Hacking Case

Digital Forensics Report

Panagiotis Kolliopoulos

September 2023

Intern on Zelus IKE

Abstract

In this scenario an old Dell CPi notebook computer has been found and it is suspected that a so-called hacking suspect “Greg Schardt“, is the owner of this device. A hard drive disc image has been generated and made available to us for analysis. We will analyze the disc using the free software Autopsy and we will try to answer 31 questions to gather evidence about this case.

Information

Forensics Examiner: Panagiotis Kolliopoulos
Offence: Hacking
Suspect: Greg Schardt

Scenario

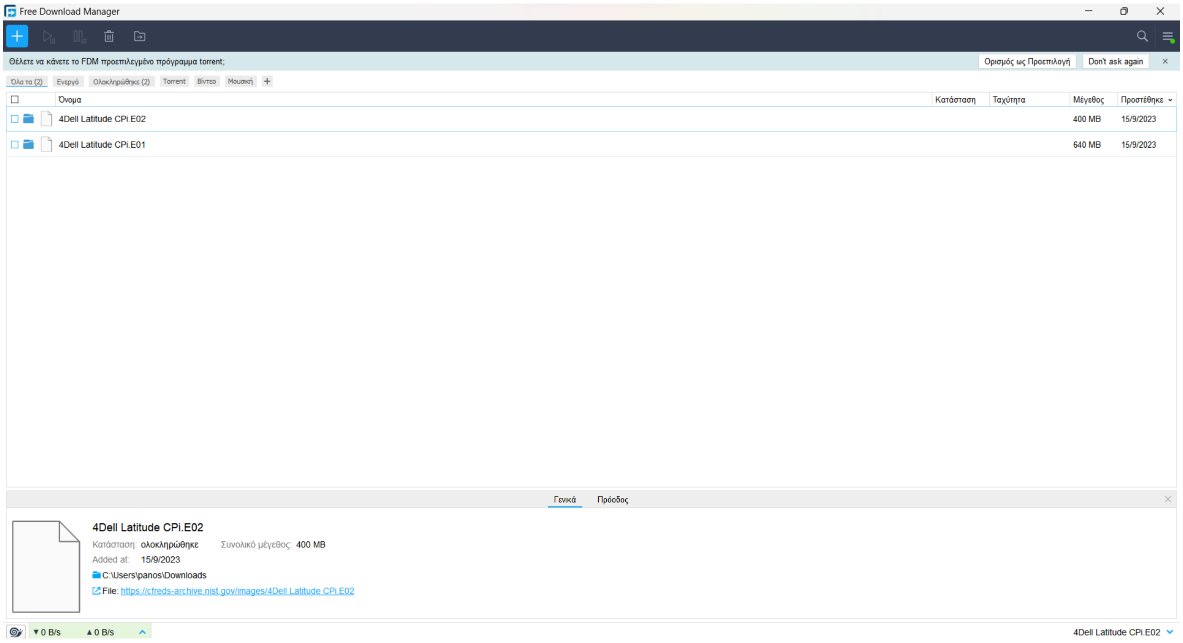
On 09/20/04, a Dell CPi notebook computer, serial # VLQLW, was found abandoned along with a wireless PCMCIA card and an external homemade 802.11b antennae. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, G=r=e=g S=c=h=a=r=d=t. (The equal signs are just to prevent web crawlers from indexing this name; there are no equal signs in the image files.) Schardt also goes by the online nickname of “Mr. Evil” and some of his associates have said that he would park his vehicle within range of Wireless Access Points (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords. This test image requires a variety of skills to answer the given questions. Find any hacking software, evidence of their use, and any data that might have been generated. Attempt to tie the computer to the suspect, G=r=e=g S=c=h=a=r=d=t.

Software that used

- Autopsy 4.20.0
- Free Download Manager
- Epoch Converter
- DCode v5.5
- OUI Lookup Tool

Evidence that collected

We have a disc drive image (split in 8 parts) and also an EnCase image that we collected from Hacking Case (nist.gov). The final format of the image will be the same, either using the disc drive image or the EnCase image. It will be a file full of symbols that we can see by just clicking on one of the image links: https://www.cfreds.nist.gov/images/4Dell%20Latitude%20CPi.E01. So, as the raw images and the EnCase images are in the same format, I chose the EnCase one. I am using Free Download Manager because I had issues downloading the images by myself. I just copied the link of the image file into this tool and it will download the data into one file.



Όνομα	Κατάσταση	Ταχύτητα	Μέγεθος	Προστέθηκε
4Dell Latitude CPi.E02			400 MB	15/9/2023
4Dell Latitude CPi.E01			640 MB	15/9/2023

4Dell Latitude CPi.E02
Κατάσταση: ολοκληρώθηκε Συνολικό μέγεθος: 400 MB
Added at: 15/9/2023
C:\Users\panos\Downloads
File: https://cfreds-archive.nist.gov/images/4Dell Latitude CPi.E02

Figure 1. Downloading images

For the analysis of the image, I’m using the open source Autopsy software for Windows. I just started a new “Case” in Autopsy by loading the forensic image. Then I landed on the main screen of the software and started the analysis of the disc image.
To test the image first we have to upload the image in Autopsy. The steps to upload the image in autopsy are shown below.

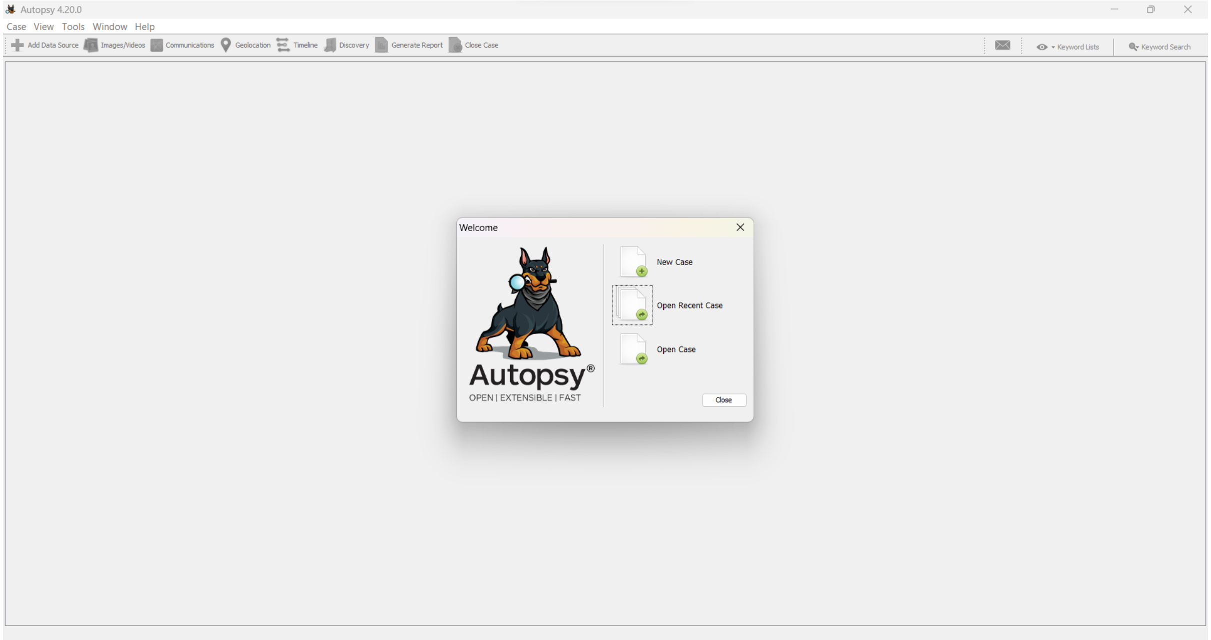
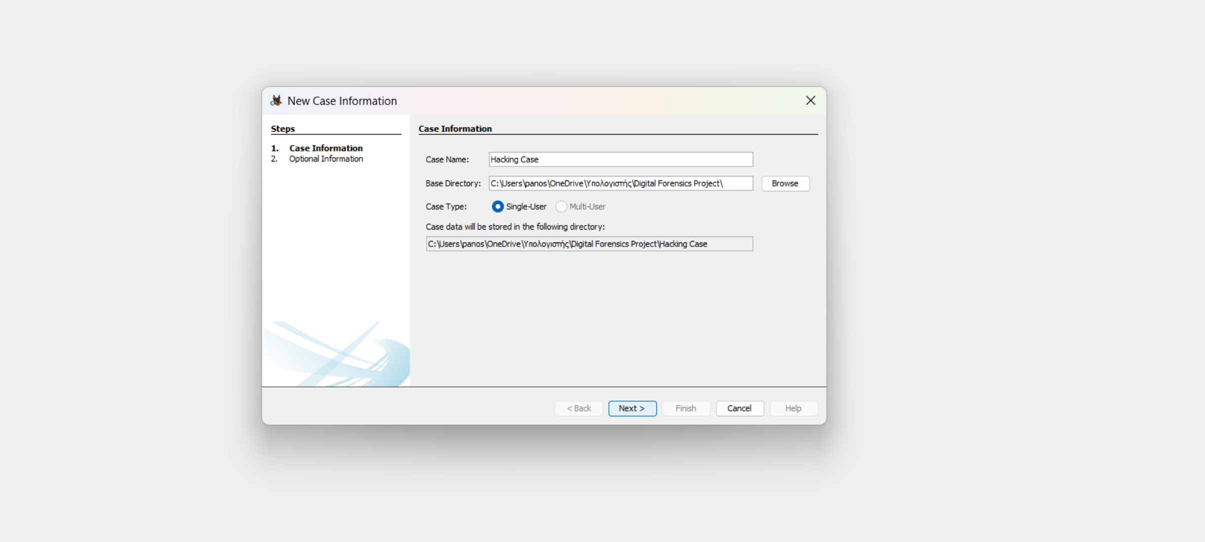


Figure 2. Autopsy home page



Case Name: Hacking Case

Base Directory: C:\Users\panos\OneDrive\Υπολογιστής\Digital Forensics Project\

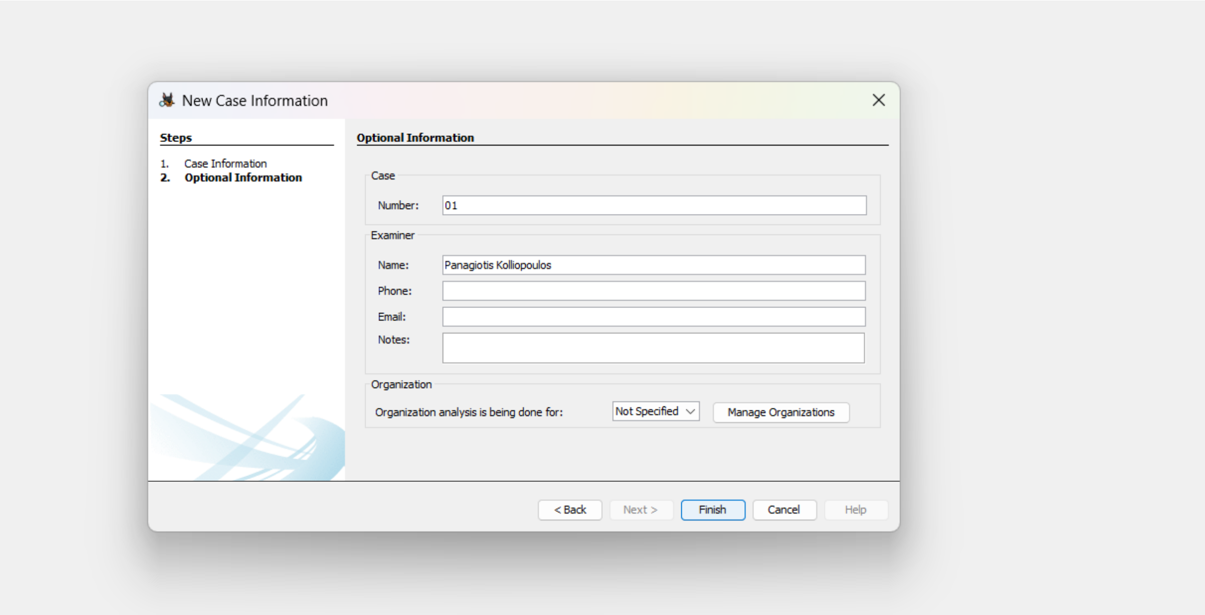
Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\panos\OneDrive\Υπολογιστής\Digital Forensics Project\Hacking Case

Figure 3. Entering case information

Figure 4. Entering optional information



Case

Number: 01

Examiner

Name: Panagiotis Kolliopoulos

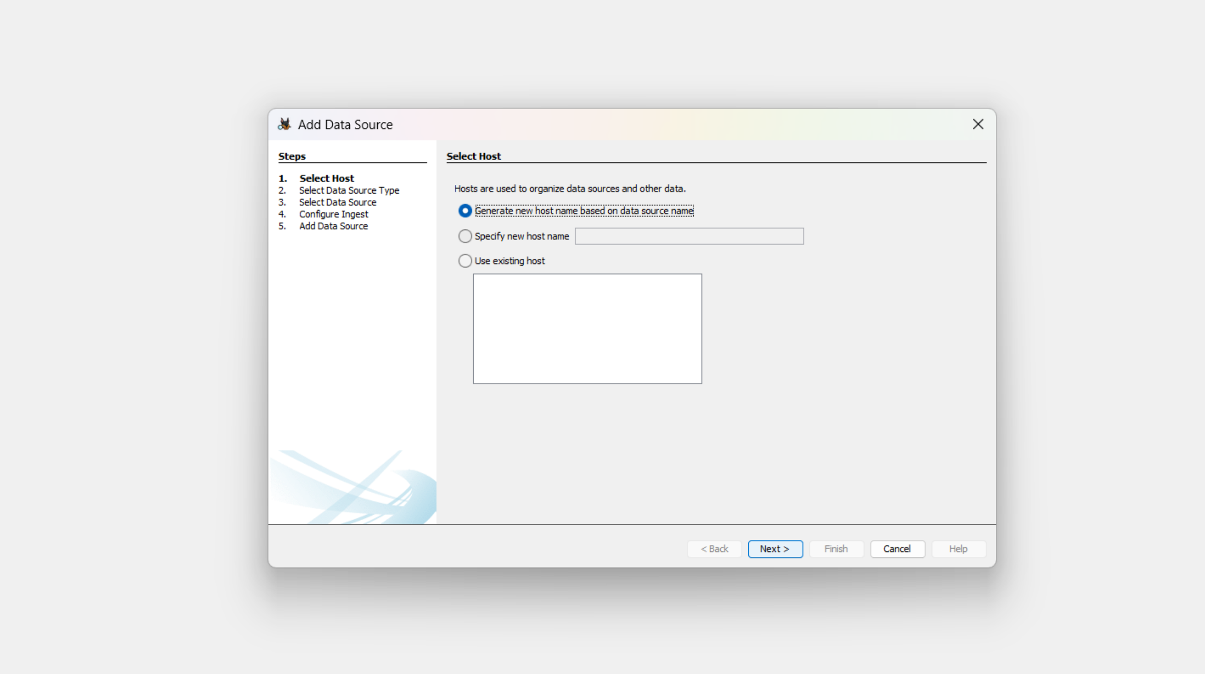
Phone:

Email:

Notes:

Organization

Organization analysis is being done for: Not Specified



Add Data Source

Steps

1. **Select Host**
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

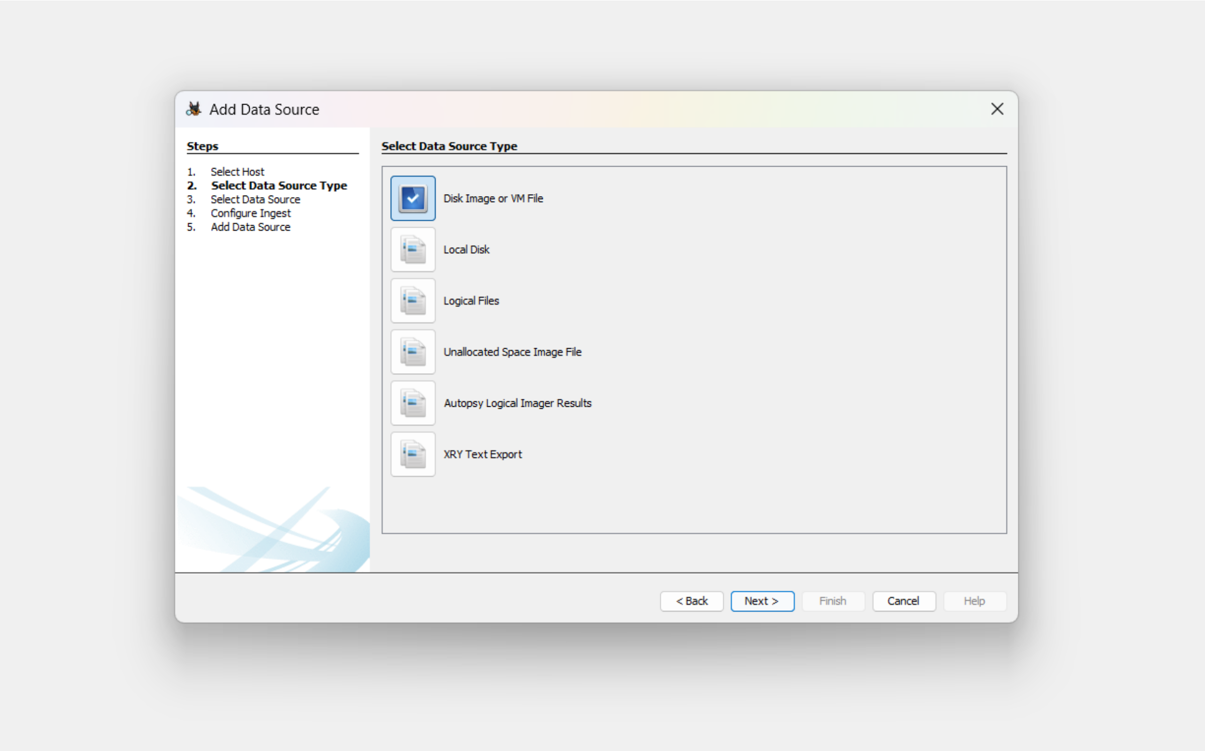
Hosts are used to organize data sources and other data.

● Generate new host name based on data source name

○ Specify new host name

○ Use existing host

Figure 5. SelectinHost



Add Data Source

Steps

1. Select Host
2. **Select Data Source Type**
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

☑ Disk Image or VM File

Local Disk

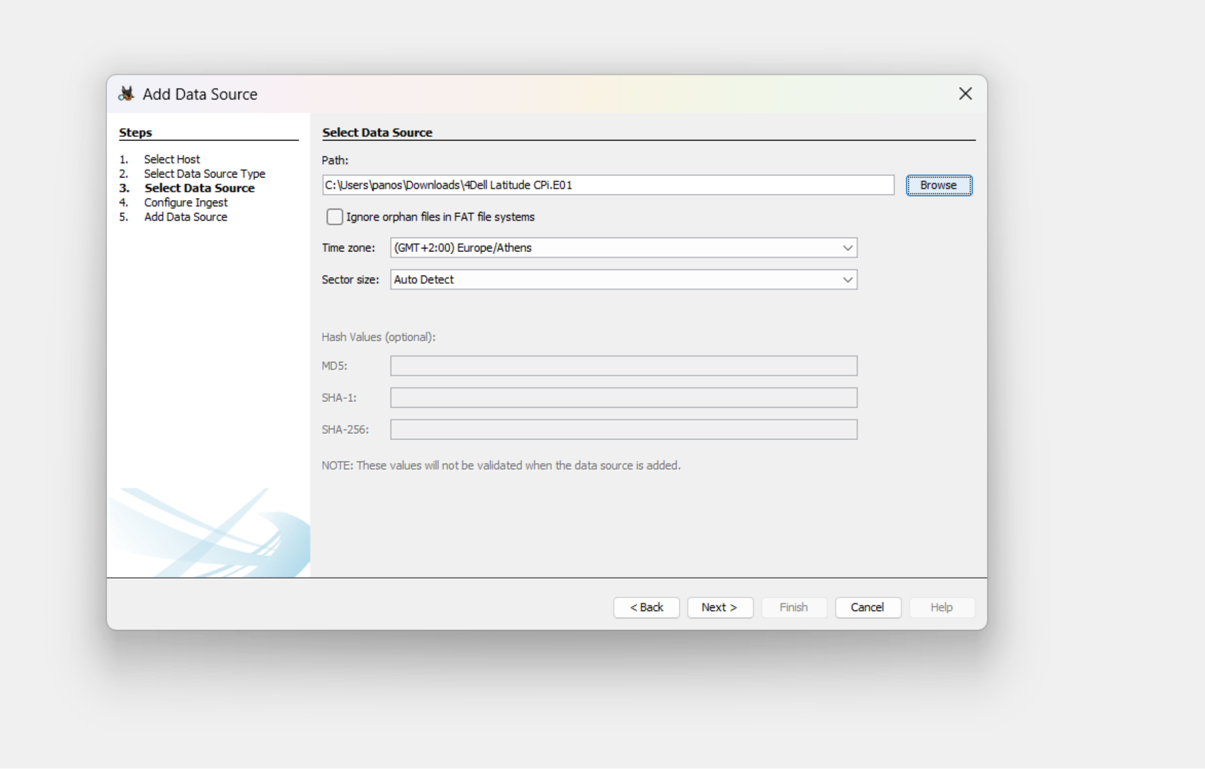
Logical Files

Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export

Figure 6. Selecting Data Source type



Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: C:\Users\panos\Downloads\4Dell Latitude CPi.E01

□ Ignore orphan files in FAT file systems

Time zone: (GMT+2:00) Europe/Athens

Sector size: Auto Detect

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Figure 7. Selecting Data Source Path

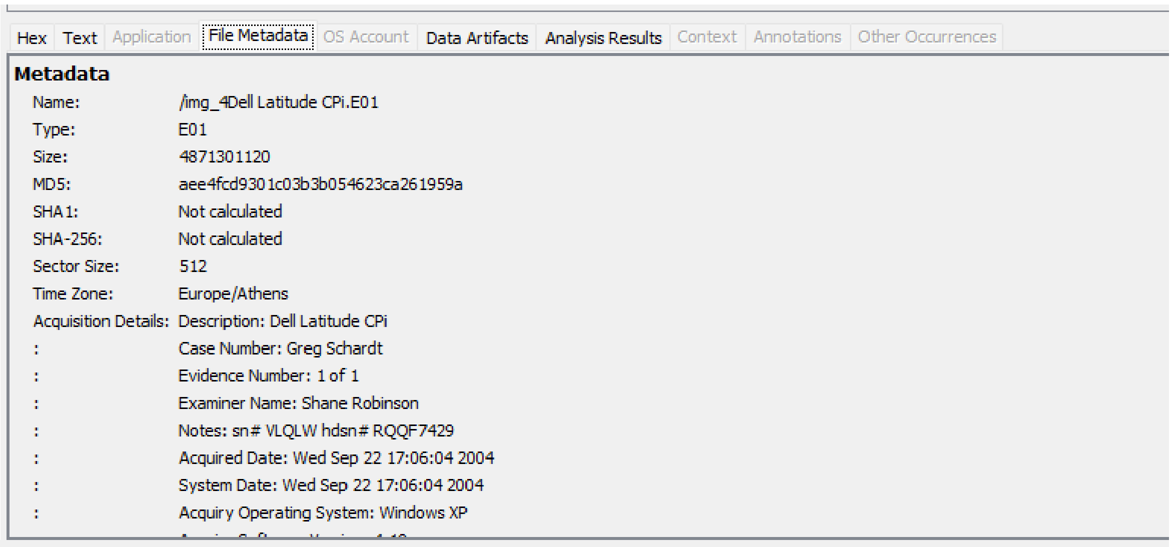
Then we click "Finish" and we are done. We can now start the analysis of the image!

Forensic examination of evidence

For the examination of evidence we had to answer the following questions.

1. What is the image hash? Does the acquisition and verification hash match?

2. What operating system was used on the computer?



Metadata

```
Name:                 /img_4Dell Latitude CPi.E01
Type:                 E01
Size:                 4871301120
MD5:                  aee4fcd9301c03b3b054623ca261959a
SHA1:                 Not calculated
SHA-256:              Not calculated
Sector Size:          512
Time Zone:            Europe/Athens
Acquisition Details:  Description: Dell Latitude CPi
:                     Case Number: Greg Schardt
:                     Evidence Number: 1 of 1
:                     Examiner Name: Shane Robinson
:                     Notes: sn# VLQLW hdsn# RQQF7429
:                     Acquired Date: Wed Sep 22 17:06:04 2004
:                     System Date: Wed Sep 22 17:06:04 2004
:                     Acquiry Operating System: Windows XP
```

Figure 8. Image hash and operating system

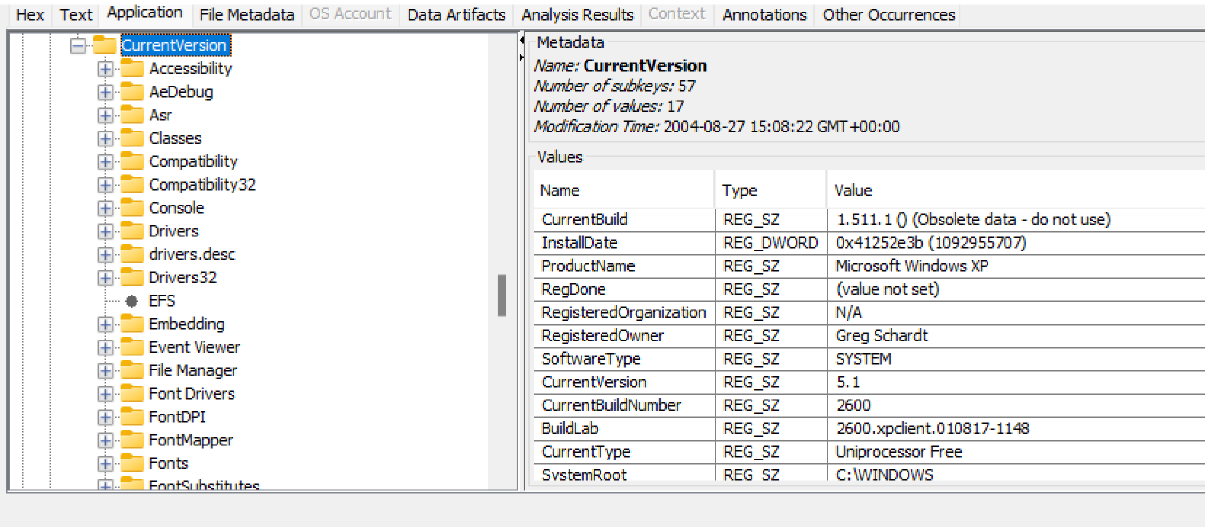
We find this info in "Acquisition details" which we find by clicking on Data Source -> image file. Then in the file metadata, we find the required info. Acquisition hash is not given in the above scenario. So, we don’t say whether the acquisition hash & verification hash match or not.

From the above method, we find that the Operating system used in the computer is “Microsoft Windows XP”.

3. When was the install date?

5. Who is the registered owner?

First, we google search to find the registry location where the windows installation date is stored. After the search, we find that the registry value is “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate”. So our full path is:- “C:\Windows\system32\config\Software\Microsoft\Windows NT\CurrentVersion\” and we will click on “Application”.



Metadata

Name: **CurrentVersion**
Number of subkeys: 57
Number of values: 17
Modification Time: 2004-08-27 15:08:22 GMT+00:00

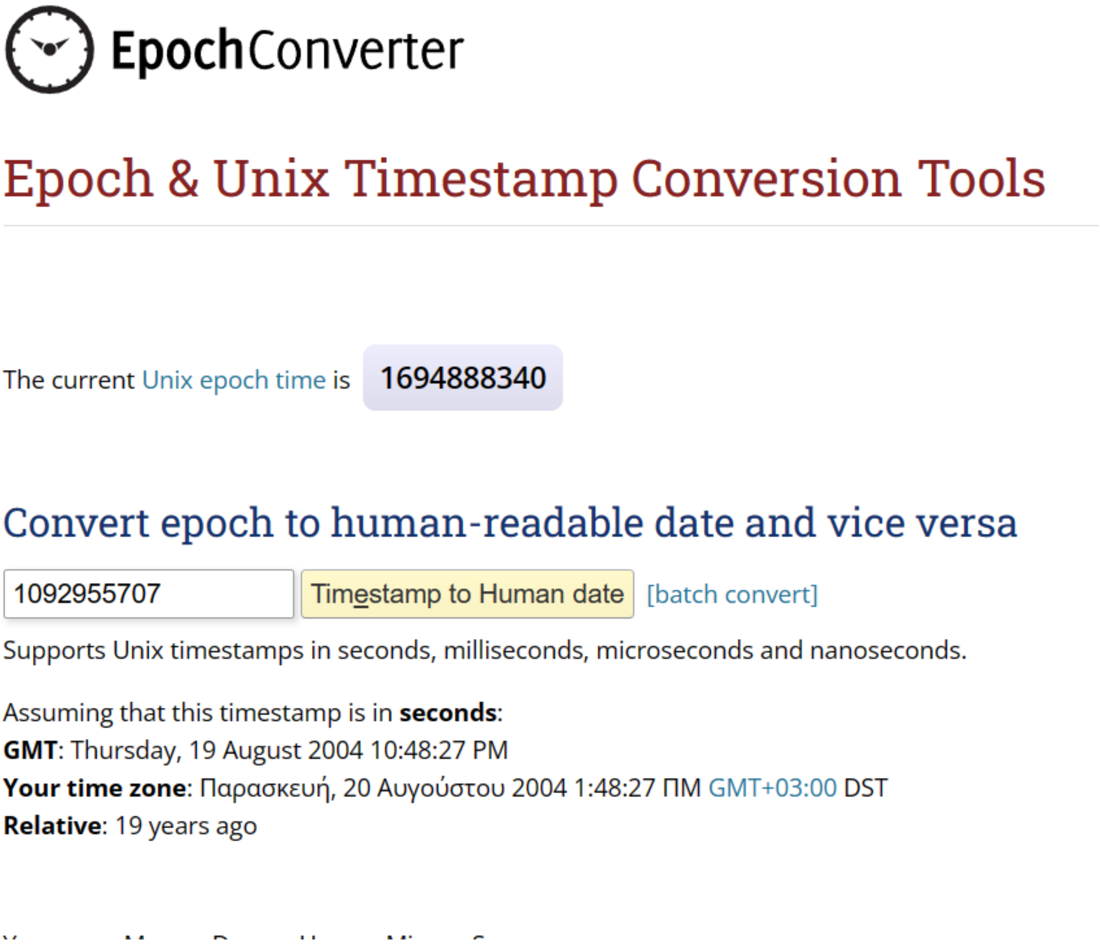
Values

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

Figure 9. Installation date and registered owner

Note: It is mentioned in the google search that it stores the date in UNIX time format. So after getting the time we have to convert it in human-readable format too.

On opening the required registry we find that the install date is “1092955707”. So we must convert it into a human-readable format. I used the Epoch Converter for the conversion.



Epoch & Unix Timestamp Conversion Tools

The current Unix epoch time is 1694888340

Convert epoch to human-readable date and vice versa

1092955707 Timestamp to Human date [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

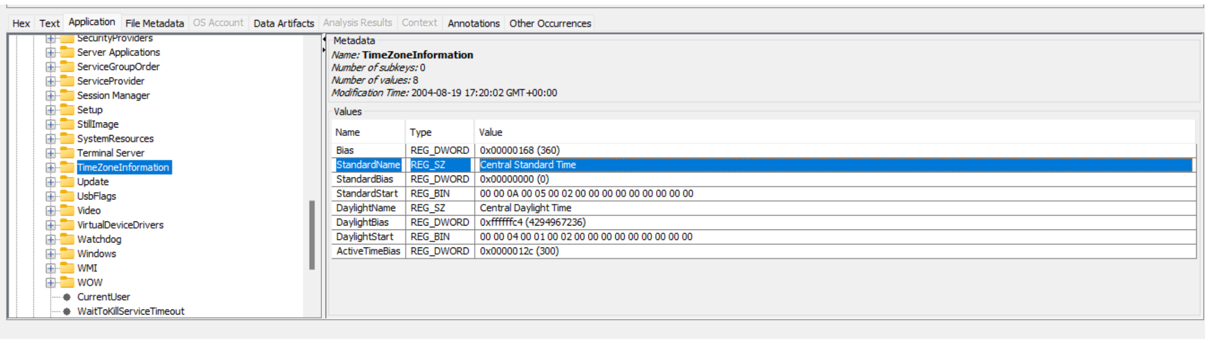
Assuming that this timestamp is in **seconds**:
GMT: Thursday, 19 August 2004 10:48:27 PM
Your time zone: Παρασκευή, 20 Αυγούστου 2004 1:48:27 ΠΜ GMT+03:00 DST
Relative: 19 years ago

Figure 10. Conversion of Unix time into GMT

So the install date in GMT is “Thursday, August 19, 2004 10:48:27 PM”. (Till now we don’t know the timezone of the acquired system so maybe the time is different in the system than the time which we find above.)

Then as we can observe, from this path we have the answer for question 5 too. On seeing the above image we find that the registered owner's name is “Greg Schardt”.

4. What is the timezone settings?
To find this first I search for the registry location which stores information related to timezone. After searching I found a site in which the location of the registry is given as “HKEY_LOCAL_MACHINE\system\CurrentControlSet\Control\TimeZoneInformation”.
So the Full Path is =
“C:\windows\system32\config\system\CurrentControlSet\Control\TimeZoneInformation”.
On visiting the required registry we find that the required timezone is “Central Standard Time (CST)”.



Metadata

Name: **TimeZoneInformation**
Number of subkeys: 0
Number of values: 8
Modification Time: 2004-08-19 17:20:02 GMT+00:00

Values

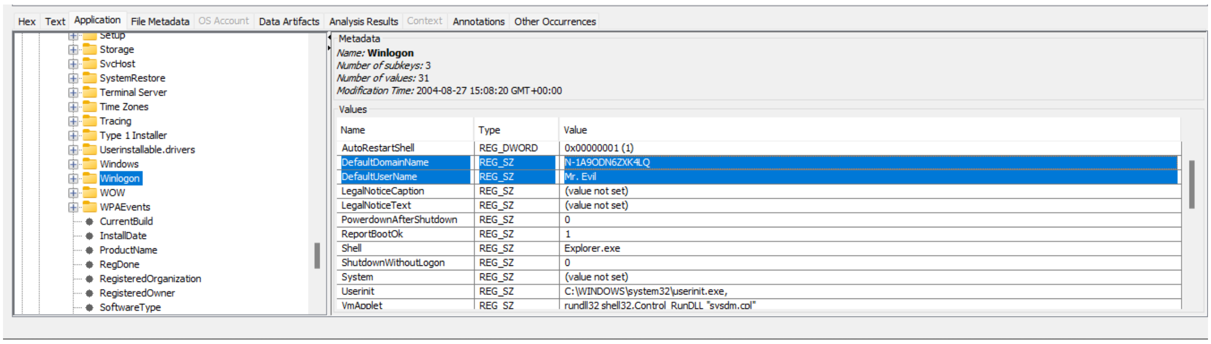
Name	Type	Value
Bias	REG_DWORD	0x00000168 (360)
StandardName	REG_SZ	Central Standard Time
StandardBias	REG_DWORD	0x00000000 (0)
StandardStart	REG_BIN	00 00 0A 00 05 00 02 00 00 00 00 00 00 00 00 00
DaylightName	REG_SZ	Central Daylight Time
DaylightBias	REG_DWORD	0xffffffc4 (4294967236)
DaylightStart	REG_BIN	00 00 04 00 01 00 02 00 00 00 00 00 00 00 00 00
ActiveTimeBias	REG_DWORD	0x0000012c (300)

Figure 11. Timezone information

Then I search for the relation between CST & GMT. After the search, we find that CST is (GMT- 06:00). So the time zone of the system is “Central Standard Time (GMT — 06:00)”. (NOTE: Now, the installation date of system according to its timezone is “Thursday, August 19, 2004 04:48:27 PM” instead of “Thursday, August 19, 2004 10:48:27 PM” because now we know that the timezone of the system is CST which is “GMT — 06:00”.)

6. What is the computer account name?
7. What is the primary domain name?
We searched on the internet again and we found that we have to check this registry “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon”. So the Full Path is “C:\windows\system32\config\software\Microsoft\Windows NT\CurrentVersion\Winlogon”
On seeing the DefaultUserName we say that the computer account name is “Mr. Evil”.

On seeing this registry we find out the answer to question 7 too, in the DefaultDomainName. So the primary domain name is “N-1A9ODN6ZXK4LQ”.



Metadata

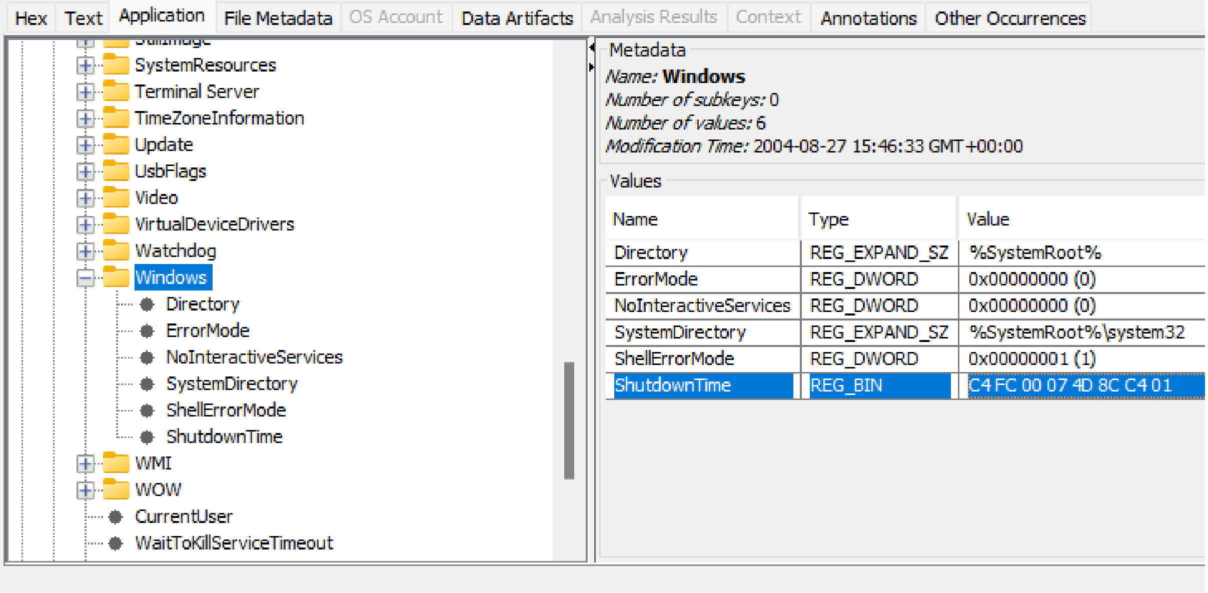
Name: **Winlogon**
Number of subkeys: 3
Number of values: 31
Modification Time: 2004-08-27 15:08:20 GMT+00:00

Values

Name	Type	Value
AutoRestartShell	REG_DWORD	0x00000001 (1)
DefaultDomainName	REG_SZ	N-1A9ODN6ZXK4LQ
DefaultUserName	REG_SZ	Mr. Evil
LegalNoticeCaption	REG_SZ	(value not set)
LegalNoticeText	REG_SZ	(value not set)
PowerdownAfterShutdown	REG_SZ	0
ReportBootOk	REG_SZ	1
Shell	REG_SZ	Explorer.exe
ShutdownWithoutLogon	REG_SZ	0
System	REG_SZ	(value not set)
Userinit	REG_SZ	C:\WINDOWS\system32\userinit.exe,
VmApplet	REG_SZ	rundll32 shell32.Control_RunDLL "sysdm.cpl"

Figure 12. Computer account and primary domain names

8. When was the last recorded computer shutdown date/time?
To find this, first I search for the registry that stores the last shutdown date/time. On searching, we found that the required registry is “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows\ShutdownTime”. On opening the registry in Autopsy we find that the Shutdown time is “C4 FC 00 07 4D 8C C4 01”.



SystemResources
Terminal Server
TimeZoneInformation
Update
UsbFlags
Video
VirtualDeviceDrivers
Watchdog
Windows
Directory
ErrorMode
NoInteractiveServices
SystemDirectory
ShellErrorMode
ShutdownTime
WMI
WOW
CurrentUser
WaitToKillServiceTimeout

Metadata

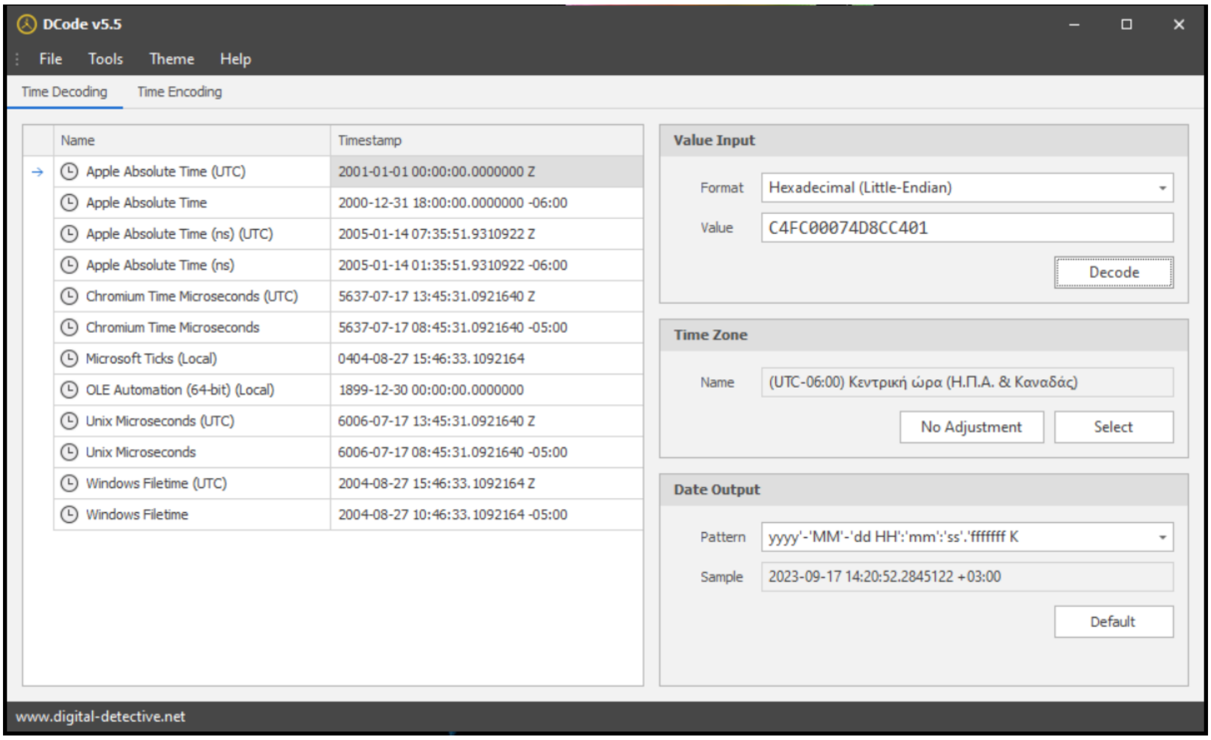
Name: **Windows**
Number of subkeys: 0
Number of values: 6
Modification Time: 2004-08-27 15:46:33 GMT+00:00

Values

Name	Type	Value
Directory	REG_EXPAND_SZ	%SystemRoot%
ErrorMode	REG_DWORD	0x00000000 (0)
NoInteractiveServices	REG_DWORD	0x00000000 (0)
SystemDirectory	REG_EXPAND_SZ	%SystemRoot%\system32
ShellErrorMode	REG_DWORD	0x00000001 (1)
ShutdownTime	REG_BIN	C4 FC 00 07 4D 8C C4 01

Figure 13. Shutdown time

Path = “C:\windows\system32\config\system\CurrentControlSet\Control\Windows\ShutdownTime” Now, I don’t know how to convert that shutdown time into human-readable form. So I searched online and found a tool named “DCode” which is a timestamp decoder. After inserting the shutdown time in that tool. I get the time in human-readable form as “2004–08–27 10:46:33 AM”. So, the last recorded computer shutdown date/time is “2004–08–27 10:46:33 AM”.



Name	Timestamp
Apple Absolute Time (UTC)	2001-01-01 00:00:00.0000000 Z
Apple Absolute Time	2000-12-31 18:00:00.0000000 -06:00
Apple Absolute Time (ns) (UTC)	2005-01-14 07:35:51.9310922 Z
Apple Absolute Time (ns)	2005-01-14 01:35:51.9310922 -06:00
Chromium Time Microseconds (UTC)	5637-07-17 13:45:31.0921640 Z
Chromium Time Microseconds	5637-07-17 08:45:31.0921640 -05:00
Microsoft Ticks (Local)	0404-08-27 15:46:33.1092164
OLE Automation (64-bit) (Local)	1899-12-30 00:00:00.0000000
Unix Microseconds (UTC)	6006-07-17 13:45:31.0921640 Z
Unix Microseconds	6006-07-17 08:45:31.0921640 -05:00
Windows Filetime (UTC)	2004-08-27 15:46:33.1092164 Z
Windows Filetime	2004-08-27 10:46:33.1092164 -05:00

Value Input

Format: Hexadecimal (Little-Endian)
Value: C4FC00074D8CC401

Time Zone

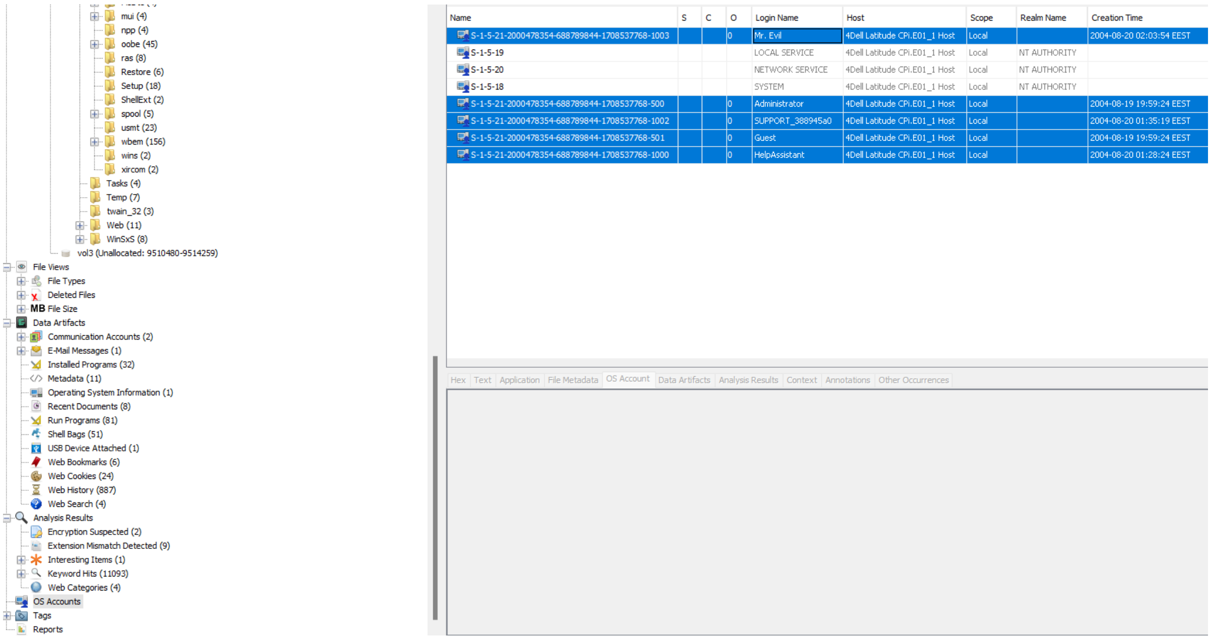
Name: (UTC-06:00) Κεντρική ώρα (Η.Π.Α. & Καναδάς)

Date Output

Pattern: yyyy'-'MM'-'dd HH':'mm':'ss'.'fffffff K
Sample: 2023-09-17 14:20:52.2845122 +03:00

Figure 14. Decoding shutdown time

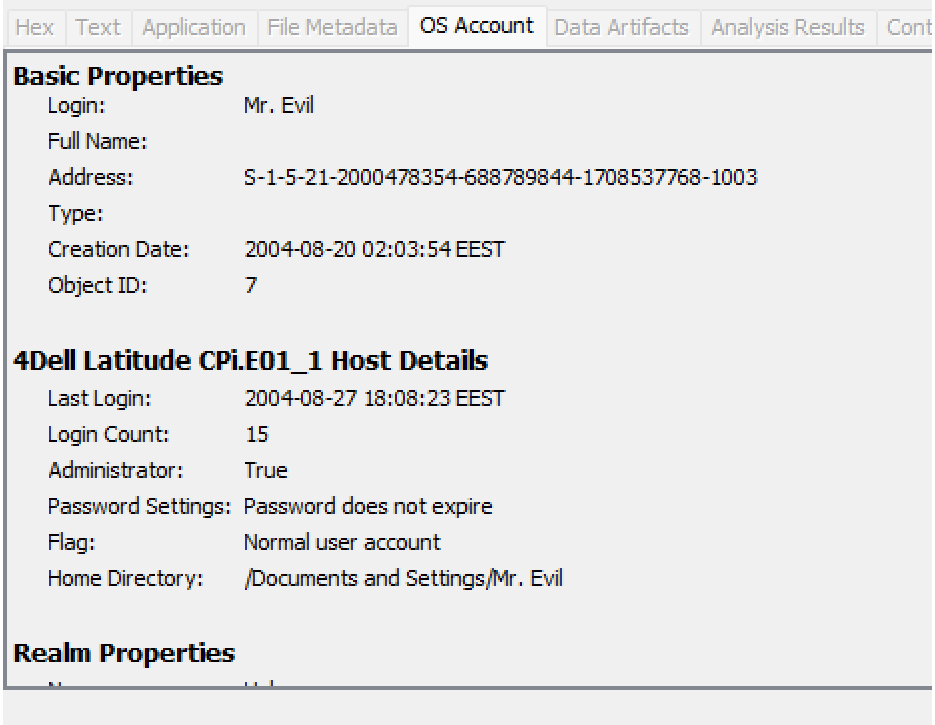
9. How many accounts are recorded (total number)?
10. What is the account name of the user who mostly uses the computer?
In Autopsy we go to “OS Accounts” in the left tree structure. The account name is present in the Login Name column. So the total number of recorded accounts is 5 (Administrator, Guest, HelpAssistant, Mr. Evil, Support_388945a0).



Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-2000478354-688789844-1708537768-1003			0	Mr. Evil	4Dell Latitude CPi.E01_1 Host	Local		2004-08-20 02:03:54 EEST
S-1-5-19				LOCAL SERVICE	4Dell Latitude CPi.E01_1 Host	Local	NT AUTHORITY	
S-1-5-20				NETWORK SERVICE	4Dell Latitude CPi.E01_1 Host	Local	NT AUTHORITY	
S-1-5-18				SYSTEM	4Dell Latitude CPi.E01_1 Host	Local	NT AUTHORITY	
S-1-5-21-2000478354-688789844-1708537768-500			0	Administrator	4Dell Latitude CPi.E01_1 Host	Local		2004-08-19 19:59:24 EEST
S-1-5-21-2000478354-688789844-1708537768-1002			0	SUPPORT_388945a0	4Dell Latitude CPi.E01_1 Host	Local		2004-08-20 01:35:19 EEST
S-1-5-21-2000478354-688789844-1708537768-501			0	Guest	4Dell Latitude CPi.E01_1 Host	Local		2004-08-19 19:59:24 EEST
S-1-5-21-2000478354-688789844-1708537768-1000			0	HelpAssistant	4Dell Latitude CPi.E01_1 Host	Local		2004-08-20 01:28:24 EEST

Figure 15. Accounts

I clicked on each user and i found a field called “Login Count” which stores the number of times the user logged in the system.



Basic Properties

Login:	Mr. Evil
Full Name:	
Address:	S-1-5-21-2000478354-688789844-1708537768-1003
Type:	
Creation Date:	2004-08-20 02:03:54 EEST
Object ID:	7

4Dell Latitude CPi.E01_1 Host Details

Last Login:	2004-08-27 18:08:23 EEST
Login Count:	15
Administrator:	True
Password Settings:	Password does not expire
Flag:	Normal user account
Home Directory:	/Documents and Settings/Mr. Evil

Realm Properties

Figure 16. User login count

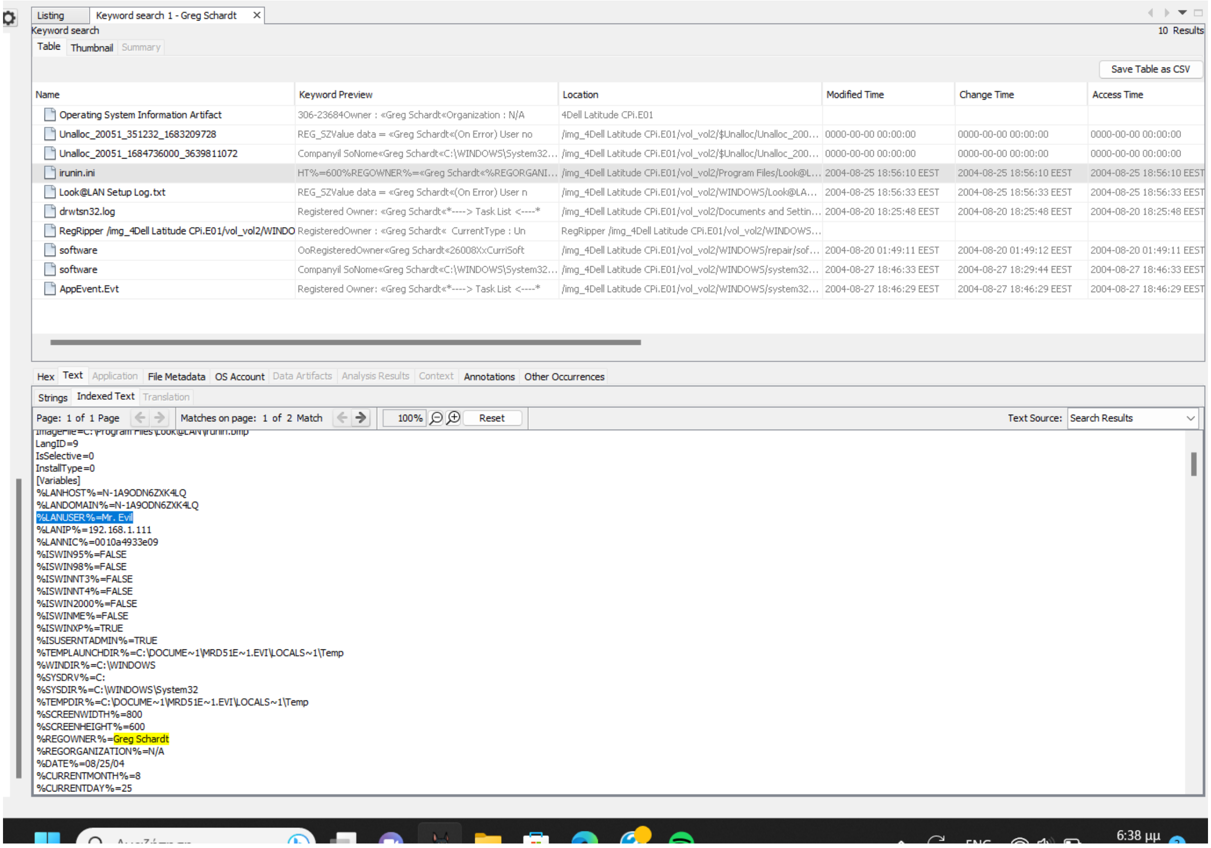
On seeing the above image we found out that only “Mr. Evil” logged into the system 15 times. So, the account name of the user who mostly uses the computer is “Mr. Evil”.

11. Who was the last user to logon to the computer?

On searching on google, I found that the name of the last user who logged in successfully appears in the key “DefaultUserName” of registry and we know from question 6 that the answer is “Mr. Evil”. So the last user who logon into the computer is “Mr. Evil”.

12. A search for the name of “G=r=e=g S=c=h=a=r=d=t” reveals multiple hits. One of these proves that G=r=e=g S=c=h=a=r=d=t is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to?
14. This same file reports the IP address and MAC address of the computer. What are they?

To search for “Greg Schardt” I entered the name in the keyword search & I got 10 results. After searching every file I found one interesting file whose location is “C:\Program Files\Look@LAN\irunin.ini”. On searching for the file I found that Look@LAN is an application that allows users to monitor the clients who are connected to LAN. In the irunin.ini file, it is mentioned that regowner is Greg Schardt while the LAN user is Mr. Evil which proves that both are the same.



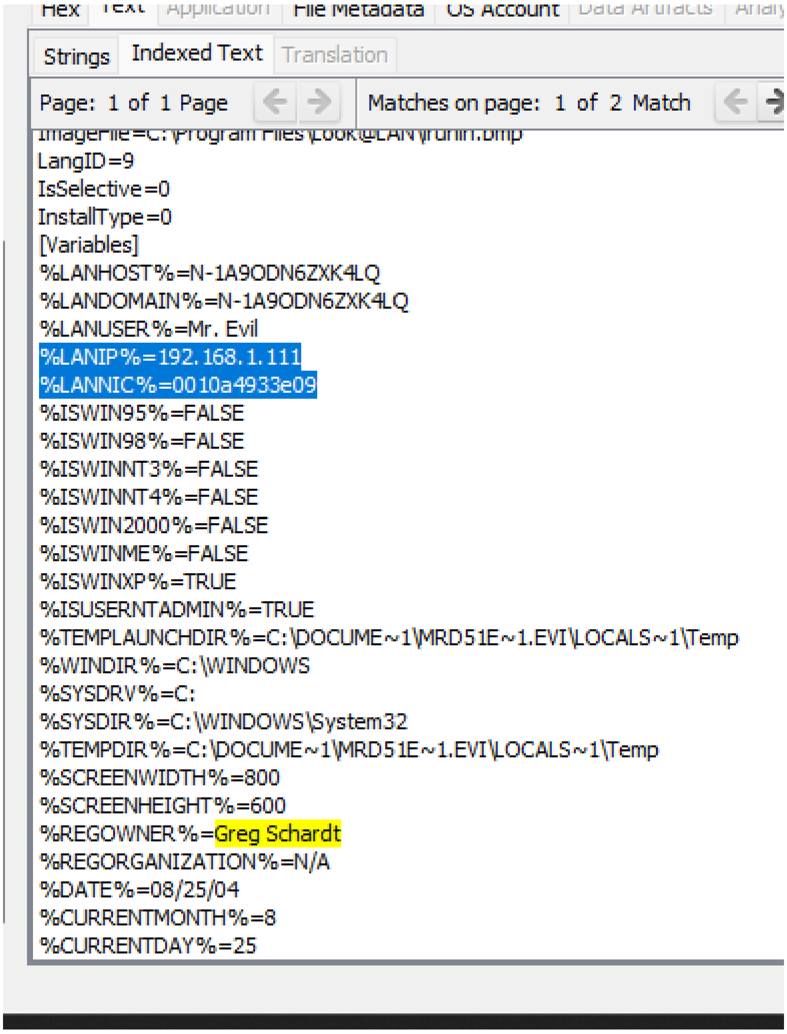
Name	Keyword Preview	Location	Modified Time	Change Time	Access Time
Operating System Information Artifact	306-23684Owner : «Greg Schardt«Organization : N/A	4Dell Latitude CPi.E01			
Unalloc_20051_351232_1683209728	REG_SZValue data = «Greg Schardt«(On Error) User no	/img_4Dell Latitude CPi.E01/vol_vol2/$Unalloc/Unalloc_200…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Unalloc_20051_1684736000_3639811072	Companyil SoNome«Greg Schardt«C:\WINDOWS\System32…	/img_4Dell Latitude CPi.E01/vol_vol2/$Unalloc/Unalloc_200…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
irunin.ini	HT%=600%REGOWNER%=«Greg Schardt«%REGORGANI…	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Look@L…	2004-08-25 18:56:10 EEST	2004-08-25 18:56:10 EEST	2004-08-25 18:56:10 EEST
Look@LAN Setup Log.txt	REG_SZValue data = «Greg Schardt«(On Error) User n	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/Look@LA…	2004-08-25 18:56:33 EEST	2004-08-25 18:56:33 EEST	2004-08-25 18:56:33 EEST
drwtsn32.log	Registered Owner: «Greg Schardt«*----> Task List <----*	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin…	2004-08-20 18:25:48 EEST	2004-08-20 18:25:48 EEST	2004-08-20 18:25:48 EEST
RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/WINDO	RegisteredOwner : «Greg Schardt« CurrentType : Un	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS…			
software	OoRegisteredOwner«Greg Schardt«26008XxCurriSoft	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/repair/sof…	2004-08-20 01:49:11 EEST	2004-08-20 01:49:12 EEST	2004-08-20 01:49:11 EEST
software	Companyil SoNome«Greg Schardt«C:\WINDOWS\System32…	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32…	2004-08-27 18:46:33 EEST	2004-08-27 18:29:44 EEST	2004-08-27 18:46:33 EEST
AppEvent.Evt	Registered Owner: «Greg Schardt«*----> Task List <----*	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32…	2004-08-27 18:46:29 EEST	2004-08-27 18:46:29 EEST	2004-08-27 18:46:29 EEST

```
ImageFile=C:\Program Files\Look@LAN\irunin.bmp
LangID=9
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=N-1A9ODN6ZXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
%ISWIN95%=FALSE
%ISWIN98%=FALSE
%ISWINNT3%=FALSE
%ISWINNT4%=FALSE
%ISWIN2000%=FALSE
%ISWINME%=FALSE
%ISWINXP%=TRUE
%ISUSERNTADMIN%=TRUE
%TEMPLAUNCHDIR%=C:\DOCUME~1\MRD51E~1.EVI\LOCALS~1\Temp
%WINDIR%=C:\WINDOWS
%SYSDRV%=C:
%SYSDIR%=C:\WINDOWS\System32
%TEMPDIR%=C:\DOCUME~1\MRD51E~1.EVI\LOCALS~1\Temp
%SCREENWIDTH%=800
%SCREENHEIGHT%=600
%REGOWNER%=Greg Schardt
%REGORGANIZATION%=N/A
%DATE%=08/25/04
%CURRENTMONTH%=8
%CURRENTDAY%=25
```

Figure 17. Keyword search result

So the name of the file is “irunin.ini” & the name of the software program is “Look@LAN”.

If we look closely at the elements of this file we can also answer question 14, because we know that the Look@LAN application monitors the client which is connected to the LAN.



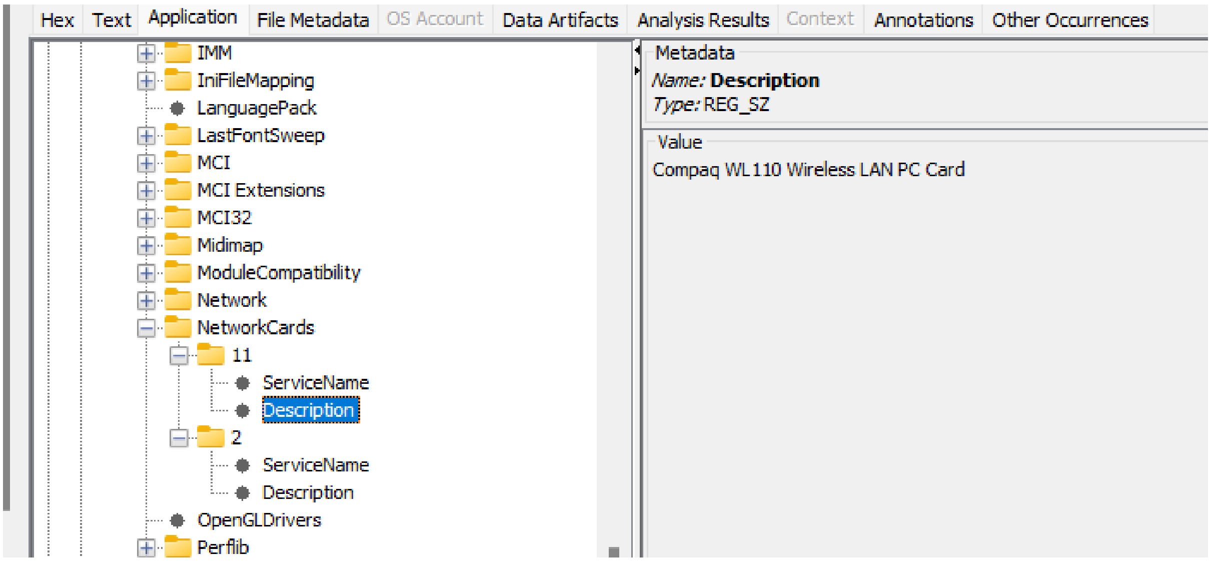
```
ImageFile=C:\Program Files\Look@LAN\irunin.bmp
LangID=9
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=N-1A9ODN6ZXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
%ISWIN95%=FALSE
%ISWIN98%=FALSE
%ISWINNT3%=FALSE
%ISWINNT4%=FALSE
%ISWIN2000%=FALSE
%ISWINME%=FALSE
%ISWINXP%=TRUE
%ISUSERNTADMIN%=TRUE
%TEMPLAUNCHDIR%=C:\DOCUME~1\MRD51E~1.EVI\LOCALS~1\Temp
%WINDIR%=C:\WINDOWS
%SYSDRV%=C:
%SYSDIR%=C:\WINDOWS\System32
%TEMPDIR%=C:\DOCUME~1\MRD51E~1.EVI\LOCALS~1\Temp
%SCREENWIDTH%=800
%SCREENHEIGHT%=600
%REGOWNER%=Greg Schardt
%REGORGANIZATION%=N/A
%DATE%=08/25/04
%CURRENTMONTH%=8
%CURRENTDAY%=25
```

Figure 18. IP and MAC address

On seeing the above image we find out that the IP address & MAC address of the computer are 192.168.1.111 & 0010a4933e09 respectively.

13. *List the network cards used by this computer*

First I searched for the registry which stores info about network cards and I found out the registry location is “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards”. Now in Autopsy, I go to this registry and see the network cards details. The Full Path is = “C:\windows\system32\config\software\Microsoft\WindowsNT\CurrentVersion\NetworkCards”



Metadata

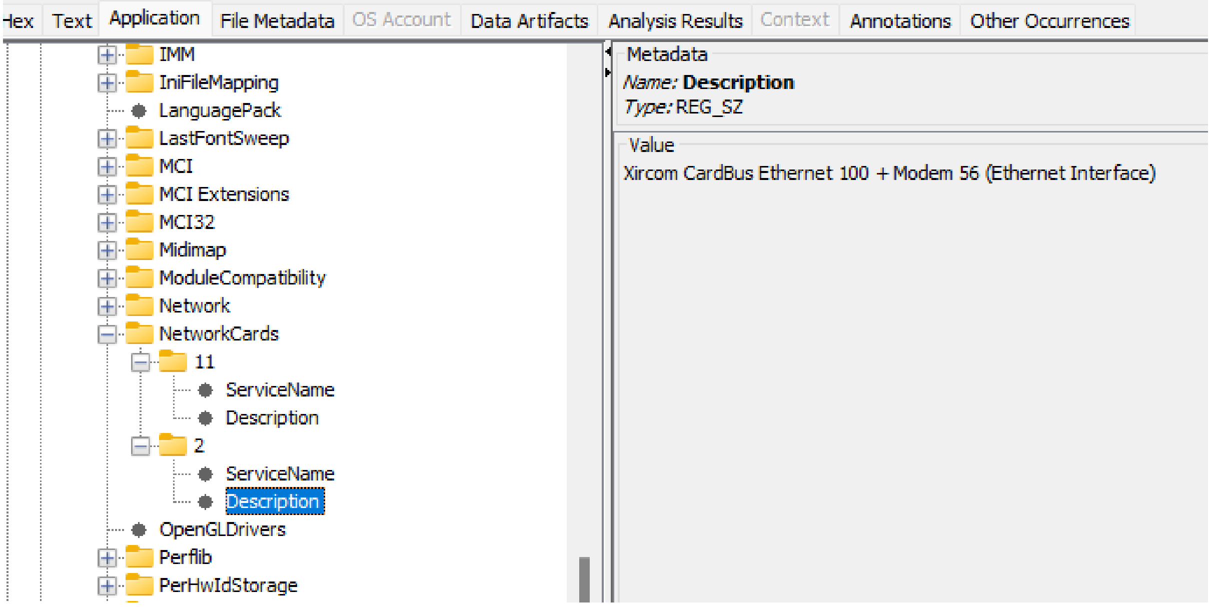
Name: **Description**

Type: REG_SZ

Value

Compaq WL110 Wireless LAN PC Card

Figure 19. First network card



Metadata

Name: **Description**

Type: REG_SZ

Value

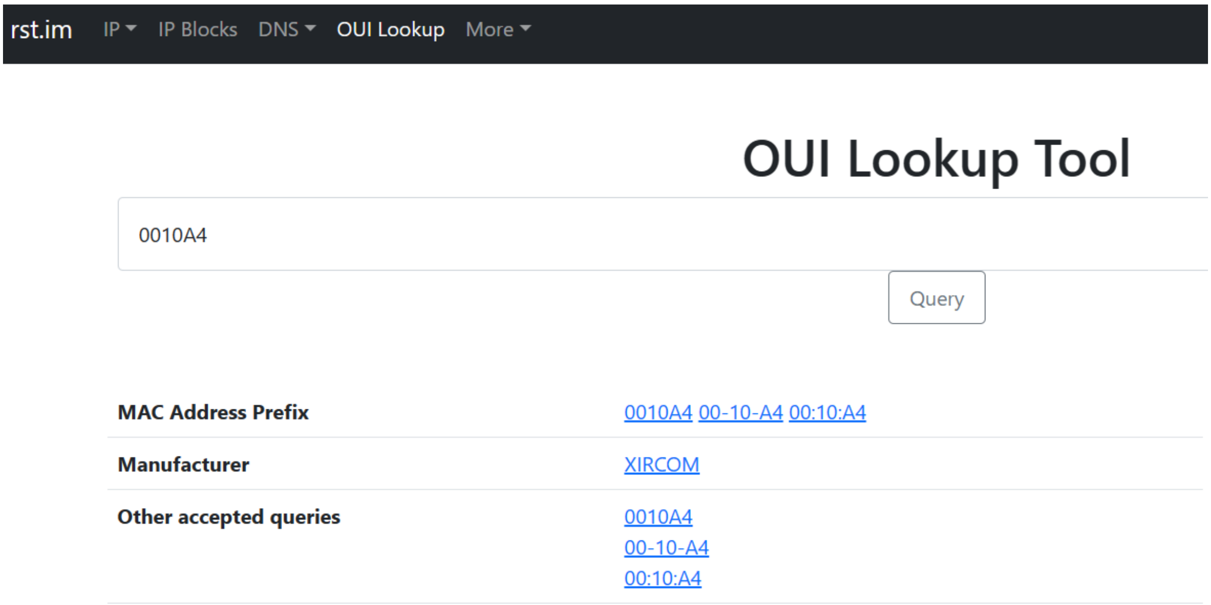
Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)

Figure 20. Second network card

From both the above images we find out that the name of both the network cards is “Compaq WL110 Wireless LAN PC Card” & “Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)”.

15. An internet search for vendor name/model of NIC cards by MAC address can be used to find out which network interface was used. In the above answer, the first 3 hex characters of the MAC address report the vendor of the card. Which NIC card was used during the installation and set-up for LOOK@LAN?

In question 14, we find out that the NIC which is used in the system has MAC address 0010a4933e09, so now we search for the vendor name. In the site https://rst.im/oui/ we find out that the NIC card which was used during the installation & set-up for Look@LAN is “Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)”.



OUI Lookup Tool

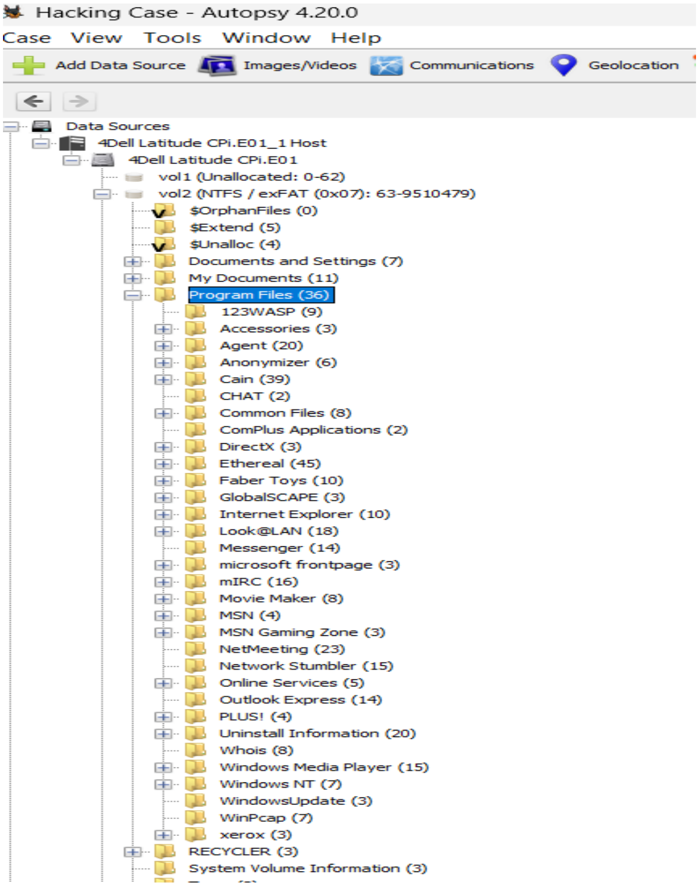
0010A4

MAC Address Prefix	0010A4 00-10-A4 00:10:A4
Manufacturer	XIRCOM
Other accepted queries	0010A4 00-10-A4 00:10:A4

Figure 21. OUI lookup or vendor lookup

16. Find 6 installed programs that may be used for hacking.

On seeing into “C:\Program Files” we can easily find out all the installed programs. Then I search each program to find out the programs which may be used for hacking.

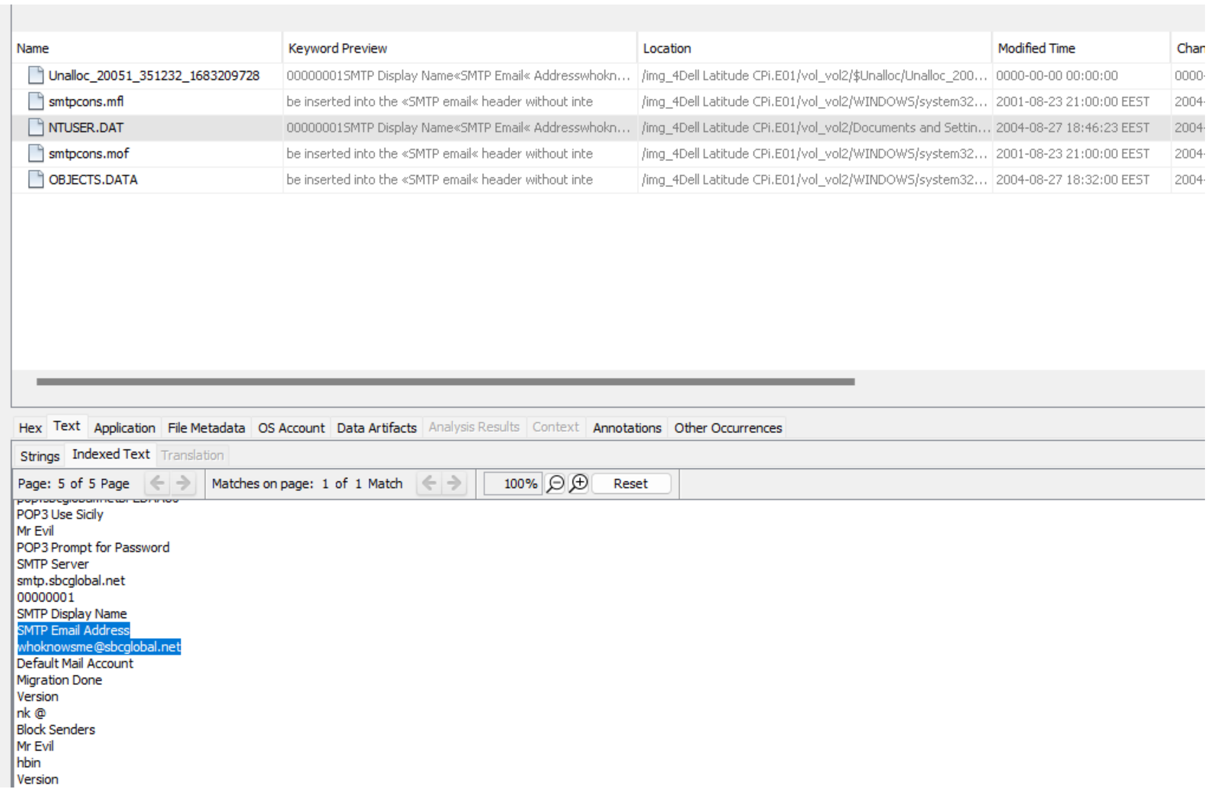


```
Data Sources
  4Dell Latitude CPi.E01_1 Host
    4Dell Latitude CPi.E01
      vol1 (Unallocated: 0-62)
      vol2 (NTFS / exFAT (0x07): 63-9510479)
        $OrphanFiles (0)
        $Extend (5)
        $Unalloc (4)
        Documents and Settings (7)
        My Documents (11)
        Program Files (36)
          123WASP (9)
          Accessories (3)
          Agent (20)
          Anonymizer (6)
          Cain (39)
          CHAT (2)
          Common Files (8)
          ComPlus Applications (2)
          DirectX (3)
          Ethereal (45)
          Faber Toys (10)
          GlobalSCAPE (3)
          Internet Explorer (10)
          Look@LAN (18)
          Messenger (14)
          microsoft frontpage (3)
          mIRC (16)
          Movie Maker (8)
          MSN (4)
          MSN Gaming Zone (3)
          NetMeeting (23)
          Network Stumbler (15)
          Online Services (5)
          Outlook Express (14)
          PLUS! (4)
          Uninstall Information (20)
          Whois (8)
          Windows Media Player (15)
          Windows NT (7)
          WindowsUpdate (3)
          WinPcap (7)
          xerox (3)
        RECYCLER (3)
        System Volume Information (3)
```

Figure 22. Installed Program list

After searching I found out the following 6 programs which may be used for hacking:-
a) 123WASP:- Software used to get all stored passwords.
b) Anonymizer:- Tool used to create a proxy.
c) Cain:- Password cracking tool
d) Ethereal (Today's Wireshark):- network protocol analyzer
e) Look@LAN:- Network monitoring tool
f) NetStumbler:- wireless networking tool to hack wifi password

17. What is the SMTP email address for Mr. Evil?
18. What are the NNTP (news server) settings for Mr. Evil?
To find this I take the help of keyword search. I simply searched for "SMTP email" & got some results. After searching through all the files, I found a file named "NTUSER.DAT" in which I found an SMTP email address for Mr. Evil.
Path = "C:\Documents and Settings\Mr.Evil\NTUSER.DAT"



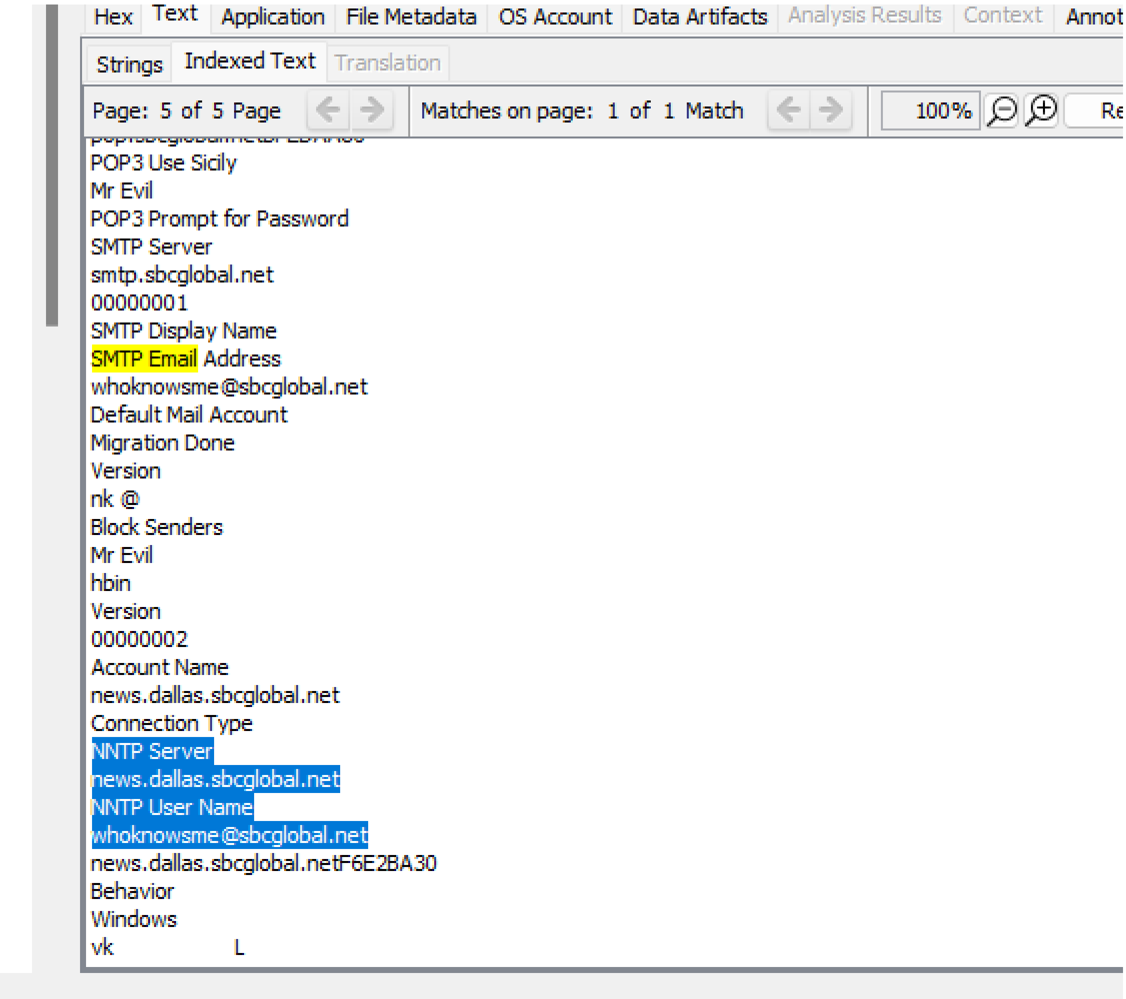
Name	Keyword Preview	Location	Modified Time	Char
Unalloc_20051_351232_1683209728	00000001SMTP Display Name«SMTP Email« Addresswhokn...	/img_4Dell Latitude CPi.E01/vol_vol2/$Unalloc/Unalloc_200...	0000-00-00 00:00:00	0000
smtpcons.mfl	be inserted into the «SMTP email« header without inte	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32...	2001-08-23 21:00:00 EEST	2004
NTUSER.DAT	00000001SMTP Display Name«SMTP Email« Addresswhokn...	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-27 18:46:23 EEST	2004
smtpcons.mof	be inserted into the «SMTP email« header without inte	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32...	2001-08-23 21:00:00 EEST	2004
OBJECTS.DATA	be inserted into the «SMTP email« header without inte	/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32...	2004-08-27 18:32:00 EEST	2004

```
POP3 Use Sicily
Mr Evil
POP3 Prompt for Password
SMTP Server
smtp.sbcglobal.net
00000001
SMTP Display Name
SMTP Email Address
whoknowsme@sbcglobal.net
Default Mail Account
Migration Done
Version
nk @
Block Senders
Mr Evil
hbin
Version
```

Figure 23. SMTP info

So, we find out that the SMTP email address of Mr. Evil is "whoknowsme@sbcglobal.net".

In the same file I observed that it had information about question 18 too.



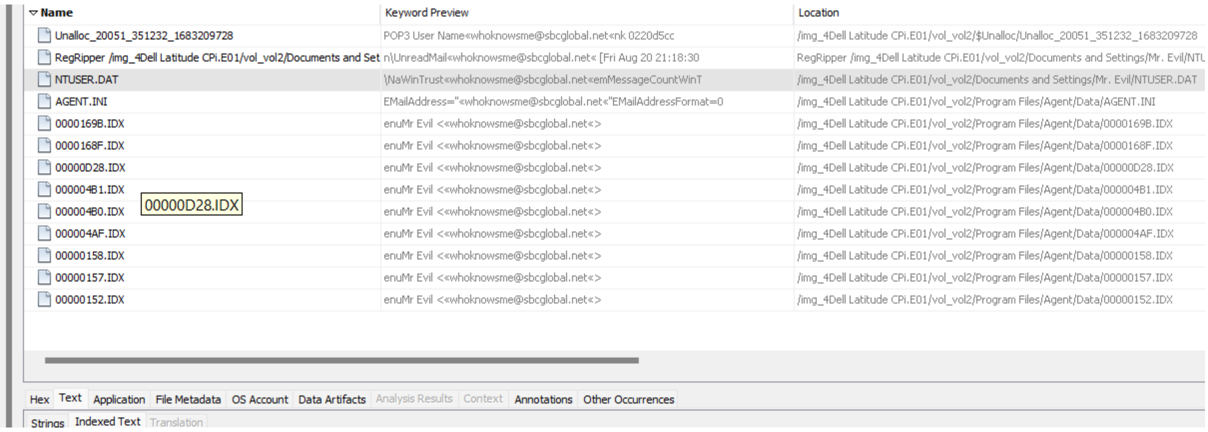
```
POP3 Use Sicily
Mr Evil
POP3 Prompt for Password
SMTP Server
smtp.sbcglobal.net
00000001
SMTP Display Name
SMTP Email Address
whoknowsme@sbcglobal.net
Default Mail Account
Migration Done
Version
nk @
Block Senders
Mr Evil
hbin
Version
00000002
Account Name
news.dallas.sbcglobal.net
Connection Type
NNTP Server
news.dallas.sbcglobal.net
NNTP User Name
whoknowsme@sbcglobal.net
news.dallas.sbcglobal.netF6E2BA30
Behavior
Windows
vk              L
```

Figure 24. NNTP info

On seeing highlighted text in the above image we found out that NNTP
a) server name is “news.dallas.sbcglobal.net”,
b) username is “whoknowsme@sbcglobal.net”.

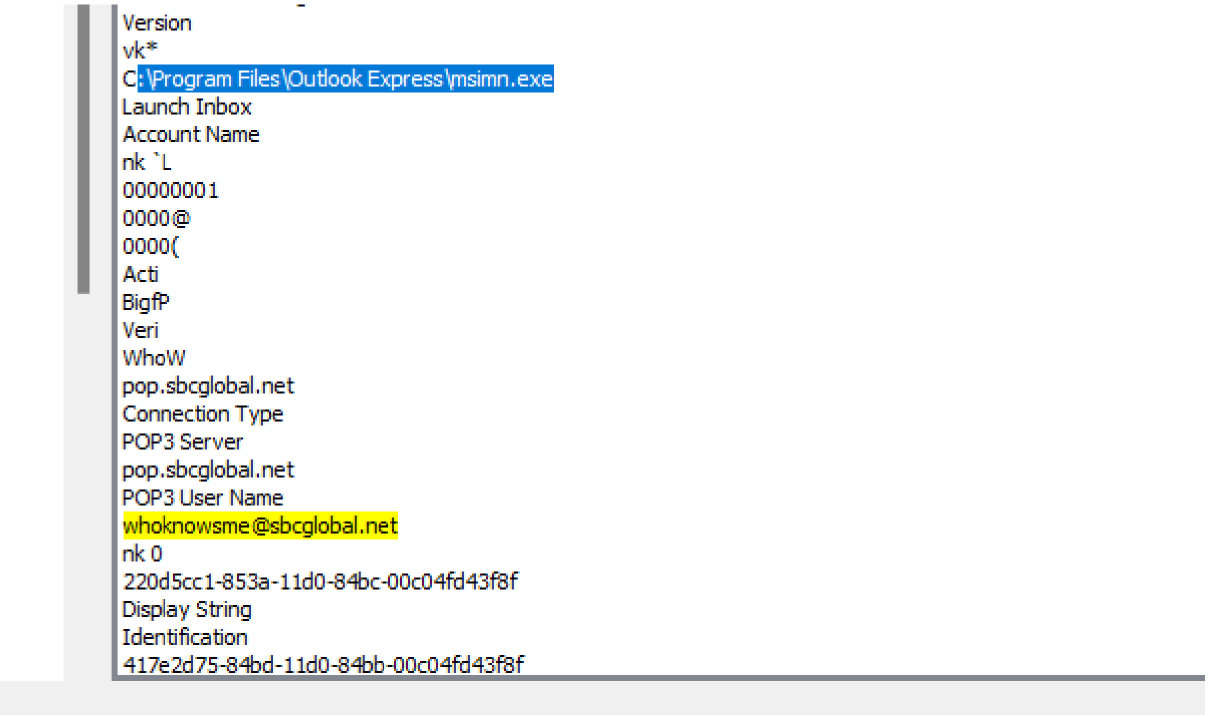
19. What two installed programs show this information?

For this question I searched for “whoknowsme@sbcglobal.net”. From the results I searched the files and I have found two files that show this information. The first one is NTUSER.DAT that we can connect it with Outlook if we search on it’s text field and the second one is AGENT.INI that we can connect it with Forte Agent if we follow the same tactic.



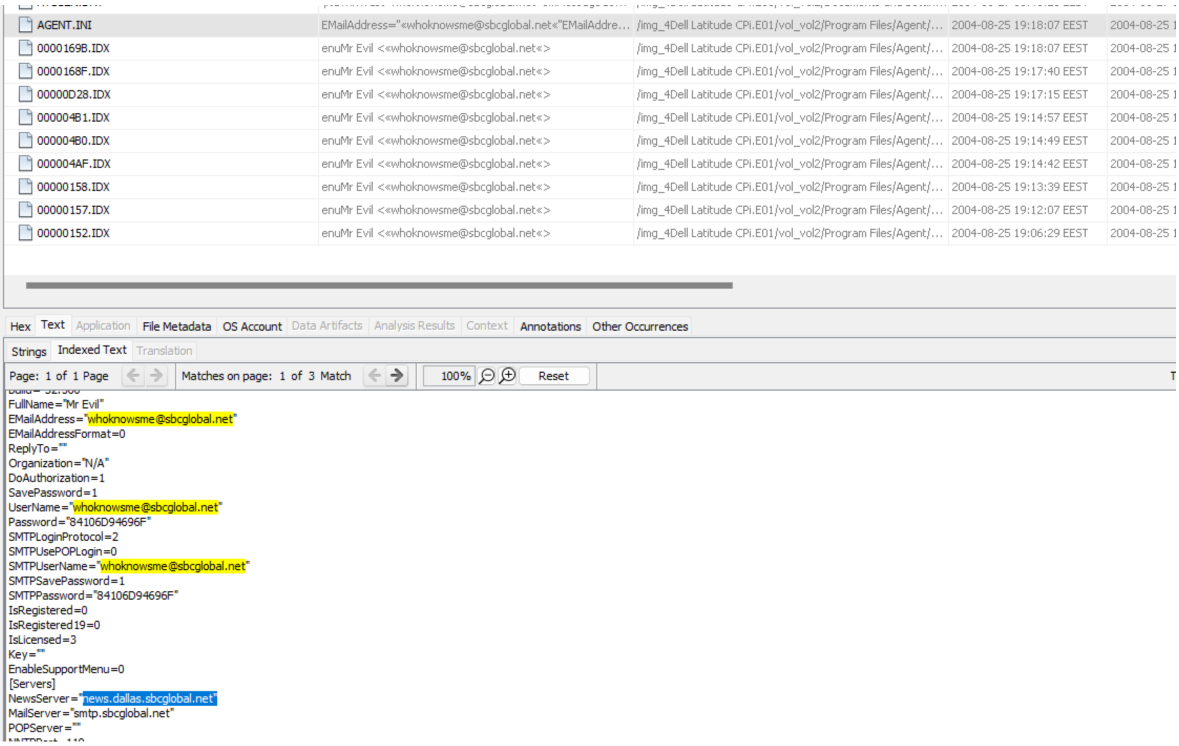
Name	Keyword Preview	Location
Unalloc_20051_351232_1683209728	POP3 User Name«whoknowsme@sbcglobal.net«nk 0220d5cc	/img_4Dell Latitude CPi.E01/vol_vol2/$Unalloc/Unalloc_20051_351232_1683209728
RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Set	n\UnreadMail«whoknowsme@sbcglobal.net« [Fri Aug 20 21:18:30	RegRipper /img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/NTU
NTUSER.DAT	\NaWinTrust«whoknowsme@sbcglobal.net«emMessageCountWinT	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/NTUSER.DAT
AGENT.INI	EMailAddress="«whoknowsme@sbcglobal.net«"EMailAddressFormat=0	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/AGENT.INI
0000169B.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/0000169B.IDX
0000168F.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/0000168F.IDX
00000D28.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/00000D28.IDX
000004B1.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/000004B1.IDX
000004B0.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/000004B0.IDX
000004AF.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/000004AF.IDX
00000158.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/00000158.IDX
00000157.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/00000157.IDX
00000152.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/00000152.IDX

Figure 25. Keyword search



```
Version
vk*
C:\Program Files\Outlook Express\msimn.exe
Launch Inbox
Account Name
nk `L
00000001
0000@
0000(
Acti
BigfP
Veri
WhoW
pop.sbcglobal.net
Connection Type
POP3 Server
pop.sbcglobal.net
POP3 User Name
whoknowsme@sbcglobal.net
nk 0
220d5cc1-853a-11d0-84bc-00c04fd43f8f
Display String
Identification
417e2d75-84bd-11d0-84bb-00c04fd43f8f
```

Figure 26. NTUSER.DAT text



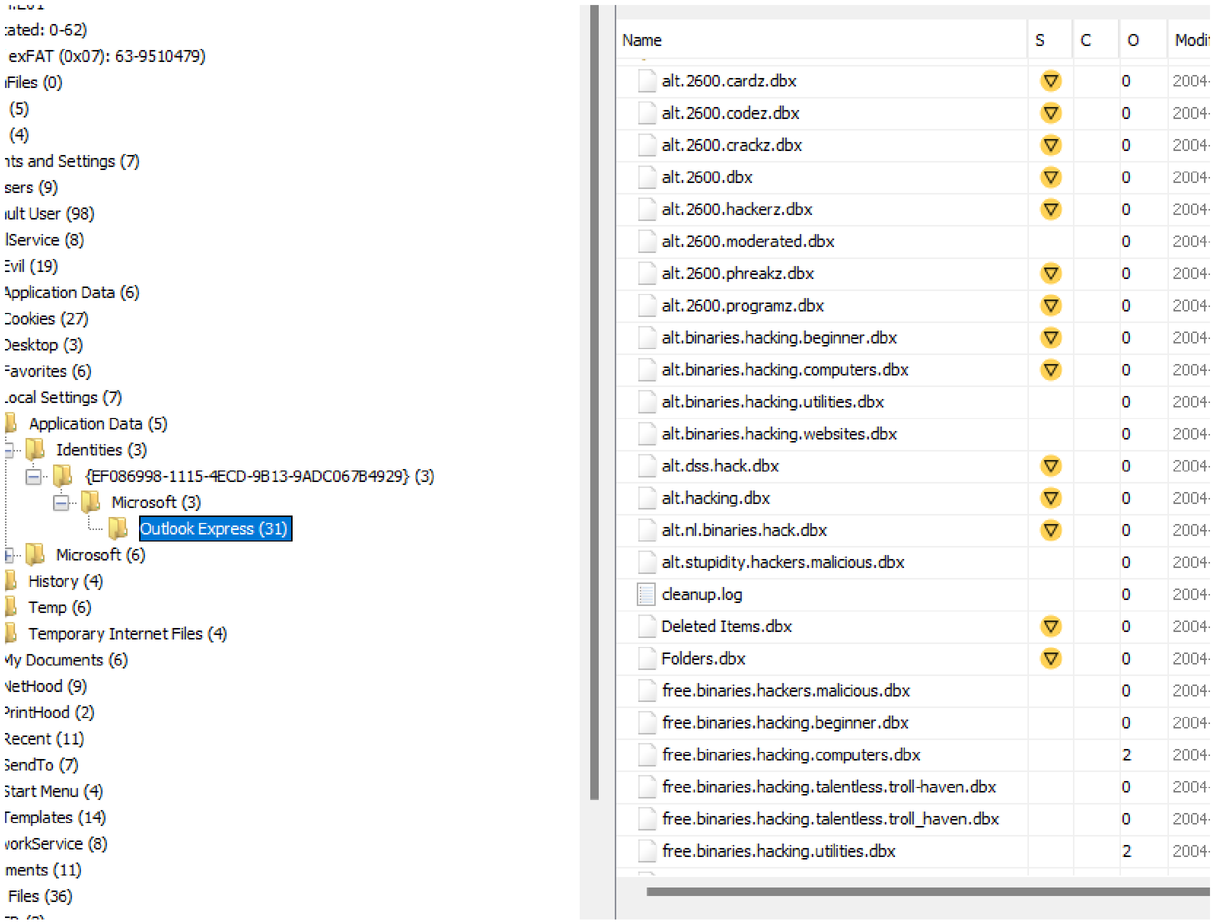
AGENT.INI	EMailAddress="«whoknowsme@sbcglobal.net«"EMailAddre…	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/…	2004-08-25 19:18:07 EEST	2004-08-25 1
0000169B.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/…	2004-08-25 19:18:07 EEST	2004-08-25 1
0000168F.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/…	2004-08-25 19:17:40 EEST	2004-08-25 1
00000D28.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/…	2004-08-25 19:17:15 EEST	2004-08-25 1
000004B1.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/…	2004-08-25 19:14:57 EEST	2004-08-25 1
000004B0.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/…	2004-08-25 19:14:49 EEST	2004-08-25 1
000004AF.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/…	2004-08-25 19:14:42 EEST	2004-08-25 1
00000158.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/…	2004-08-25 19:13:39 EEST	2004-08-25 1
00000157.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/…	2004-08-25 19:12:07 EEST	2004-08-25 1
00000152.IDX	enuMr Evil <«whoknowsme@sbcglobal.net«>	/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/…	2004-08-25 19:06:29 EEST	2004-08-25 1

```
FullName="Mr Evil"
EMailAddress="whoknowsme@sbcglobal.net"
EMailAddressFormat=0
ReplyTo=""
Organization="N/A"
DoAuthorization=1
SavePassword=1
UserName="whoknowsme@sbcglobal.net"
Password="84106D94696F"
SMTPLoginProtocol=2
SMTPUsePOPLogin=0
SMTPUserName="whoknowsme@sbcglobal.net"
SMTPSavePassword=1
SMTPPassword="84106D94696F"
IsRegistered=0
IsRegistered19=0
IsLicensed=3
Key=""
EnableSupportMenu=0
[Servers]
NewsServer="news.dallas.sbcglobal.net"
MailServer="smtp.sbcglobal.net"
POPServer=""
```

Figure 27. AGENT.INI text

20. List 5 newsgroups that Mr. Evil has subscribed to?

For this question I searched on where all the Outlook Express email folders and messages are stored. I found that the location of this directory is :
Documents and
Settings\user_name\LocalSettings\ApplicationData\Identities\Microsoft\Outlook Express
So we go to the Path: “C:\Document and Settings\Mr. Evil\Local Settings\Application Data\Identities\{EF086998–1115–4ECD-9B13 9ADC067B4929} \Microsoft\Outlook Express” and we found many newsgroup to which Mr. Evil has subscribed. Some of them are: “Alt.binaries.hacking.utilities, Alt.stupidity.hackers.malicious, Free.binaries.hackers.malicious, Free.binaries.hacking.talentless.troll_haven, alt.dss.hack ”.



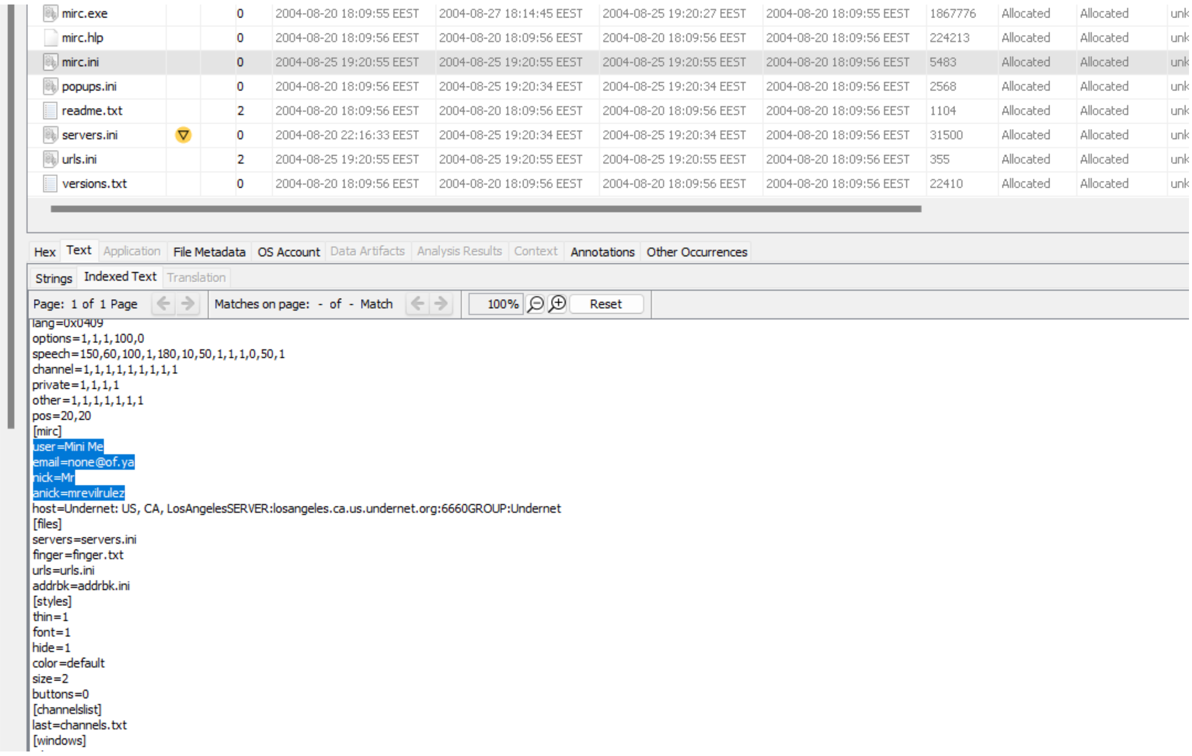
```
:ated: 0-62)
 exFAT (0x07): 63-9510479)
ıFiles (0)
 (5)
 (4)
ıts and Settings (7)
sers (9)
ıult User (98)
lService (8)
Evil (19)
Application Data (6)
Cookies (27)
Desktop (3)
Favorites (6)
Local Settings (7)
  Application Data (5)
    Identities (3)
      {EF086998-1115-4ECD-9B13-9ADC067B4929} (3)
        Microsoft (3)
          Outlook Express (31)
    Microsoft (6)
  History (4)
  Temp (6)
  Temporary Internet Files (4)
My Documents (6)
NetHood (9)
PrintHood (2)
Recent (11)
SendTo (7)
Start Menu (4)
Templates (14)
vorkService (8)
ments (11)
 Files (36)
```

Name	S	C	O	Modi
alt.2600.cardz.dbx	▽		0	2004-
alt.2600.codez.dbx	▽		0	2004-
alt.2600.crackz.dbx	▽		0	2004-
alt.2600.dbx	▽		0	2004-
alt.2600.hackerz.dbx	▽		0	2004-
alt.2600.moderated.dbx			0	2004-
alt.2600.phreakz.dbx	▽		0	2004-
alt.2600.programz.dbx	▽		0	2004-
alt.binaries.hacking.beginner.dbx	▽		0	2004-
alt.binaries.hacking.computers.dbx	▽		0	2004-
alt.binaries.hacking.utilities.dbx			0	2004-
alt.binaries.hacking.websites.dbx			0	2004-
alt.dss.hack.dbx	▽		0	2004-
alt.hacking.dbx	▽		0	2004-
alt.nl.binaries.hack.dbx	▽		0	2004-
alt.stupidity.hackers.malicious.dbx			0	2004-
cleanup.log			0	2004-
Deleted Items.dbx	▽		0	2004-
Folders.dbx	▽		0	2004-
free.binaries.hackers.malicious.dbx			0	2004-
free.binaries.hacking.beginner.dbx			0	2004-
free.binaries.hacking.computers.dbx			2	2004-
free.binaries.hacking.talentless.troll-haven.dbx			0	2004-
free.binaries.hacking.talentless.troll_haven.dbx			0	2004-
free.binaries.hacking.utilities.dbx			2	2004-

Figure 28. Outlook subscribed newsgroup

21. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that were shown when the user was online and in a chat channel?

To view the user settings of MIRC we have to see the file “mirc.ini” whose path is “C:\Program Files\mIRC\mirc.ini”.



mirc.exe		0	2004-08-20 18:09:55 EEST	2004-08-27 18:14:45 EEST	2004-08-25 19:20:27 EEST	2004-08-20 18:09:55 EEST	1867776	Allocated	Allocated	unk
mirc.hlp		0	2004-08-20 18:09:56 EEST	2004-08-20 18:09:56 EEST	2004-08-20 18:09:56 EEST	2004-08-20 18:09:56 EEST	224213	Allocated	Allocated	unk
mirc.ini		0	2004-08-25 19:20:55 EEST	2004-08-25 19:20:55 EEST	2004-08-25 19:20:55 EEST	2004-08-20 18:09:56 EEST	5483	Allocated	Allocated	unk
popups.ini		0	2004-08-20 18:09:56 EEST	2004-08-25 19:20:34 EEST	2004-08-25 19:20:34 EEST	2004-08-20 18:09:56 EEST	2568	Allocated	Allocated	unk
readme.txt		2	2004-08-20 18:09:56 EEST	2004-08-20 18:09:56 EEST	2004-08-20 18:09:56 EEST	2004-08-20 18:09:56 EEST	1104	Allocated	Allocated	unk
servers.ini	▽	0	2004-08-20 22:16:33 EEST	2004-08-25 19:20:34 EEST	2004-08-25 19:20:34 EEST	2004-08-20 18:09:56 EEST	31500	Allocated	Allocated	unk
urls.ini		2	2004-08-25 19:20:55 EEST	2004-08-25 19:20:55 EEST	2004-08-25 19:20:55 EEST	2004-08-20 18:09:56 EEST	355	Allocated	Allocated	unk
versions.txt		0	2004-08-20 18:09:56 EEST	2004-08-20 18:09:56 EEST	2004-08-20 18:09:56 EEST	2004-08-20 18:09:56 EEST	22410	Allocated	Allocated	unk

```
lang=0x0409
options=1,1,1,100,0
speech=150,60,100,1,180,10,50,1,1,1,0,50,1
channel=1,1,1,1,1,1,1,1,1
private=1,1,1,1
other=1,1,1,1,1,1,1
pos=20,20
[mirc]
user=Mini Me
email=none@of.ya
nick=Mr
anick=mrevilrulez
host=Undernet: US, CA, LosAngelesSERVER:losangeles.ca.us.undernet.org:6660GROUP:Undernet
[files]
servers=servers.ini
finger=finger.txt
urls=urls.ini
addrbk=addrbk.ini
[styles]
thin=1
font=1
hide=1
color=default
size=2
buttons=0
[channelslist]
last=channels.txt
[windows]
```

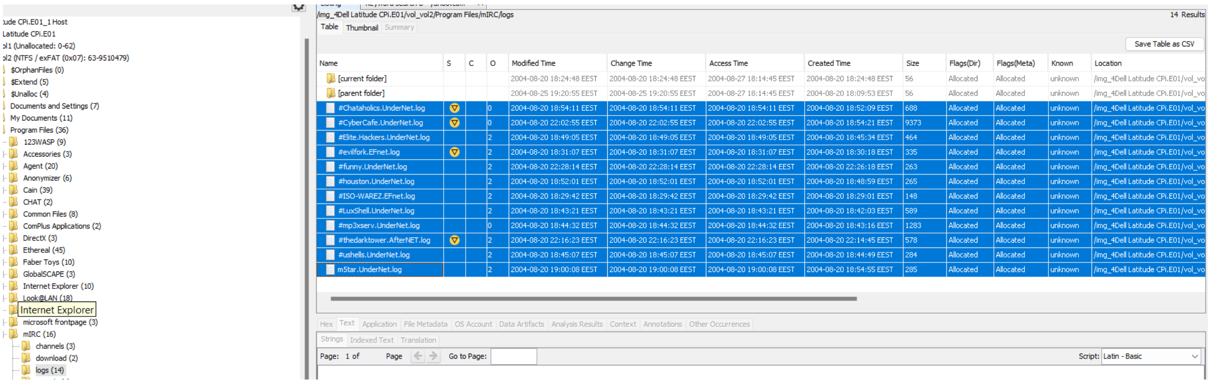
Figure 29. IRC user settings

User settings which were shown when the user was online are highlighted as follows: “user=Mini Me, email=none@of.ya, nick=Mr, & anick=mrevilrulez”.

22. This IRC program has the capability to log chat sessions. List 3 IRC channels that the user of this computer accessed.

To view the logs we have to go inside the logs directory of mIRC.

Path: “C:\Program Files\mIRC\logs”



```
ude CPi.E01_1 Host
Latitude CPi.E01
ol1 (Unallocated: 0-62)
ol2 (NTFS / exFAT (0x07): 63-9510479)
  $OrphanFiles (0)
  $Extend (5)
  $Unalloc (4)
  Documents and Settings (7)
  My Documents (11)
  Program Files (36)
    123WASP (9)
    Accessories (3)
    Agent (20)
    Anonymizer (6)
    Cain (39)
    CHAT (2)
    Common Files (8)
    ComPlus Applications (2)
    DirectX (3)
    Ethereal (45)
    Faber Toys (10)
    GlobalSCAPE (3)
    Internet Explorer (10)
    Look@LAN (18)
    Internet Explorer
    microsoft frontpage (3)
    mIRC (16)
      channels (3)
      download (2)
      logs (14)
```

/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/mIRC/logs

14 Results

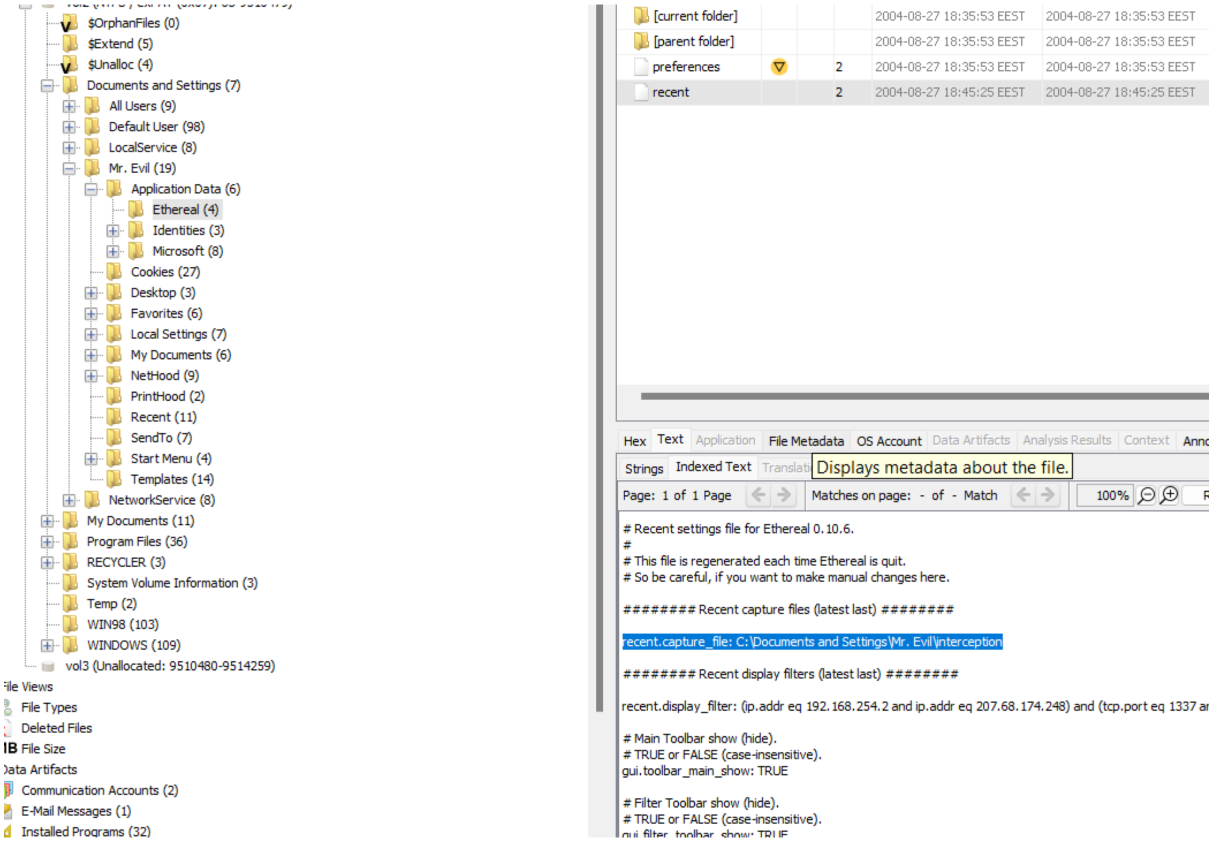
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2004-08-20 18:24:48 EEST	2004-08-20 18:24:48 EEST	2004-08-27 18:14:45 EEST	2004-08-20 18:24:48 EEST	56	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
[parent folder]				2004-08-25 19:20:55 EEST	2004-08-25 19:20:55 EEST	2004-08-27 18:14:45 EEST	2004-08-20 18:09:53 EEST	56	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
#Chataholics.UnderNet.log	▽		0	2004-08-20 18:54:11 EEST	2004-08-20 18:54:11 EEST	2004-08-20 18:54:11 EEST	2004-08-20 18:52:09 EEST	688	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
#CyberCafe.UnderNet.log	▽		0	2004-08-20 22:02:55 EEST	2004-08-20 22:02:55 EEST	2004-08-20 22:02:55 EEST	2004-08-20 18:54:21 EEST	9373	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
#Elite.Hackers.UnderNet.log			2	2004-08-20 18:49:05 EEST	2004-08-20 18:49:05 EEST	2004-08-20 18:49:05 EEST	2004-08-20 18:45:34 EEST	464	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
#evilfork.EFnet.log	▽		2	2004-08-20 18:31:07 EEST	2004-08-20 18:31:07 EEST	2004-08-20 18:31:07 EEST	2004-08-20 18:30:18 EEST	335	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
#funny.UnderNet.log			2	2004-08-20 22:28:14 EEST	2004-08-20 22:28:14 EEST	2004-08-20 22:28:14 EEST	2004-08-20 22:26:18 EEST	263	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
#houston.UnderNet.log			2	2004-08-20 18:52:01 EEST	2004-08-20 18:52:01 EEST	2004-08-20 18:52:01 EEST	2004-08-20 18:48:59 EEST	265	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
#ISO-WAREZ.EFnet.log			2	2004-08-20 18:29:42 EEST	2004-08-20 18:29:42 EEST	2004-08-20 18:29:42 EEST	2004-08-20 18:29:01 EEST	148	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
#LuxShell.UnderNet.log			2	2004-08-20 18:43:21 EEST	2004-08-20 18:43:21 EEST	2004-08-20 18:43:21 EEST	2004-08-20 18:42:03 EEST	589	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
#mp3xserv.UnderNet.log			0	2004-08-20 18:44:32 EEST	2004-08-20 18:44:32 EEST	2004-08-20 18:44:32 EEST	2004-08-20 18:43:16 EEST	1283	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
#thedarktower.AfterNET.log	▽		2	2004-08-20 22:16:23 EEST	2004-08-20 22:16:23 EEST	2004-08-20 22:16:23 EEST	2004-08-20 22:14:45 EEST	578	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
#ushells.UnderNet.log			2	2004-08-20 18:45:07 EEST	2004-08-20 18:45:07 EEST	2004-08-20 18:45:07 EEST	2004-08-20 18:44:49 EEST	284	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo
m5tar.UnderNet.log			2	2004-08-20 19:00:08 EEST	2004-08-20 19:00:08 EEST	2004-08-20 19:00:08 EEST	2004-08-20 18:54:55 EEST	285	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vo

Figure 30. IRC channel list

In the above image, the list of IRC channels are selected. Some IRC channels are as follows: Ushells.undernet.log, Elite.hackers.undernet.log, and Mp3xserv.undernet.log.

23. Ethereal, a popular "sniffing" program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data?

On searching, we find that the "recent" file of the ethereal directory holds this info whose path is:"C:\Documents and Settings\Mr. Evil\Application Data\Ethereal\recent". On viewing the recent file we find that the location of the file which stores captured or intercepted data is "C:\Documents and Settings\Mr. Evil\interception". Hence, the name of the file which stores intercepted data is "interception".



[current folder]			2004-08-27 18:35:53 EEST	2004-08-27 18:35:53 EEST
[parent folder]			2004-08-27 18:35:53 EEST	2004-08-27 18:35:53 EEST
preferences	▽	2	2004-08-27 18:35:53 EEST	2004-08-27 18:35:53 EEST
recent		2	2004-08-27 18:45:25 EEST	2004-08-27 18:45:25 EEST

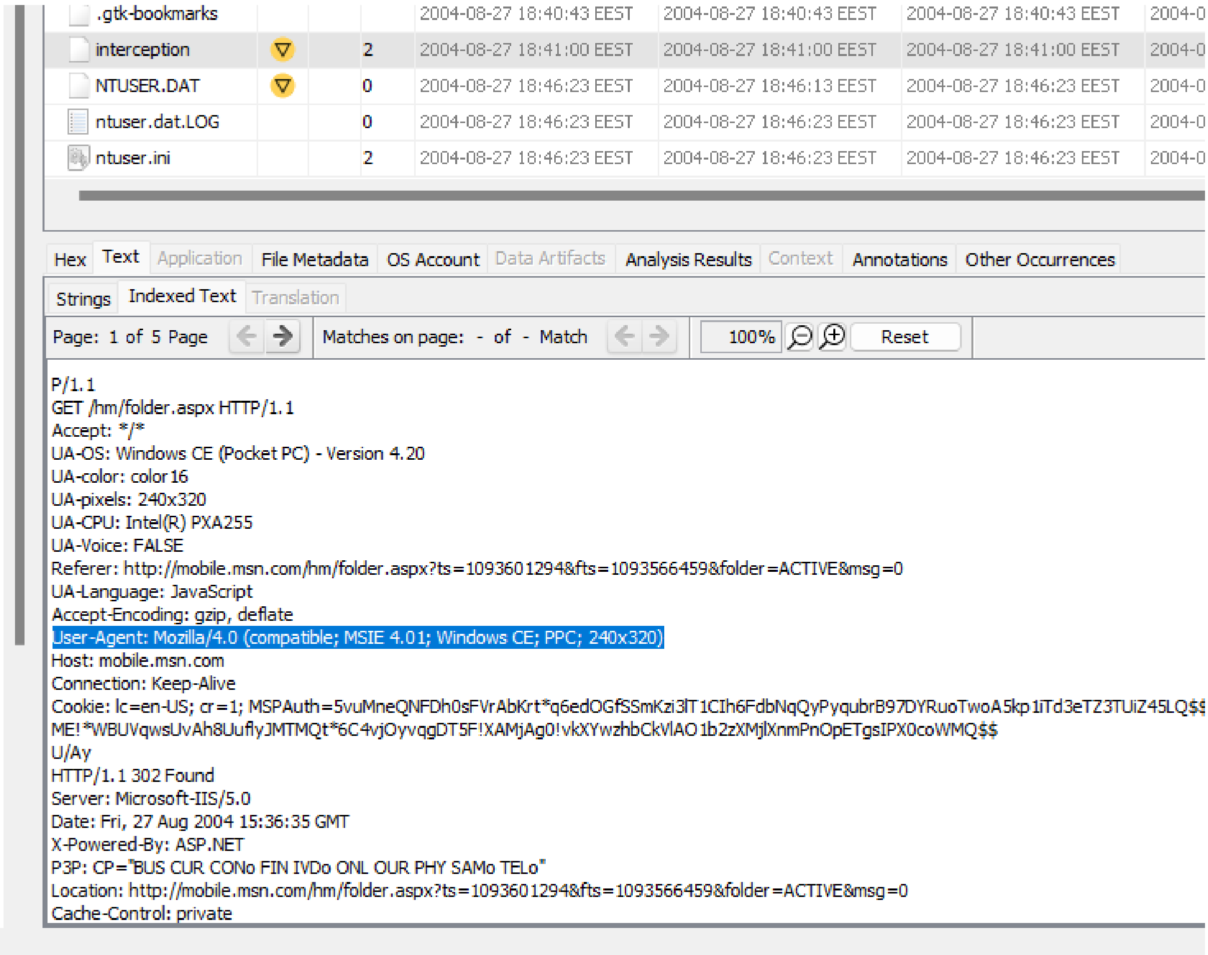
```
# Recent settings file for Ethereal 0.10.6.
#
# This file is regenerated each time Ethereal is quit.
# So be careful, if you want to make manual changes here.

######## Recent capture files (latest last) ########

recent.capture_file: C:\Documents and Settings\Mr. Evil\interception

######## Recent display filters (latest last) ########

recent.display_filter: (ip.addr eq 192.168.254.2 and ip.addr eq 207.68.174.248) and (tcp.port eq 1337 ar

# Main Toolbar show (hide).
# TRUE or FALSE (case-insensitive).
gui.toolbar_main_show: TRUE

# Filter Toolbar show (hide).
# TRUE or FALSE (case-insensitive).
gui.filter_toolbar_show: TRUE
```

Figure 31. Recent file of ethereal

24. Viewing the file in a text format reveals much information about who and what was intercepted. What type of wireless computer was the victim (person who had his internet surfing recorded) using?

25. What websites was the victim accessing?

In the above question, we find the location of the file as "C:\Documents and Settings\Mr. Evil\interception". On viewing the file we find out that the user agent is MSIE 4.01 with Windows CE. Hence, the type of wireless computer which was used by the victim is "Microsoft Internet Explorer (MSIE) 4.01 with Windows CE (Pocket PC)".

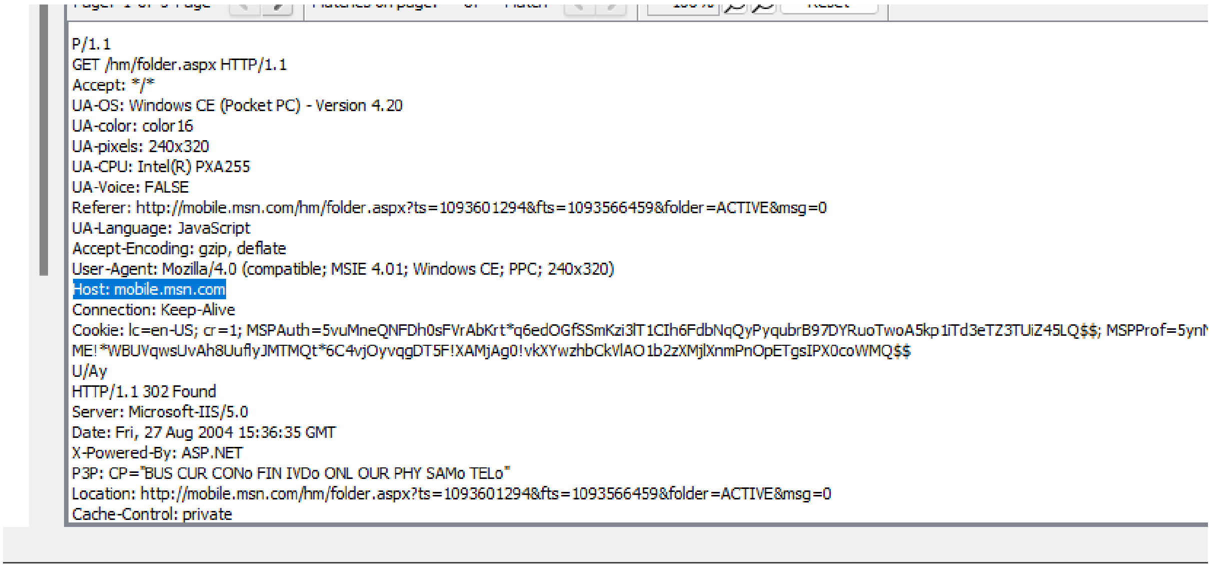


.gtk-bookmarks			2004-08-27 18:40:43 EEST	2004-08-27 18:40:43 EEST	2004-08-27 18:40:43 EEST	2004-0
interception	▽	2	2004-08-27 18:41:00 EEST	2004-08-27 18:41:00 EEST	2004-08-27 18:41:00 EEST	2004-0
NTUSER.DAT	▽	0	2004-08-27 18:46:23 EEST	2004-08-27 18:46:13 EEST	2004-08-27 18:46:23 EEST	2004-0
ntuser.dat.LOG		0	2004-08-27 18:46:23 EEST	2004-08-27 18:46:23 EEST	2004-08-27 18:46:23 EEST	2004-0
ntuser.ini		2	2004-08-27 18:46:23 EEST	2004-08-27 18:46:23 EEST	2004-08-27 18:46:23 EEST	2004-0

```
P/1.1
GET /hm/folder.aspx HTTP/1.1
Accept: */*
UA-OS: Windows CE (Pocket PC) - Version 4.20
UA-color: color16
UA-pixels: 240x320
UA-CPU: Intel(R) PXA255
UA-Voice: FALSE
Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; cr=1; MSPAuth=5vuMneQNFDh0sFVrAbKrt*q6edOGfSSmKzi3lT1CIh6FdbNqQyPyqubrB97DYRuoTwoA5kp1iTd3eTZ3TUiZ45LQ$$
ME!*WBUVqwsUvAh8UuflyJMTMQt*6C4vjOyvqgDT5F!XAMjAg0!vkXYwzhbCkVlAO1b2zXMjlXnmPnOpETgsIPX0coWMQ$$
U/Ay
HTTP/1.1 302 Found
Server: Microsoft-IIS/5.0
Date: Fri, 27 Aug 2004 15:36:35 GMT
X-Powered-By: ASP.NET
P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
Location: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
Cache-Control: private
```

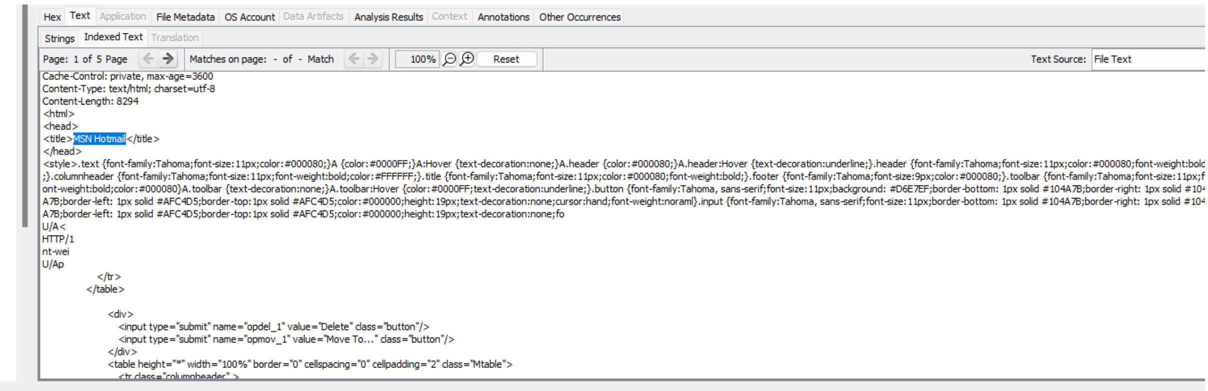
Figure 32. Interception file

From this file we can answer the question 25 too.



```
P/1.1
GET /hm/folder.aspx HTTP/1.1
Accept: */*
UA-OS: Windows CE (Pocket PC) - Version 4.20
UA-color: color16
UA-pixels: 240x320
UA-CPU: Intel(R) PXA255
UA-Voice: FALSE
Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; cr=1; MSPAuth=5vuMneQNFDh0sFVrAbKrt*q6edOGfSSmKzi3lT1CIh6FdbNqQyPyqubrB97DYRuoTwoA5kp1iTd3eTZ3TUiZ45LQ$$; MSPProf=5ynI
ME!*WBUVqwsUvAh8UuflyJMTMQt*6C4vjOyvqgDT5F!XAMjAg0!vkXYwzhbCkVlAO1b2zXMjlXnmPnOpETgsIPX0coWMQ$$
U/Ay
HTTP/1.1 302 Found
Server: Microsoft-IIS/5.0
Date: Fri, 27 Aug 2004 15:36:35 GMT
X-Powered-By: ASP.NET
P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
Location: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
Cache-Control: private
```

Figure 33. First access website



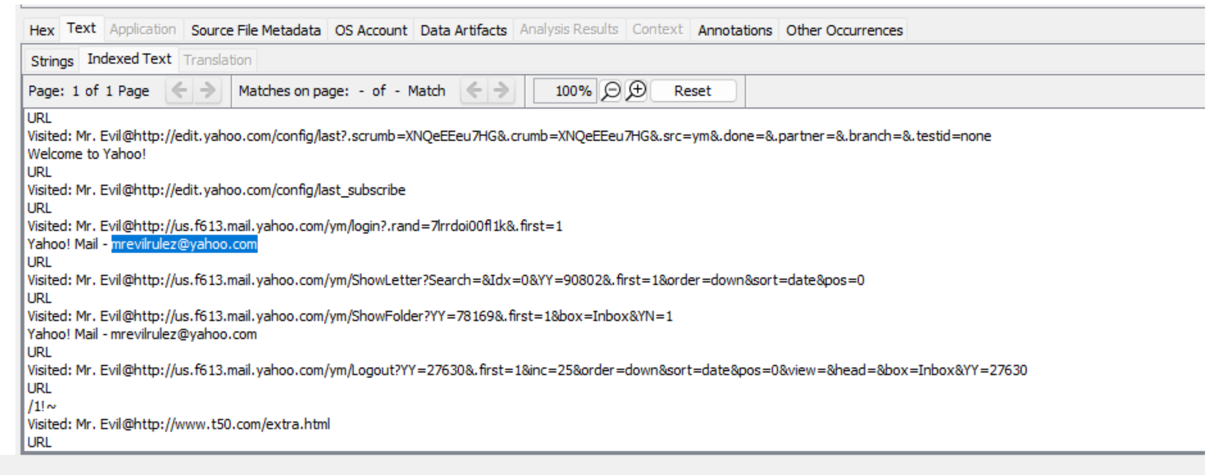
```
Cache-Control: private, max-age=3600
Content-Type: text/html; charset=utf-8
Content-Length: 8294
<html>
<head>
<title>MSN Hotmail</title>
</head>
<style>.text {font-family:Tahoma;font-size:11px;color:#000080;}A {color:#0000FF;}A:Hover {text-decoration:none;}A.header {color:#000080;}A.header:Hover {text-decoration:underline;}.header {font-family:Tahoma;font-size:11px;color:#000080;font-weight:bold
;}.columnheader {font-family:Tahoma;font-size:11px;font-weight:bold;color:#FFFFFF;}.title {font-family:Tahoma;font-size:11px;color:#000080;font-weight:bold;}.footer {font-family:Tahoma;font-size:9px;color:#000080;}.toolbar {font-family:Tahoma;font-size:11px;f
ont-weight:bold;color:#000080}A.toolbar {text-decoration:none;}A.toolbar:Hover {color:#0000FF;text-decoration:underline;}.button {font-family:Tahoma, sans-serif;font-size:11px;background: #D6E7EF;border-bottom: 1px solid #104A7B;border-right: 1px solid #104
A7B;border-left: 1px solid #AFC4D5;border-top:1px solid #AFC4D5;color:#000000;height:19px;text-decoration:none;cursor:hand;font-weight:noraml}.input {font-family:Tahoma, sans-serif;font-size:11px;border-bottom: 1px solid #104A7B;border-right: 1px solid #104
A7B;border-left: 1px solid #AFC4D5;border-top:1px solid #AFC4D5;color:#000000;height:19px;text-decoration:none;fo
U/A<
HTTP/1
nt-wei
U/Ap
         </tr>
       </table>

           <div>
             <input type="submit" name="opdel_1" value="Delete" class="button"/>
             <input type="submit" name="opmov_1" value="Move To..." class="button"/>
           </div>
           <table height="*" width="100%" border="0" cellspacing="0" cellpadding="2" class="Mtable">
             <tr class="columnheader" >
```

Figure 34. Second access website

On seeing the above images from the interception file we say that the victim tried to access the "mobile.msn.com & MSN Hotmail" website.

26. Search for the main users web based email address. What is it?

In the Extracted content web history (left-side tree structure), we can find many historical browsing files. Searching through these files, we can see some instances where the user had to login. It reveals the email address "mrevilrulez@yahoo.com".

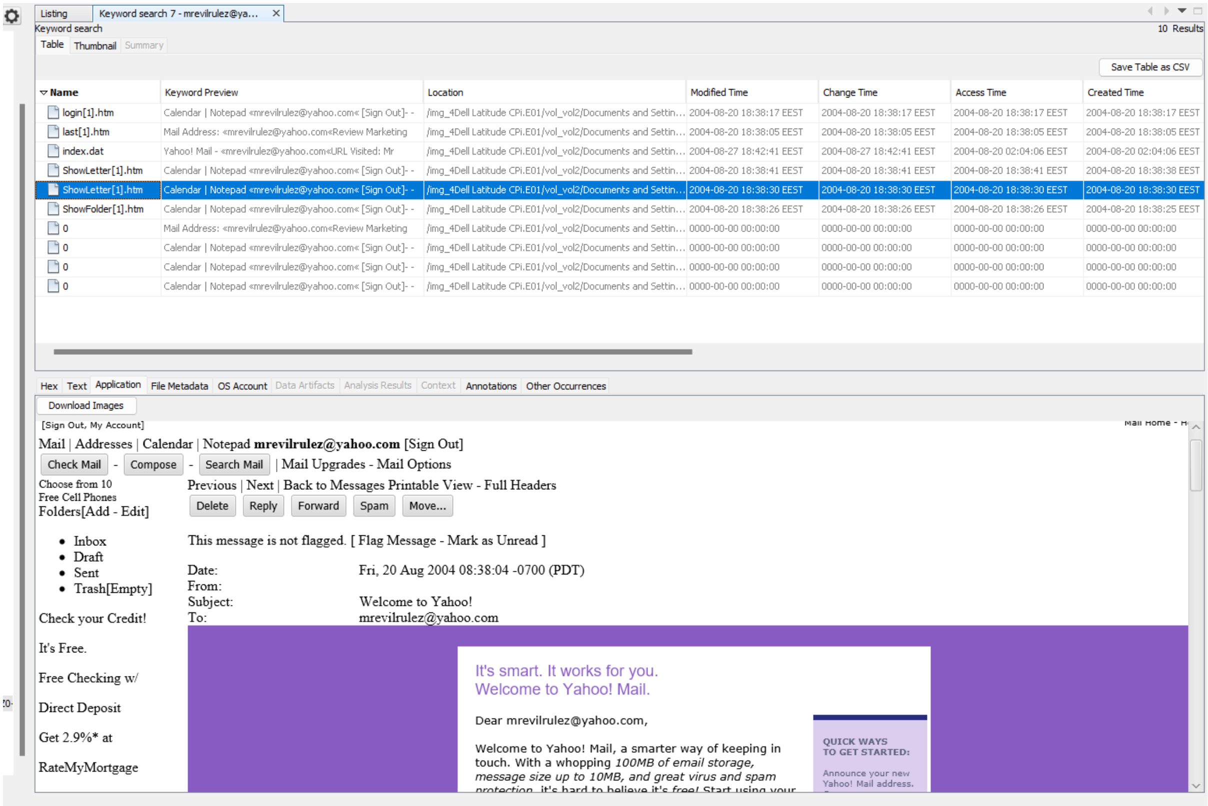


```
URL
Visited: Mr. Evil@http://edit.yahoo.com/config/last?.scrumb=XNQeEEeu7HG&.crumb=XNQeEEeu7HG&.src=ym&.done=&.partner=&.branch=&.testid=none
Welcome to Yahoo!
URL
Visited: Mr. Evil@http://edit.yahoo.com/config/last_subscribe
URL
Visited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/login?.rand=7lrrdoi00fl1k&.first=1
Yahoo! Mail - mrevilrulez@yahoo.com
URL
Visited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/ShowLetter?Search=&Idx=0&YY=90802&.first=1&order=down&sort=date&pos=0
URL
Visited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/ShowFolder?YY=78169&.first=1&box=Inbox&YN=1
Yahoo! Mail - mrevilrulez@yahoo.com
URL
Visited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/Logout?YY=27630&.first=1&inc=25&order=down&sort=date&pos=0&view=&head=&box=Inbox&YY=27630
URL
/1!~
Visited: Mr. Evil@http://www.t50.com/extra.html
URL
```

Figure 35. User main email address

27. Yahoo mail, a popular web based email service, saves copies of the email under what file name?

To find this, I do a keyword search on the email address which we found in the above question.



Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time
login[1].htm	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-20 18:38:17 EEST	2004-08-20 18:38:17 EEST	2004-08-20 18:38:17 EEST	2004-08-20 18:38:17 EEST
last[1].htm	Mail Address: «mrevilrulez@yahoo.com«Review Marketing	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-20 18:38:05 EEST	2004-08-20 18:38:05 EEST	2004-08-20 18:38:05 EEST	2004-08-20 18:38:05 EEST
index.dat	Yahoo! Mail - «mrevilrulez@yahoo.com«URL Visited: Mr	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-27 18:42:41 EEST	2004-08-27 18:42:41 EEST	2004-08-20 02:04:06 EEST	2004-08-20 02:04:06 EEST
ShowLetter[1].htm	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-20 18:38:41 EEST	2004-08-20 18:38:41 EEST	2004-08-20 18:38:41 EEST	2004-08-20 18:38:38 EEST
ShowLetter[1].htm	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-20 18:38:30 EEST	2004-08-20 18:38:30 EEST	2004-08-20 18:38:30 EEST	2004-08-20 18:38:30 EEST
ShowFolder[1].htm	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-20 18:38:26 EEST	2004-08-20 18:38:26 EEST	2004-08-20 18:38:26 EEST	2004-08-20 18:38:25 EEST
0	Mail Address: «mrevilrulez@yahoo.com«Review Marketing	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
0	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
0	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
0	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

[Sign Out, My Account]

Mail | Addresses | Calendar | Notepad **mrevilrulez@yahoo.com** [Sign Out]

Check Mail - Compose - Search Mail | Mail Upgrades - Mail Options

Choose from 10
Free Cell Phones
Folders[Add - Edit]

- Inbox
- Draft
- Sent
- Trash[Empty]

Check your Credit!

It's Free.

Free Checking w/

Direct Deposit

Get 2.9%* at

RateMyMortgage

Previous | Next | Back to Messages Printable View - Full Headers

Delete Reply Forward Spam Move...

This message is not flagged. [Flag Message - Mark as Unread]

Date: Fri, 20 Aug 2004 08:38:04 -0700 (PDT)
From:
Subject: Welcome to Yahoo!
To: mrevilrulez@yahoo.com

It's smart. It works for you.
Welcome to Yahoo! Mail.

Dear mrevilrulez@yahoo.com,

Welcome to Yahoo! Mail, a smarter way of keeping in touch. With a whopping *100MB of email storage, message size up to 10MB, and great virus and spam protection*, it's hard to believe it's *free!* Start using your

QUICK WAYS
TO GET STARTED:

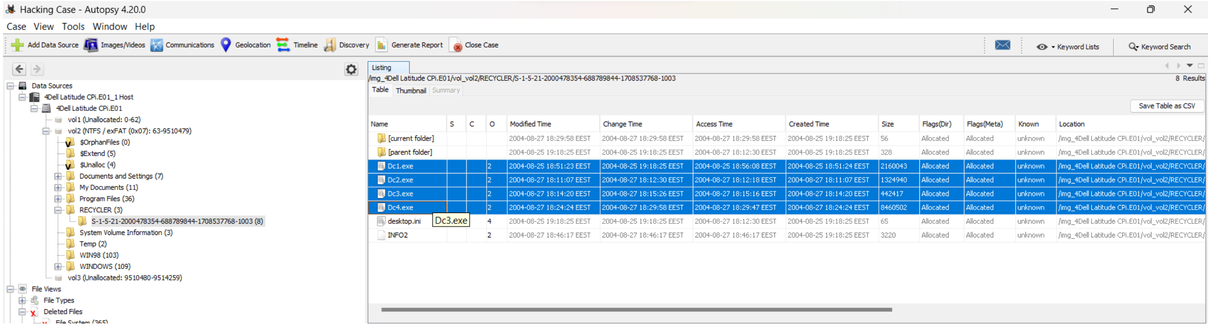
Announce your new Yahoo! Mail address.

Figure 36. Filename which stores copies of email

After searching all the files of search results I found out that "ShowLetter[1].htm" is the file in which yahoo saves copies of the email.

28. How many executable files are in the recycle bin?

For this, I go into the Recycle Bin folder whose path is:
"C:\RECYCLER\S-1–5–21–2000478354–688789844–1708537768–1003\



/img_4Dell Latitude CPi.E01/vol_vol2/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2004-08-27 18:29:58 EEST	2004-08-27 18:29:58 EEST	2004-08-27 18:29:58 EEST	2004-08-25 19:18:25 EEST	56	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/RECYCLER/
[parent folder]				2004-08-25 19:18:25 EEST	2004-08-25 19:18:25 EEST	2004-08-27 18:12:30 EEST	2004-08-25 19:18:25 EEST	328	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/RECYCLER/
Dc1.exe			2	2004-08-25 18:51:23 EEST	2004-08-25 19:18:25 EEST	2004-08-25 18:56:08 EEST	2004-08-25 18:51:24 EEST	2160043	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/RECYCLER/
Dc2.exe			2	2004-08-27 18:11:07 EEST	2004-08-27 18:12:30 EEST	2004-08-27 18:12:18 EEST	2004-08-27 18:11:07 EEST	1324940	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/RECYCLER/
Dc3.exe			2	2004-08-27 18:14:20 EEST	2004-08-27 18:15:26 EEST	2004-08-27 18:15:16 EEST	2004-08-27 18:14:20 EEST	442417	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/RECYCLER/
Dc4.exe			2	2004-08-27 18:24:24 EEST	2004-08-27 18:29:58 EEST	2004-08-27 18:29:47 EEST	2004-08-27 18:24:24 EEST	8460502	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/RECYCLER/
desktop.ini			4	2004-08-25 19:18:25 EEST	2004-08-25 19:18:25 EEST	2004-08-27 18:12:30 EEST	2004-08-25 19:18:25 EEST	65	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/RECYCLER/
INFO2			2	2004-08-27 18:46:17 EEST	2004-08-27 18:46:17 EEST	2004-08-27 18:46:17 EEST	2004-08-25 19:18:25 EEST	3220	Allocated	Allocated	unknown	/img_4Dell Latitude CPi.E01/vol_vol2/RECYCLER/

Figure 37. Recycler folder

On seeing the above image of the Recycler folder we found out that there are "4" executable files in the recycle bin.

29. Are these files really deleted?

No, they are not really deleted. As they are in the recycle bin we can restore it. They are only moved inside the recycle bin or stored inside the recycle bin, not deleted.

30. How many files are actually reported to be deleted by the file system?
To find this, we just look in the Deleted files in the left-side tree structure.

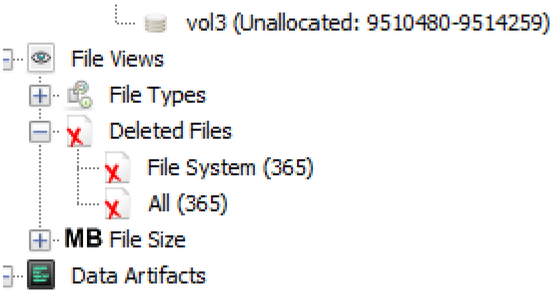


Figure 38. Deleted files

In the above image, we find out that there are a total of 365 files that are actually reported to be deleted by the file system.

31. Perform a Anti-Virus check. Are there any viruses on the computer?
Autopsy itself performs an antivirus check & it shows its result inside Interesting Items (left-side tree structure). On seeing that we find one zip bomb inside the computer whose location is “C:\My Documents\FOOTPRINTING \UNIX\unix_hack.tgz”.

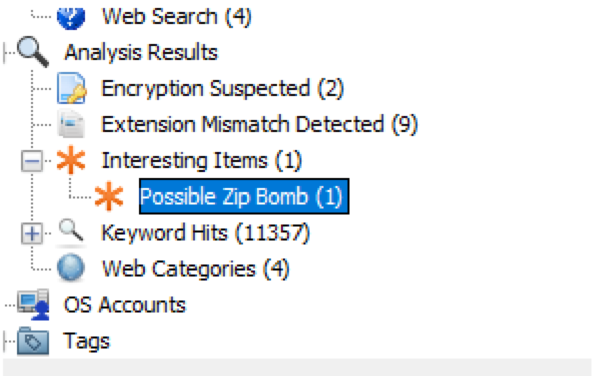
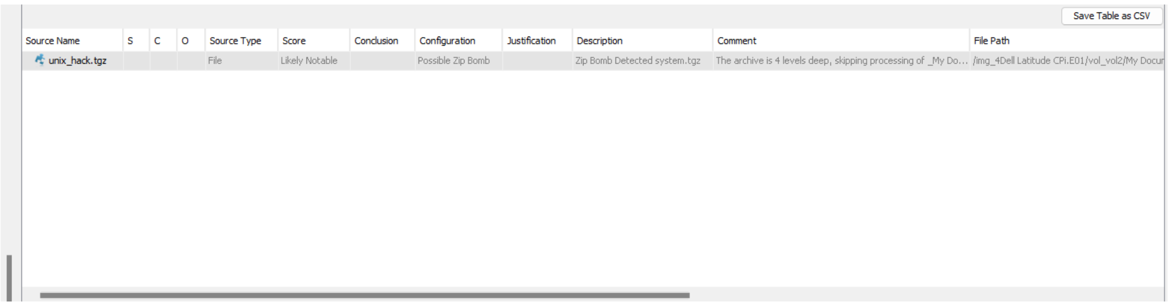


Figure 39. Possible zip bomb



Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Description	Comment	File Path
unix_hack.tgz				File	Likely Notable		Possible Zip Bomb		Zip Bomb Detected system.tgz	The archive is 4 levels deep, skipping processing of _My Do...	/img_4Dell Latitude CPi.E01/vol_vol2/My Docur

Figure 40. Malicious file

Although zip bombs are not that dangerous as compared to viruses, yet they are malicious & can crash the whole system.

Conclusion

After this writeup, it is clear now that Greg Schardt and Mr. Evil are just one single person. The seized laptop includes hacking software that was used to sniff data from victims, chats on hackers newsgroup and IRC and contains a zip bomb. So, all suspicions about Greg Schardt were true!

Chain of custody

- 01/09/2023-Reading and understanding the scenario, download disc image, open case on Autopsy and a quick look on the drive about what's inside
- 02/09/2023-Starting answering questions and deeper analysis of the disc
- 09/09/2023-Finish with the last questions and make conclusions
- 10/09/2023-Writing the report with all the findings
- 18/09/2023-Close case

Comments on the tools that used

- Autopsy loads the artifacts of the disc image a little slow, especially if the size of the disc image is big with lots of elements inside
- All the other softwares were perfect on use

Bibliography

1. Hacking Case (nist.gov)
2. https://www.autopsy.com/download/
3. Free Download Manager - download everything from the internet
4. https://www.epochconverter.com/
5. DCode™ – Timestamp Decoder - Digital Detective (digital-detective.net)
6. https://rst.im/oui/
7. Download 123 Write All Stored Passwords (WASP) - MajorGeeks
8. https://en.wikipedia.org/wiki/Anonymizer_(company)
9. https://en.wikipedia.org/wiki/Cain_and_Abel_(software)
10. Download - www.profibus.com
11. Download Look@LAN - MajorGeeks
12. The award-winning wireless networking tool and the best source for your daily Wi-Fi, WiMAX, 3G and VoIP news. | NetStumbler
13. Zip bomb - Wikipedia
14. mIRC: Internet Relay Chat client
15. Outlook Express Email Forensics – Analyze DBX Mail Header (mailxaminer.com)
16. NNTP Network News Transfer Protocol tutorial - CCNA TUTORIALS
17. Find Network Card Interfaces via Windows Registry | AndryHacks
18. determine the last logged on user? (microsoft.com)
19. FILETIME & conversion issues. – General (Technical, Procedural, Software, Hardware etc.) – Forensic Focus Forums
20. How to Determine the Last Shutdown Time and Date in Windows » Winhelponline
21. How can I set the default domain on the Windows NT logon screen? (itprotoday.com)
22. Change the Registered Owner Name in Windows 7/8/10 (helpdeskgeek.com)
23. Configuring the time zone and code page with Group Policy - Dennis Span