	
Proxy No	**Proxy Provider** -	

Figure 36 - Information about the target address

Then, by entering the coordinate data into the "Google Maps" application (https://www.google.com/maps), it is clear that the location corresponds to the address

"1 Park Row, New York" (Figure 37), which, as can be seen in Figure 38, is very close (450 feet - 137 meters) to a "Starbucks" store.

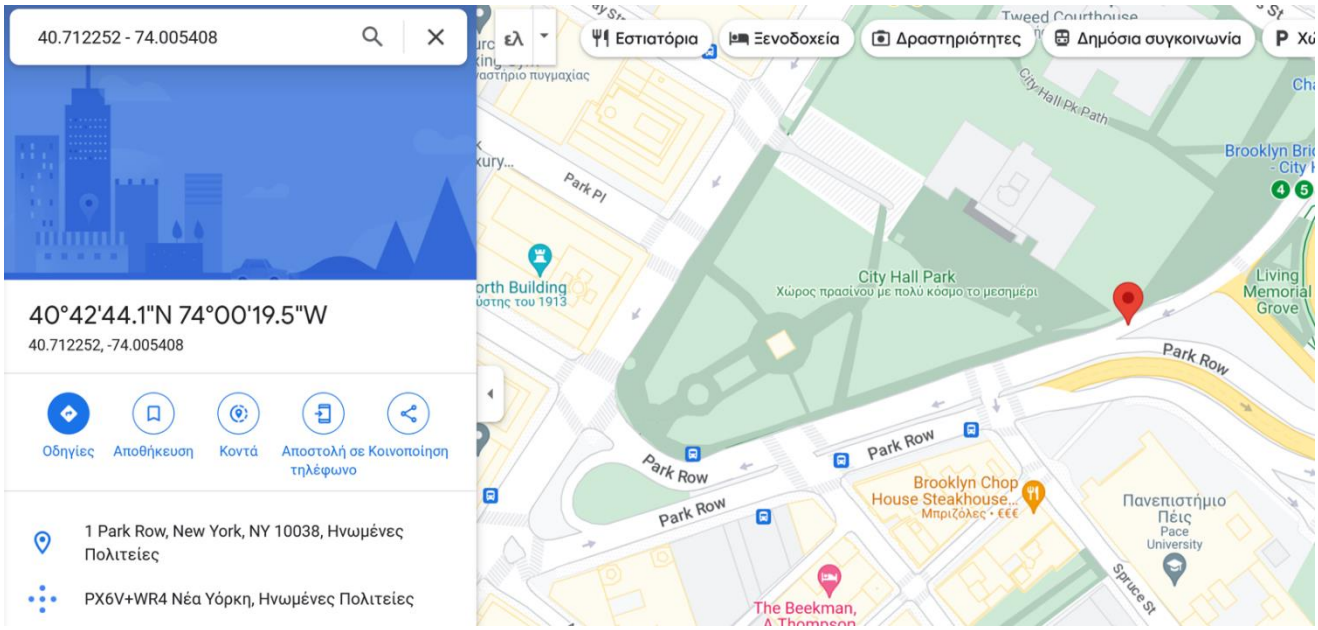

Figure 37 - The location corresponding to the target address

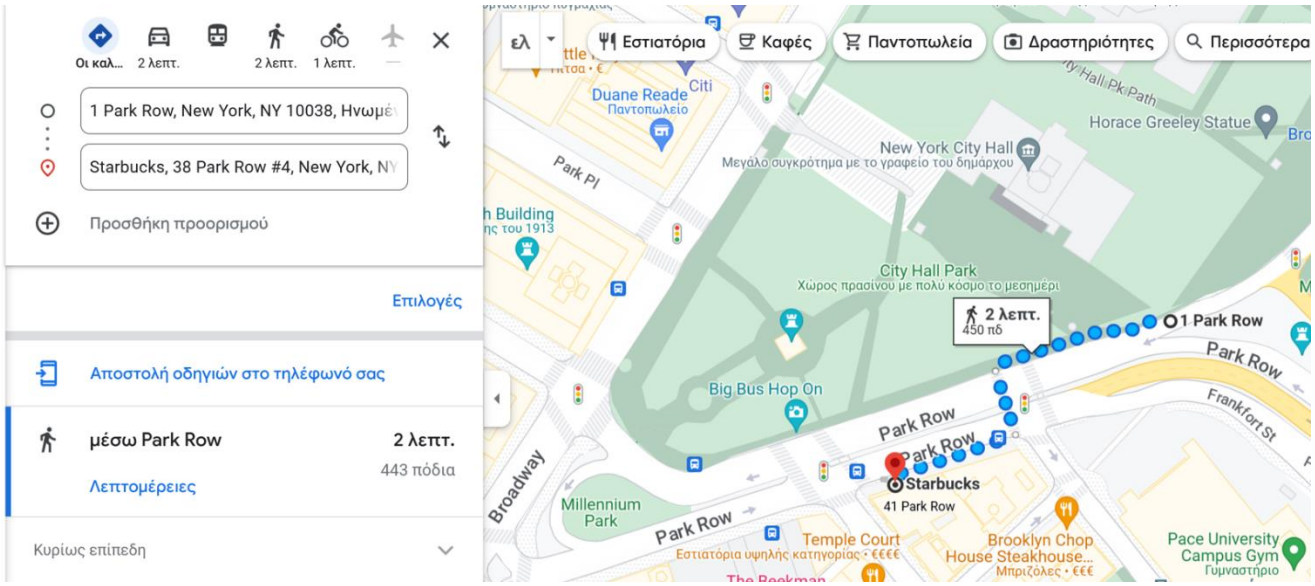

Figure 38 - The distance of the location of the target address from the nearest "Starbucks"

Therefore, the testimonies of his accomplices are true and are valid as evidence for additional prosecution.

3.12. Investigation of traces of child pornography

The first step in investigating traces of child pornography was to search for images with relevant content. As no evidence was found, the next step was to search the folders of the "Outlook Express" application (C:/ Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express), which the suspect used to manage his emails. Within the folder, several files from newsgroups were found, with topics such as "hacking" and "computer software". Among them, there is the file named "Folder.dbx", which contains all the newsgroups to which the suspect subscribed. Regarding the requests of the analysis of the evidence, among others, the following newsgroups were found:

- alt.binaries.erotic.children
- free.binaries.pictures.children
- free.binaries.pictures.child.erotica.femalex=:,
- free.binaries.erotica.teen.female.nonude
- free.binaries.pictures.child.erotica.for.peter-j-ross
- free.binaries.nospam.teenfeem.repost
- free.binaries.pictures.barefoot.children
- free.binaries.pictures.child.erotica.for
- free.binaries.pictures.child.erotica.male
- alt.japanese.neojapan.pedophilia
- alt.pedophile.bob-curtis
- alt.pedophile.bruce-ediger
- alt.pedophile.david-ratcliffe
- alt.pedophile.grady-booch
- alt.pedophile.jason-durbin
- alt.pedophile.nick-sandru
- alt.pedophile.richard-tietjens
- alt.pedophile.robbie-honerkamp
- alt.svens.house.of.12.year-old.lust

All the above are newsgroups that the suspect subscribed to at will, to which users can send messages and play multimedia. Therefore, the suspect's interest in this topic is perceived.

For a better understanding and analysis of the suspect's actions, it was considered necessary to recreate his movements from the launch of the “Outlook Express” application to the subscription to a news group. More specifically, a virtual machine with a “Windows 98” operating system was created, on which the email application was pre-installed, a newsgroups account was created (Figure 39) and then a subscription to some of them was made (Figures 40 and 41).

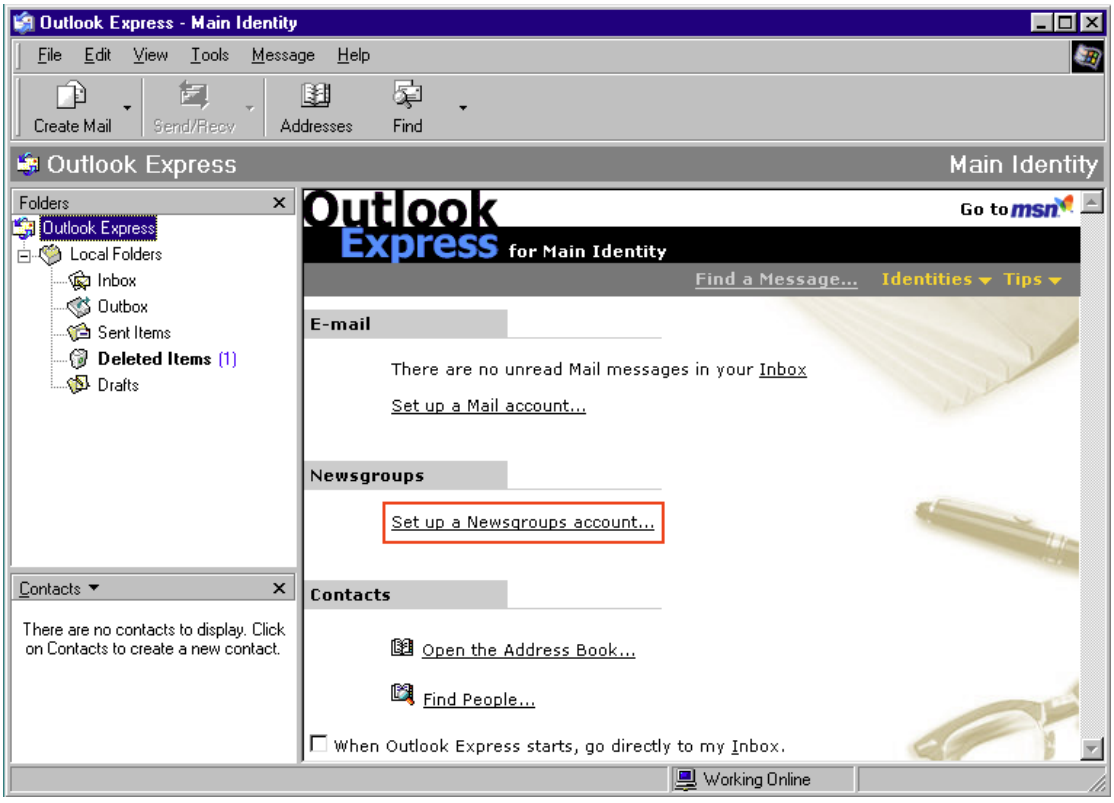

Figure 39 - Setting up a newsgroup account in the "Outlook Express" tool

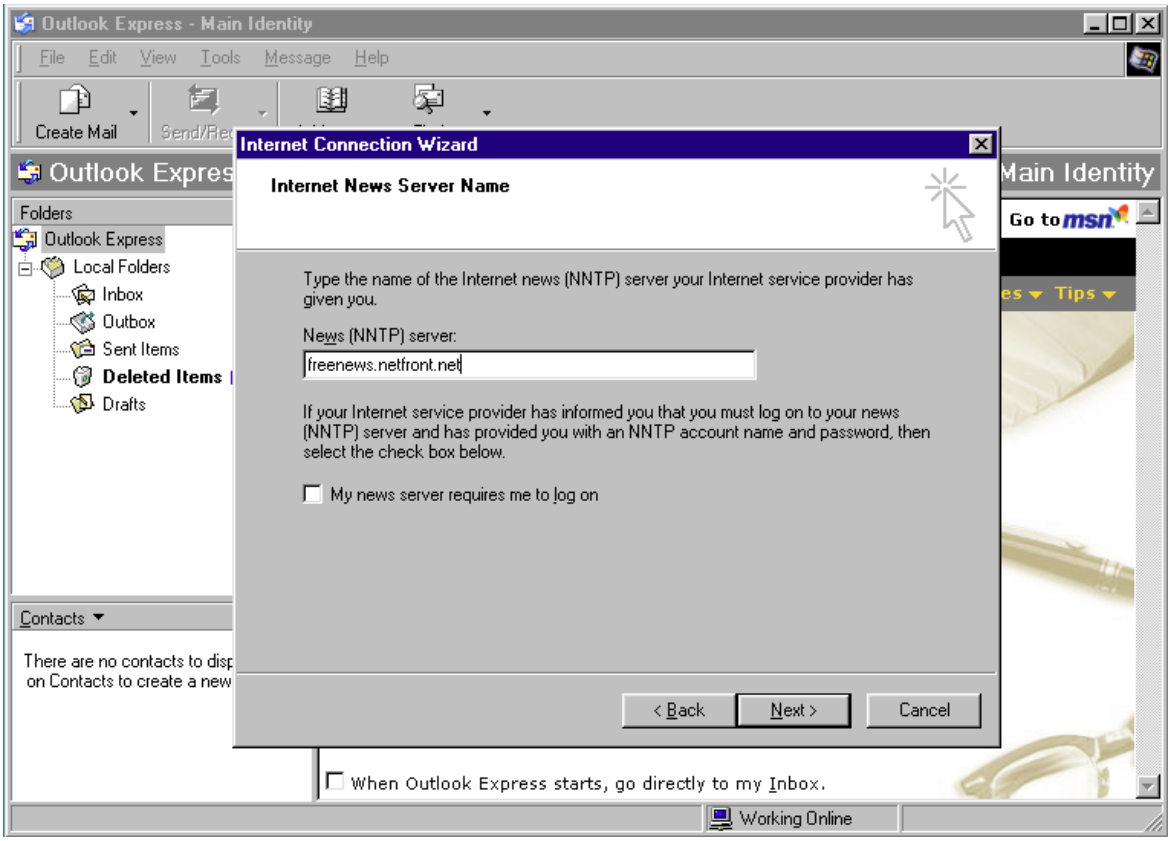

Figure 40 - Typing the address of an NNTP server

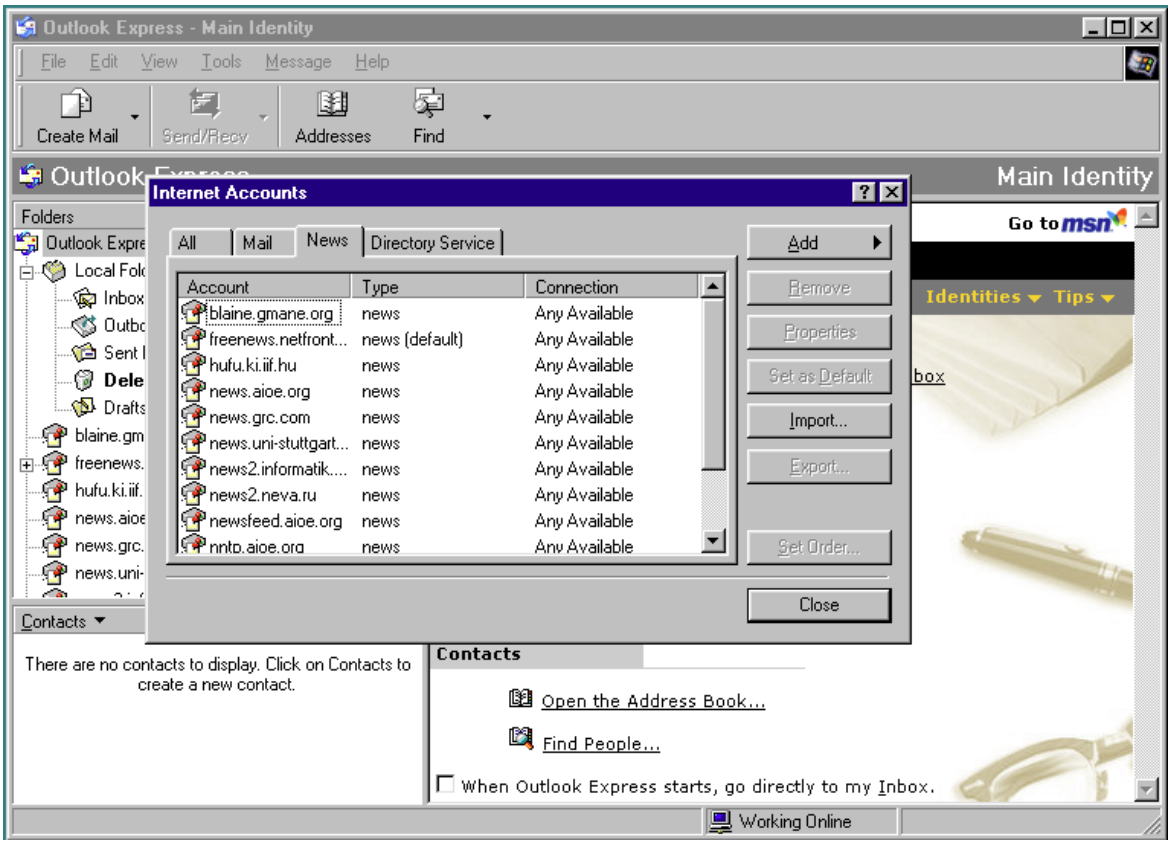

Figure 41 - Some of the newsgroups

Below (Figure 42) is a possible form of the suspect's email application environment.

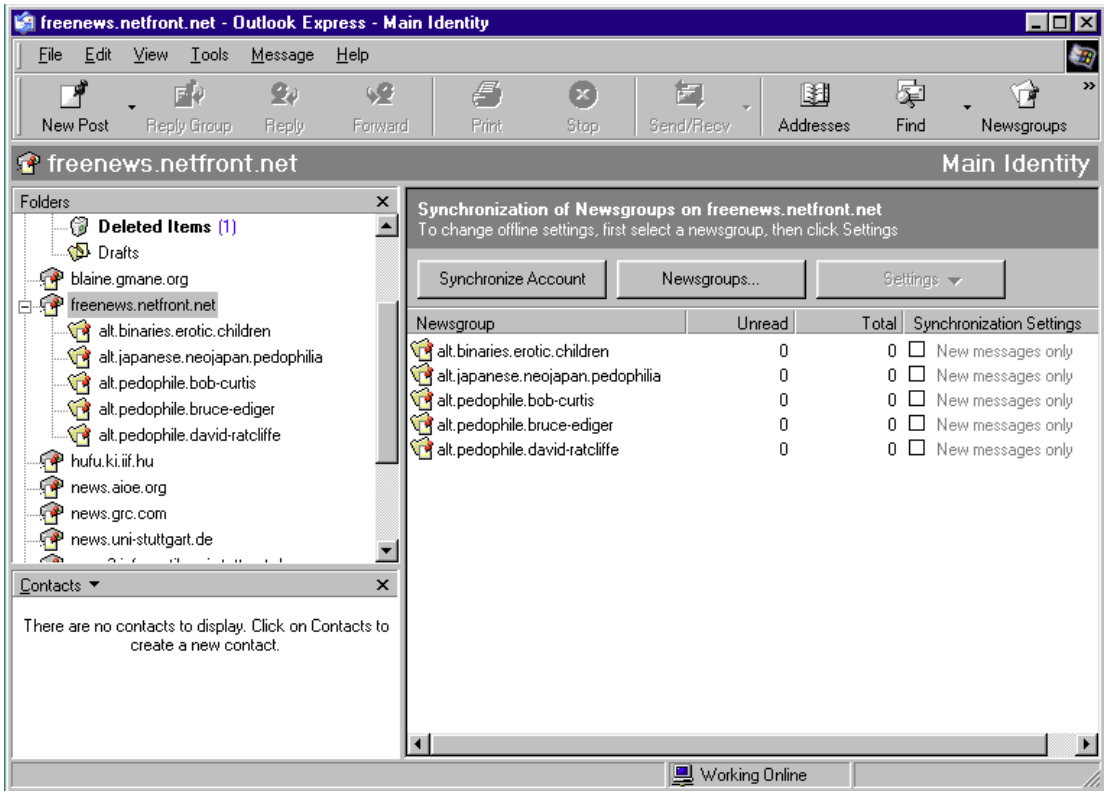

Figure 42 - Possible form of the suspect's email application interface

3.13. Investigation of traces of economic crimes

First, the results of the analysis of the "Autopsy" tool (https://www.autopsy.com/) were examined for findings regarding the existence of credit card data on the virtual disk. This examination led to the file "alt.2600.cardz.dbx" (Figure 43), corresponding to a newsgroup to which the suspect had subscribed via the Outlook Express application. A newsgroup is an email sharing group in which a user interacts either by sharing content or simply browsing it. The file was read with the help of the "SysInfo Tools DBX File Viewer" tool (https://www.sysinfotools.com/recovery/dbx-file-viewer.php), which found email messages with subjects such as "CC's (Credit Card) CVV2 4 (for) Sale", "US and Int. PayPal's for sale", "Free Credit Card Validator and Extractor" and "Ebay Accts Available" (Figure 44), which demonstrate the suspect's direct or indirect involvement with financial crime cases.

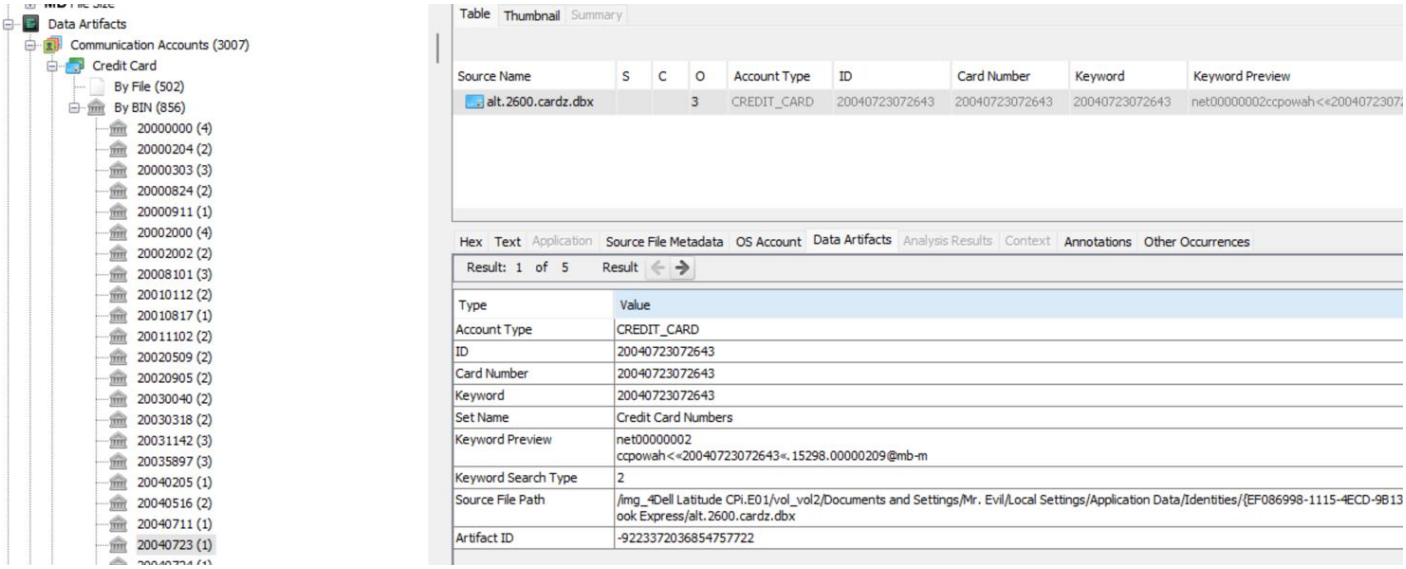

Figure 43 - The file "alt.2600.cardz.dbx"

C:\Users\Administrator\Desktop\Outlook Express\alt.2600.cardz.dbx

From	Subject	To	Email Status	Date/Time
<Filter>	<Filter>	<Filter>	<Filter>	<Filter>
"id scanz <idscanz@aol.co...	ebay accts available		Existing	Sun Jul 11 10:01:58 2004
"PsYcHo <krawling@trance...	CC's with CVV2 4 Sale		Existing	Sun Jul 11 13:49:08 2004
"id scanz <idscanz@aol.co...	CC's with CVV2 4 Sale		Existing	Mon Jul 12 02:16:52 2004
"just_me <who_cares162@...	Free non ratio ftp's		Existing	Mon Jul 12 16:02:07 2004
"CardMaster19 <yabapmatt...	Magnetic Stripe Encoding Problem		Existing	Wed Jul 14 23:34:56 2004
"sarah@gmail.com <sarah...	My Silicon Titties 9668		Existing	Fri Jul 16 23:11:20 2004
"den <""user <dadano\"@h...	QUESTIONS ANSWERED		Existing	Sat Jul 17 22:53:53 2004
"castro <cazeza@sapo.pt>"	New way to get Credit Cards!		Existing	Sun Jul 18 02:03:11 2004
"officerdibble <officerdibble...	New way to get Credit Cards!		Existing	Sun Jul 18 15:32:12 2004
"officerdibble <officerdibble...	fuckin idiots		Existing	Sun Jul 18 15:38:04 2004
"rad-montreal <redbel@hot...	Magnetic Stripe Encoding Problem		Existing	Sun Jul 18 21:26:22 2004
"rad-montreal <redbel@hot...	Magnetic Stripe Encoding Problem		Existing	Sun Jul 18 21:27:23 2004
"rad-montreal <redbel@hot...	carerz partner from canada needed		Existing	Mon Jul 19 21:49:06 2004
"rad-montreal <redbel@hot...	cading partner from canada needed		Existing	Tue Jul 20 20:43:21 2004
"Amisima <dh7777@counte...	ICVerify		Existing	Wed Jul 21 00:43:18 2004
"John Cronin <gatekeeper...	where are all the		Existing	Wed Jul 21 21:19:38 2004
"Hans van Eynsbergen <Ha...	Osama Found Hanged		Existing	Thu Jul 22 19:49:19 2004
"Yomamma bin Crawdaddin ...	Osama Found Hanged		Existing	Fri Jul 23 03:49:05 2004
"id scanz <idscanz@aol.co...	ccpowah		Existing	Fri Jul 23 14:26:43 2004
"Ammon-Ra <ammon-ra@ofi...	US and Int. PayPal's for sale		Existing	Fri Jul 23 23:04:04 2004
"robot junkie <robotjunkie39...	Free one for all you! Good cc inside		Existing	Fri Jul 23 23:09:33 2004
"id scanz <idscanz@aol.co...	german aol axx - lol		Existing	Sat Jul 24 21:35:19 2004
"robot junkie <robotjunkie39...	US and Int. PayPal's for sale		Existing	Sun Jul 25 05:11:46 2004
"robot junkie <robotjunkie39...	free one for al of you guts who need one HURRY HURRY MY FRIENDS		Existing	Sun Jul 25 09:40:47 2004
"take me <yesiam@imabadli...	free card, FULL info, working now! snatch it quick!		Existing	Sun Jul 25 18:34:29 2004
"AllNet2007 <hooboo4777...	Tutorial site		Existing	Sun Jul 25 19:28:40 2004
"id scanz <idscanz@aol.co...	free card, FULL info, working now! snatch it quick!		Existing	Sun Jul 25 22:17:33 2004
"prpro <prpro@prweb.com>"	EGOLD- MAKE THOUSANDS- UNLIMITED DEPOSITS IN YOUR EGOLD ACCT-EARLY STAGES, G...		Existing	Mon Jul 26 13:51:21 2004
"Rona <wjytdtgu@viwsdsgs...	New & used car prices		Existing	Mon Jul 26 15:48:10 2004
"johny <anonymous_pal4ev...	free credit card validator and extractor		Existing	Mon Jul 26 23:34:22 2004
"johny <anonymous_pal4ev...	free credit card validator and extractor - link		Existing	Tue Jul 27 00:00:49 2004
"id scanz <idscanz@aol.co...	free credit card validator and extractor - link		Existing	Tue Jul 27 01:35:11 2004
"Lincoln'smole <bigtalker3@...	ebay accts available		Existing	Tue Jul 27 01:54:23 2004

Figure 44 - Emails related to economic crimes

3.14. Investigation of the existence of additional accomplices

After examining the virtual disk, it appears that the suspect acted alone, as no evidence was found to implicate additional accomplices. More specifically, no emails

or online conversations (mIRCs) were found to prove the existence of accomplices. It was also established, through the “Nethood” directory (C:/Documents and Settings/Mr. Evil/Nethood), which keeps a history of the computers to which a user had access at a given time, that the suspect was remotely logged on to a computer (4.12.220.254), the name of which was “ANDREWS-1”, to access network volumes [“andrews (c)”, “a”, “d”, “e”], an optical media drive [“CD Drive (F)”] (Figure 45), to use an “HP” brand printer (HP LaserJet 2100) via the network port “Ne00” (Figure 46) (evidence path: C:/$Unalloc/Unalloc_20051_1684736000_3639811072) (Figure 47) (evidence path: C:/Documents and Setting/Mr. Evil/NTUSER.DAT), but also for reading and sharing files (Figure 48) (evidence path: C:/Documents and Settings/Mr. Evil/Local Settings/History/History.IE5/index.dat) (Figure 48) (evidence path: C:/Documents and Settings/Mr. Evil/Local Settings/History/History.IE5/index.dat). Regarding the latter, the path “C:/Windows/system32/config/software\Microsoft\Windows NT\CurrentVersion/Explorer/RecentDocs” contains, in descending order, the last seven (7) files accessed by the suspect (Figure 49). Finally, in the path “C:/Documents and Setting/Mr. Evil/NTUSER.DAT\Microsoft\Windows NT\CurrentVersion/Explorer/ComputerDescriptions”, is the history of the most frequently visited locations by the suspect (Figure 50). However, it was not possible to directly associate him with one or more accomplices.

Figure 45 - The contents of the "Nethood" folder

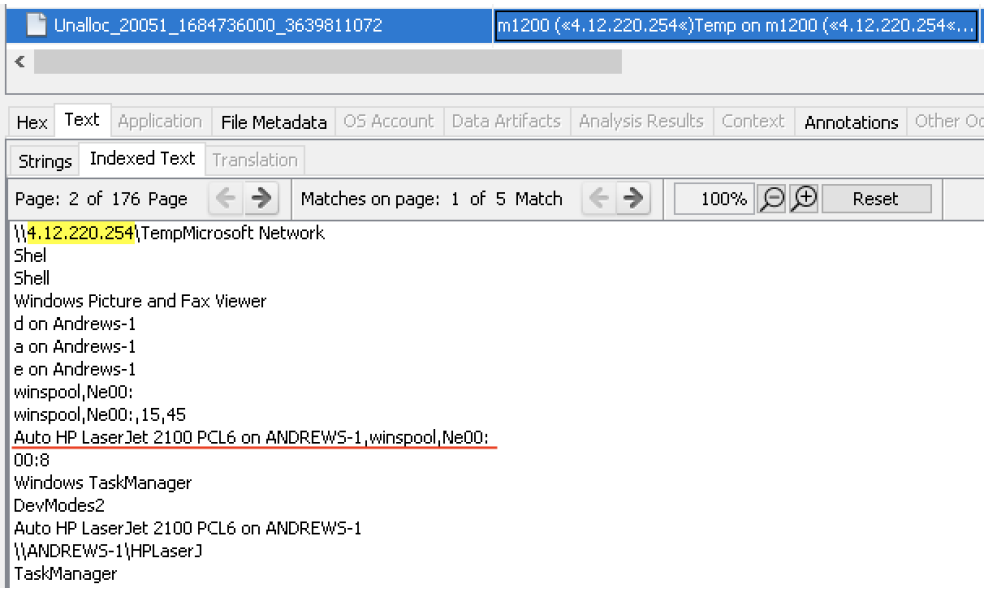

Figure 46 - Information about the "HP LaserJet 2100" printer

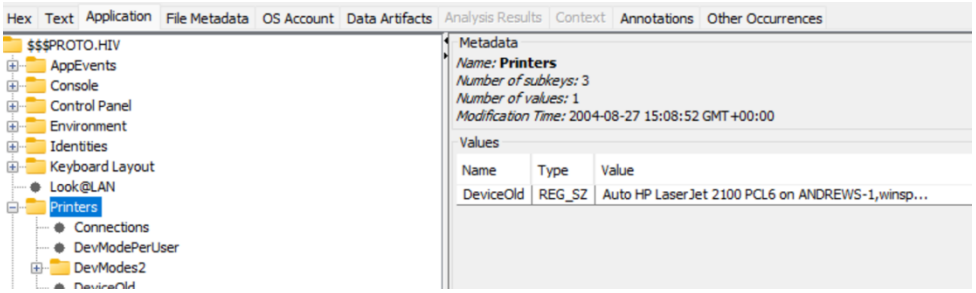

Figure 47 - Information about the "HP LaserJet 2100" printer in the Registry

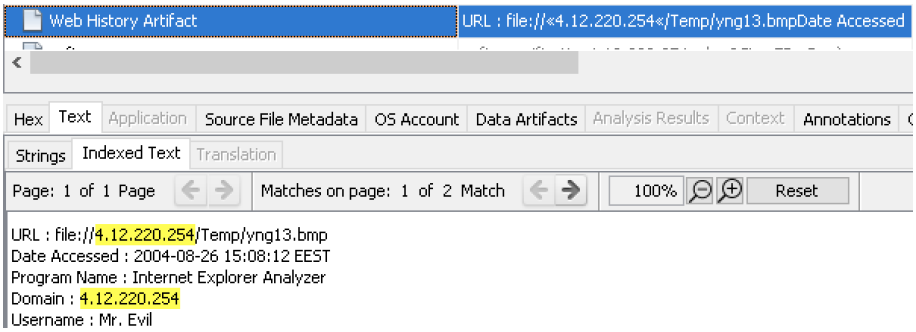

Figure 48 - Proof of file sharing to/from a remote location

```
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key
RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Thu Aug 26 15:08:15 2004 (UTC)
  7 = Temp on m1200 (4.12.220.254)
  6 = yng13.bmp
  5 = channels
  4 = channels.txt
  3 = GhostWare
  2 = Receipt.rtf
  1 = Anonyymizer
  0 = keys.txt
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.bmp
LastWrite Time Thu Aug 26 15:08:12 2004 (UTC)
MRUListEx = 0
  0 = yng13.bmp
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.rtf
LastWrite Time Fri Aug 20 15:09:16 2004 (UTC)
MRUListEx = 0
  0 = Receipt.rtf
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt
LastWrite Time Fri Aug 20 15:50:40 2004 (UTC)
MRUListEx = 1,0
  1 = channels.txt
  0 = keys.txt
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
LastWrite Time Thu Aug 26 15:08:14 2004 (UTC)
MRUListEx = 3,2,1,0
  3 = Temp on m1200 (4.12.220.254)
  2 = channels
  1 = GhostWare
  0 = Anonyymizer
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\NetHood
LastWrite Time Thu Aug 26 15:08:15 2004 (UTC)
MRUListEx = 0
  0 = \\4.12.220.254\Temp
```

Figure 49 - List of the last seven (7) files accessed by the suspect

Value Name	Value Type	Data
4.12.220.254	RegSz	m1200
TOWER	RegSz	Tower
TOWER2	RegSz	
ECSAP_LAB_SRVR	RegSz	
ECSAP_LMS	RegSz	ECSAP_LMS
N-1A9ODN6ZXK4LQ	RegSz	
BB	RegSz	
D77KSG41	RegSz	
PREFERRE-GG31M4	RegSz	
SM181068849	RegSz	
ANDREWS-1	RegSz	

Figure 50 - The history of the most frequently visited locations by the suspect

3.15. Investigation of the existence of malware (virus, worms, backdoor, etc.) that can be invoked by the suspect as a mitigating factor

As for the process of investigating the existence of malware on the virtual disk, the mounting of the virtual disk was performed on a local computer running the “Kali

Linux" operating system, so that a scan could then be carried out with the help of the "Clamav" tool (https://www.clamav.net/).

First, the "EWF-tools" tool was installed, using the command "apt install ewf-tools". Then, using the command "ewfmount 4Dell\ Latitude\ CPi.E01 output/", the files contained in the virtual disks "4Dell Latitude CPi.E01" and "4Dell Latitude CPi.E02" are converted to "RAW" format and placed in the "output" folder. Then, by running the command "mount output/ewf1 /mnt -o ro,offset=$((512*512))", the contents of the "output" folder are mounted to the "/mnt" folder, which is now a hard disk on the local system.

Then, it is possible to scan the hard disk with the command "clamscan -ir /mnt", the results of which are shown below (Figure 51):

```
 1 /mnt/My Documents/COMMANDS/enum.exe: Win.Tool.EnumPlus-1 FOUND
 2 /mnt/My Documents/COMMANDS/SAMDUMP.EXE: Win.Trojan.Pwdump-2 FOUND
 3 /mnt/My Documents/COMMANDS/snitch.exe: Win.Trojan.Snitch-1 FOUND
 4 /mnt/My Documents/ENUMERATION/NT/enum/enum.tar.gz: Win.Tool.EnumPlus-1 FOUND
 5 /mnt/My Documents/ENUMERATION/NT/enum/files/enum.exe: Win.Tool.EnumPlus-1 FOUND
 6 /mnt/My Documents/ENUMERATION/NT/Legion/Chrono.dl_: Win.Trojan.Bruteforce-3 FOUND
 7 /mnt/My Documents/ENUMERATION/NT/Legion/NetTools.ex_: Win.Trojan.Spion-4 FOUND
 8 /mnt/My Documents/ENUMERATION/NT/ntreskit.zip: Win.Trojan.Nemo-1 FOUND
 9 /mnt/My Documents/EXPLOITATION/NT/Brutus/BrutusA2.exe: Win.Tool.Brutus-3 FOUND
10 /mnt/My Documents/EXPLOITATION/NT/brutus.zip: Win.Tool.Brutus-3 FOUND
11 /mnt/My Documents/EXPLOITATION/NT/Get Admin/GetAdmin.exe: Win.Exploit.WinNT-3 FOUND
12 /mnt/My Documents/EXPLOITATION/NT/lsadump2/lsadump2.exe: Win.Trojan.Lsadump-1 FOUND
13 /mnt/My Documents/EXPLOITATION/NT/lsadump2/lsadump2.zip: Win.Trojan.Lsadump-1 FOUND
14 /mnt/My Documents/EXPLOITATION/NT/netbus/NetBus170.zip: Win.Trojan.Netbus-2 FOUND
15 /mnt/My Documents/EXPLOITATION/NT/sechole/SECHOLE.EXE: Win.Trojan.Sehole-1 FOUND
16 /mnt/My Documents/EXPLOITATION/NT/sechole/sechole3.zip: Win.Trojan.Sehole-1 FOUND
17 /mnt/My Documents/FOOTPRINTING/NT/superscan/superscan.exe: Win.Trojan.Agent-6240252-0 FOUND
18 /mnt/My Documents/FOOTPRINTING/UNIX/unix_hack.tgz: Unix.Malware.Agent-6781976-0 FOUND
19 /mnt/Program Files/Cain/Abel.dll: Win.Trojan.Cain-9 FOUND
20
21
22 ---------- SCAN SUMMARY ----------
23 Known viruses: 8666818
24 Engine version: 1.0.1
25 Scanned directories: 766
26 Scanned files: 11305
27 Infected files: 19
28 Data scanned: 2166.89 MB
29 Data read: 1768.03 MB (ratio 1.23:1)
30 Time: 2281.042 sec (38 m 1 s)
31 Start Date: 2023:05:19 11:02:22
32 End Date:   2023:05:19 11:40:23
```

Figure 51 - Scanning the suspect's hard disk for malware

In more detail:

- **My Documents/COMMANDS/enum.exe:** Tool that intercepts information about users, groups, shared items and basic information on systems running Windows NT, 2000 and XP operating systems.
- **My Documents/COMMANDS/SAMDUMP.EXE:** Tool that dumps the hash of user passwords found in the "SAM" file

(C:/Windows/system32/config/SAM) on Windows NT, 2000, XP and Vista operating systems.

- **My Documents/COMMANDS/snitch.exe:** Tool that restores the asterisks, found in the password fields, to the characters they hide.
- **My Documents/ENUMERATION/NT/enum/enum/enum.tar.gz:** Similar to “My Documents/COMMANDS/enum.exe”, with the difference that it is in a compressed file format (tar.gz).
- **My Documents/ENUMERATION/NT/enum/files/enum.exe:** Similar to “My Documents/COMMANDS/enum.exe”.
- **My Documents/ENUMERATION/NT/Legion/Chrono.dl_:** Library file of the “Legion” malware, used as a “NetBIOS scanner”.
- **My Documents/ENUMERATION/NT/Legion/NetTools.ex_:** Executable file of the “Legion” malware, used as a “NetBIOS scanner”.
- **My Documents/ENUMERATION/NT/ntreskit.zip:** Compressed file containing executable files used for enumeration.
- **My Documents/EXPLOITATION/NT/Brutus/BrutusA2.exe:** Tool that performs brute force attacks to recover passwords.
- **My Documents/EXPLOITATION/NT/brutus.zip:** Similar to “My Documents/EXPLOITATION/NT/Brutus/BrutusA2.exe”
- **My Documents/EXPLOITATION/NT/Get Admin/GetAdmin.exe:** Tool that allows a simple user to gain administrative rights.
- **My Documents/EXPLOITATION/NT/lsadump2/lsadump2.exe:** Tool that dumps users' hashes from RAM.
- **My Documents/EXPLOITATION/NT/lsadump2/lsadump2.zip:** Similar to “My Documents/EXPLOITATION/NT/lsadump2/lsadump2/lsadump2.exe”.
- **My Documents/EXPLOITATION/NT/netbus/NetBus170.zip:** Tool for remote computer management.
- **My Documents/EXPLOITATION/NT/sechole/SECHOLE.EXE:** Tool that allows an ordinary user to gain debug-level access, and then execute malicious code to gain administrative privileges.
- **My Documents/EXPLOITATION/NT/sechole/sechole3.zip:** Similar to “My Documents/EXPLOITATION/NT/sechole/SECHOLE.EXE”.

- **My Documents/FOOTPRINTING/NT/superscan/superscan.exe:** Port scanning application.
- **My Documents/FOOTPRINTING/UNIX/unix_hack.tgz:** According to the "Autopsy" tool, it is a "zipbomb", i.e. a compressed file whose purpose is to crash a system during its decompression.
- **Program Files/Cain/Abel.dll:** Library file of the Cain and Abel malware, which is a password recovery tool, allowing various types of passwords to be recovered through network sniffing.

The majority of the above tools are hacking tools and cannot be exploited to gain remote access to the suspect's computer. The only exception to this is the tool "NetBus170.zip", which is used for this purpose. However, looking at its creation and access dates (Figure 52), it can be concluded that it was never executed. Therefore, any claims made by the suspect that he was not the one acting during the attacks are not valid.

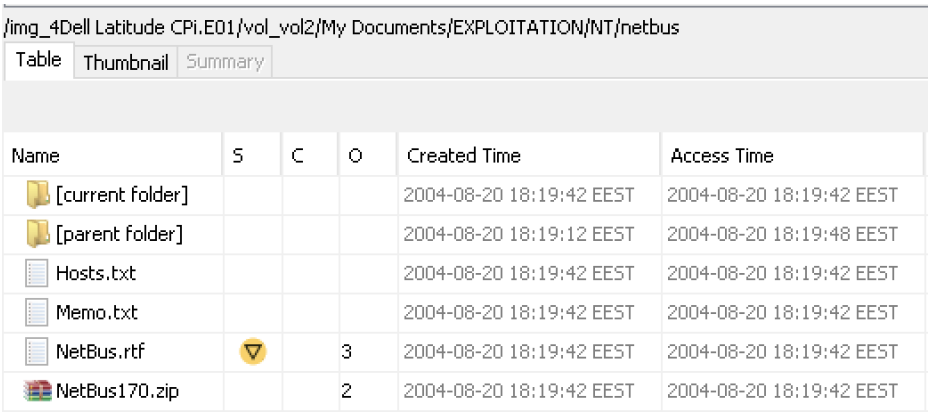
/img_4Dell Latitude CPi.E01/vol_vol2/My Documents/EXPLOITATION/NT/netbus

Table | Thumbnail | Summary

Name	S	C	O	Created Time	Access Time
[current folder]				2004-08-20 18:19:42 EEST	2004-08-20 18:19:42 EEST
[parent folder]				2004-08-20 18:19:12 EEST	2004-08-20 18:19:48 EEST
Hosts.txt				2004-08-20 18:19:42 EEST	2004-08-20 18:19:42 EEST
Memo.txt				2004-08-20 18:19:42 EEST	2004-08-20 18:19:42 EEST
NetBus.rtf			3	2004-08-20 18:19:42 EEST	2004-08-20 18:19:42 EEST
NetBus170.zip			2	2004-08-20 18:19:42 EEST	2004-08-20 18:19:42 EEST

Figure 52The creation and access dates of the "NetBus170.zip" file

3.16. Additional findings

3.16.1. Computer name

The name of the computer is "N-1A9ODN6ZXK4LQ" (C:/Windows/System32/config/system\ControlSet001\Control\ComputerName\ComputerName\ComputerName") (Figure 53).

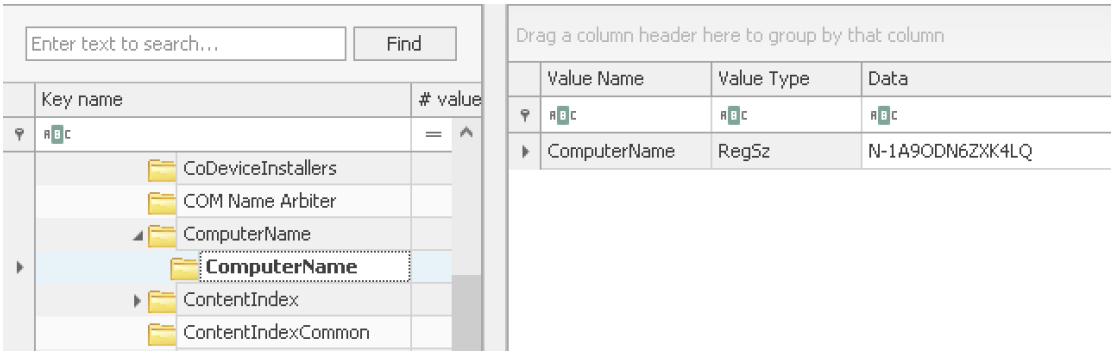

Figure 53 - The name of the computer

3.16.2. Laptop's serial number and date of image creation

After installing the "EWF-tools" tool, the details of the virtual disk host were retrieved via the command "ewfinfo 4Dell\ Latitude\ CPi.E01" (Figure 54).

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ewfinfo 4Dell\ Latitude\ CPi.E01
ewfinfo 20140813

Acquiry information
        Case number:            Greg Schardt
        Description:            Dell Latitude CPi
        Examiner name:          Shane Robinson
        Evidence number:        1 of 1
        Notes:                  sn# VLQLW  hdsn# RQQF7429
        Acquisition date:       Wed Sep 22 10:06:04 2004
        System date:            Wed Sep 22 10:06:04 2004
        Operating system used:  Windows XP
        Software version used:  4.19a
        Password:               N/A

EWF information
        File format:            EnCase 4
        Sectors per chunk:      64
        Compression method:     deflate
        Compression level:      no compression

Media information
        Media type:             fixed disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      9514260
        Media size:             4.5 GiB (4871301120 bytes)

Digest hash information
        MD5:                    aee4fcd9301c03b3b054623ca261959a
```

Figure 54 - The details of the virtual disk

3.16.3. Print queue and printers

No file traces were found in the print queue (C:/Windows/System32/spool/PRINTERS). The only printer that was connected to the

system, based on the “Printers” subkey (C:/Windows/System32/config/software/Microsoft\Windows NT\CurrentVersion\Print\Printers), is the “HP LaserJet 2100” printer (Figure 55) in the network path “\ANDREWS-1\HPLaserJ”.

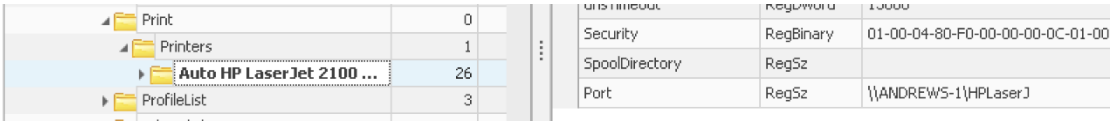

Figure 55 - The only printer that was connected to the system

3.16.4. Connected devices

In the suspect's computer there was an “IBM” brand hard drive with an “IDE” connection, a “Toshiba” brand “CD-ROM” drive (C:/Windows/System32/config/system\ControlSet001\Control\DeviceClasses) (Figure 56), as well as a USB Hub device (C:/Windows/System32/config/system\ControlSet001\Enum\USB\ROOT_HUB\4&15736a3f&0) (Figure 57).

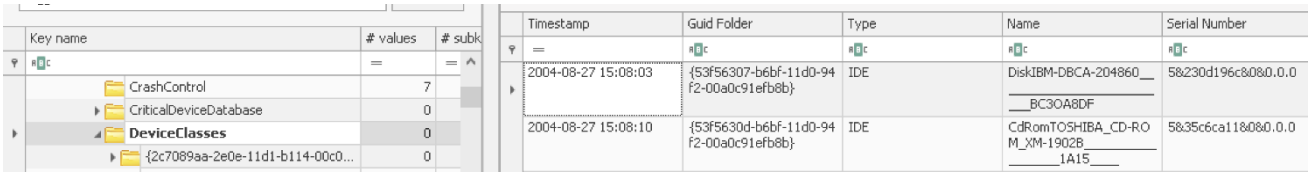

Figure 56 - The computer's hard disk and CD-ROM drive

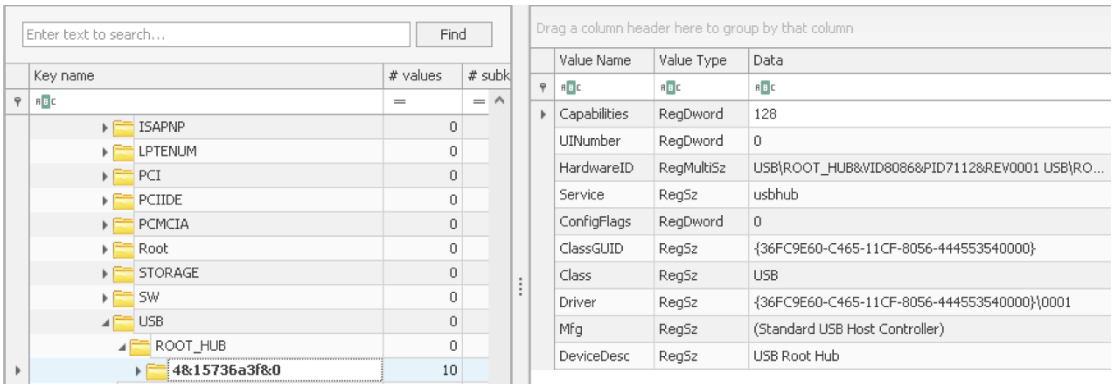

Figure 57 - The USB Hub device that was connected to the computer

3.16.5. Date and time the computer was last turned off

According to the date of the most recent entry in the “Windows” key of the path (C:/Windows/System32/config/system\ControlSet001\Control\Windows), which contains the value “ShutdownTime”, the date of the last computer shutdown was 2004-08-27 at 15:46:33 UTC (Figure 58).

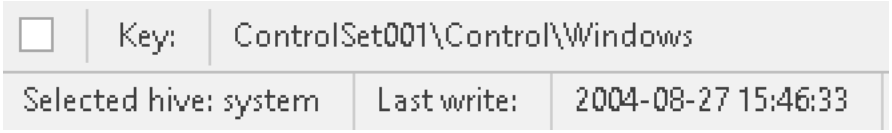

Figure 58 - The date the computer was last turned off

3.16.6. Details of the suspect's connection to the mIRC application

The suspect's connection details are:

user=Mini Me

email=none@of.ya

nick=Mr

anick=mrevilrulez

and are found in the file “mirc.ini”, located in the path (C:\Program Files\mIRC\mirc.ini)

3.16.7. The main email address of the suspect

Examining the suspect's online history (C:\Documents and Settings\Mr. Evil\Local Settings\Temporary Internet Files\Content.IE5) traces of activity since the creation of his “Yahoo” account were found (Figures 59 and 60).

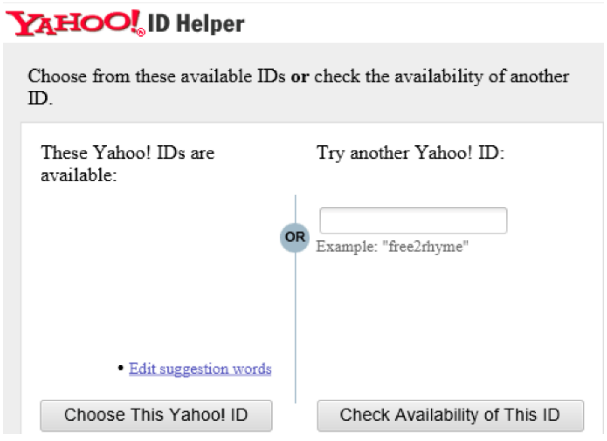

Figure 59 - Attempt to find an available "Yahoo ID" by the suspect

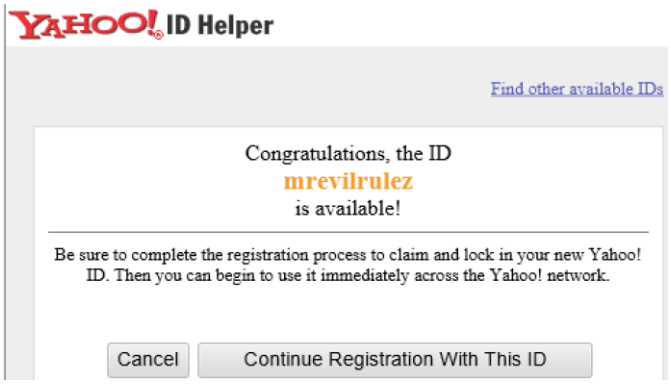

Figure 60 - Suspect finds an available "Yahoo ID"

Figures 61 and 62 show how the suspect managed to create his account, the address of which is: mrevilrulez@yahoo.com.

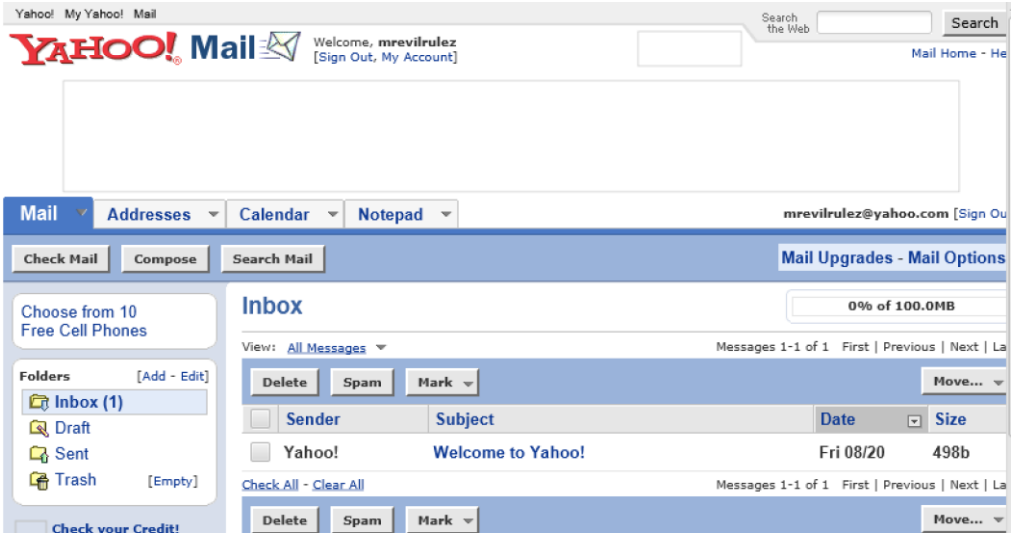

Figure 61 - The suspect's email inbox environment

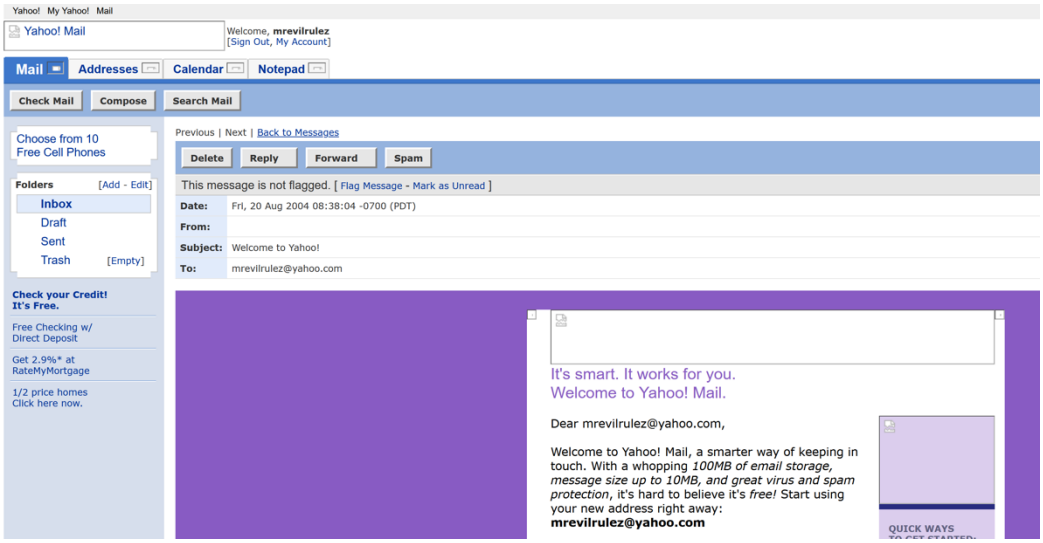

Figure 62 - The suspect's welcome email from "Yahoo! Mail"

3.16.8. Retrieved list of processes before the last hibernation

To retrieve the list of processes before the last hibernation, the following procedure was followed:

1. The Volatility 2 tool (https://github.com/volatilityfoundation/volatility/wiki/Installation) was downloaded and installed on a Kali Linux operating system.
2. The file “hiberfil.sys” was converted to “raw memory dump” format using the command “vol.py imagecopy -f hiberfil.sys -O winxp.img”.
3. Using the command “vol.py -f winxp.img --profile=WinXPSP2x86 pslist” the following processes were exported (Figure 63):

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
0x80a91800	System	4	0	46	217	————	0	
0x8097ada8	smss.exe	416	4	3	21	————	0	2004-08-20 15:01:04 UTC+0000
0x8094f020	csrss.exe	472	416	11	306	0	0	2004-08-20 15:01:09 UTC+0000
0x80936970	winlogon.exe	500	416	22	500	0	0	2004-08-20 15:01:11 UTC+0000
0x80925318	services.exe	544	500	18	259	0	0	2004-08-20 15:01:15 UTC+0000
0x80923968	lsass.exe	556	500	21	311	0	0	2004-08-20 15:01:15 UTC+0000
0x80a2b0d0	svchost.exe	736	544	10	230	0	0	2004-08-20 15:01:22 UTC+0000
0x808e95e8	svchost.exe	788	544	82	1209	0	0	2004-08-20 15:01:22 UTC+0000
0x808d5890	svchost.exe	888	544	4	83	0	0	2004-08-20 15:01:25 UTC+0000
0x808cdb20	svchost.exe	900	544	15	163	0	0	2004-08-20 15:01:25 UTC+0000
0xffbda020	spoolsv.exe	1004	544	10	132	0	0	2004-08-20 15:01:27 UTC+0000
0xffba8020	explorer.exe	1312	1232	14	338	0	0	2004-08-20 15:01:33 UTC+0000
0xffb6f020	msmsgs.exe	1556	1312	3	119	0	0	2004-08-20 15:01:38 UTC+0000
0xffaa7020	mirc.exe	1564	1312	4	117	0	0	2004-08-20 15:39:10 UTC+0000
0xffb4b020	logonui.exe	608	500	3	129	0	0	2004-08-20 19:00:19 UTC+0000

Figure 63 - The list of processes before the last hibernation

3.16.9. Registry traces of a smart cards hardware

In the path “C:/Windows/System32/config/software\Schlumberger” traces of a product of the company “Schlumberger”, which specializes in the manufacture of smart cards, were found (Figure 64).

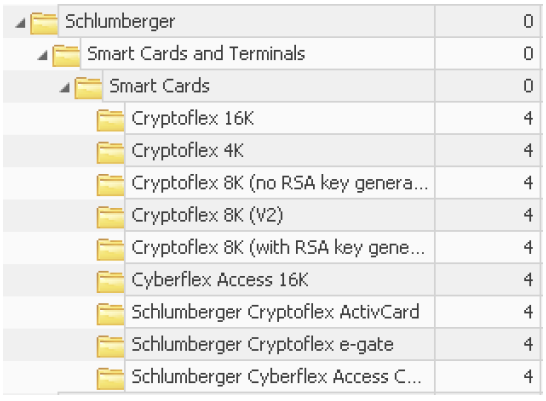

Figure 64 - Traces of "Schlumberger" product in the Registry

CHAIN OF CUSTODY

CONFIDENTIAL
DO NOT COPY

-EVIDENCE-

TO BE OPENED ONLY BY AUTHORISED AGENTS

Case No #: 01

Submitting Agent: Manios Athanasios, Bandis Christos

Device Type: Laptop

Manufacturer: Dell

Serial Number: #VLQLW

RAM: -

OS: Windows XP Professional

Architecture: x86

State: OFF

Connectivity: Ethernet, WiFi, Modem 56K

Victim's Full Name: -

Victim's SSN: -

Suspect's Full Name / Description: Greg Schardt (Mr. Evil)

Evidence Recovered By: -

Evidence Bag Sealed By: -

Date Sealed: 20/9/2021

Time Sealed: 8:30 PM

Phone #: 2133330300

Cell #: +30 6970334536, +30 6973979235

CHAIN OF CUSTODY

Label	Released By (ID#)	Received By (ID#)	Date / Time	Location / Comments
Evidence bag (sealed)	**#45 Police Officer Papadopoulos Constantine**	**#34 Bandis Christos**	**08/05/2023**	**A sealed evidence bag was received c/o Mr Manios Athanasios**

Evidence bag (sealed)	**#34 Bandis Christos**	**#23 Manios Athanasios**	**08/05/2023**	**Transfer of a sealed evidence bag to Mr Manios Athanasios**
Evidence bag (sealed)	**#23 Manios Athanasios**	**#23 Manios Athanasios**	**09/05/2023**	**Opening evidence bag with contents: 1 Dell brand laptop with serial number #VLQLW, 1 PCMCIA wireless network card, 1 external 802.11b frequency antenna**
1 Dell brand laptop with serial number #VLQLW, 1 PCMCIA wireless network card, 1 external 802.11b frequency antenna	**#23 Manios Athanasios**	**#12 George Georgiou (Data Storage and Retention Manager)**	**11/05/2023**	**Storage and safekeeping of the following items: 1 Dell brand laptop with serial number #VLQLW, 1 PCMCIA wireless network card, 1 external 802.11b frequency antenna**

F O R A G E N C Y L A B O N L Y

CONDITION OF EVIDENCE BAG UPON RECEIPT: SEALED

LAB CASE #: 01

RECEIVED BY: Bandis Christos

OPENED BY: Manios Athanasios

DATE: 09/05/2023 TIME: 10:00 AM DURATION: 48 hours

NOTES: The evidence bag was transported by Mr. Bandis and received sealed by Mr. Manios, indicating that the evidence remained unaltered during transport.

-SIGNATURES-

Bandis Christos Manios Athanasios

5. Appendix

5.1. Achievement of the objective

This technical report deals with the investigation of a cybercrime and the analysis of seized evidence in order to confirm or deny the suspect's guilt. As far as its requirements are concerned, they have been fully and thoroughly covered, with no exceptions, with sufficient information and images so that the evidence is presented in a comprehensible manner. The justification of the choices made in the collection of evidence is extensive, the description of the process of verifying the exact copy of the original digital evidence is detailed, as is the explanation of the results of the investigation. In conclusion, it has become clear that based on the technical analysis of this cybercrime, the suspect has committed criminal acts involving data theft. In addition, traces of child pornography and economic crimes were found on the suspect's computer. Finally, any allegation by the suspect that he did not commit the aforementioned acts himself is completely refuted.

5.2. List of Tables

5.3. List of Figures