



Forensic Analysis for Computer Systems

Plan of the Labs:

1. Electronic data acquisition
2. Computer Forensics technics and tools
3. Volatility Framework
4. **Autopsy (Sleuthkit)**
5. FTK (Forensic ToolKit)
6. Guidance software EnCase & ProDiscover Forensic

Course Lab4: Sleuthkit/Autopsy

4.1 Introduction

4.2 How to install Autopsy

4.3 Autopsy capabilities

4.4 Go further with Autopsy

4.5 Case Study Conclusion

4.1 Introduction

Autopsy is an open source digital forensics tool developed by Basis Technology, first released in 2000. It is a free to use and quite efficient tool for hard drive investigation with features like multi-user cases, timeline analysis, registry analysis, keyword search, email analysis, media playback, EXIF analysis, malicious file detection and much more.



4.2 How to install Autopsy (Windows OS)

Step 1: Download Autopsy from : <https://www.autopsy.com/download/>

Step 2: Run the Autopsy *msi* installer file.

Step 3: If you get a Windows prompt, click Yes.

Step 4: Click through the dialog boxes until you click a button that says Finish.

Step 5: Autopsy should be installed now.

4.3 Autopsy capabilities

Now, we will see how we can use Autopsy for investigating a hard drive. For that, we will go through a popular scenario most of us come across while studying digital forensics, and that is the scenario of ***Greg Schardt***.

The scenario in brief is as follows:

- ✓ On 09/20/04, a **Dell CPi** notebook computer, serial # VLQLW, was found abandoned.
- ✓ It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect from **Schardt**.
- ✓ **Schardt** also goes by the online **username** of "**Mr. Evil**"
- ✓ and some of his associates have said that he would park his vehicle within range of Wireless Access Points

4.3 Autopsy possibilities

- ✓ where he would then intercept internet traffic, attempting to get **credit card numbers, usernames & passwords**.
- ✓ The **investigator** have to
 - find any **hacking software, evidence** of their use, and any **data** that might have been generated.
 - Attempt to tie the computer to the **Greg Schardt** suspect.
- ✓ An EnCase image* of the abandoned computer have already been made.

* <https://cfreds.nist.gov/all/NIST/HackingCase>

The mission for us is to analyze this Encase Image and answer to questions about this case. Let's start analyzing this image and solve the case:

1) Once the program is installed, open it and click on "New Case".



2) Provide the **Case Name** and the **directory** to store the case file. Click on **Next**.

New Case Information

Steps

1. **Case Information**
2. Optional Information

Case Information

Case Name:

Base Directory:

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

< Back **Next >** Finish Cancel Help

3) Add Case Number and Examiner's details, then click on Finish.

New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 12

Examiner

Name: Lab

Phone: 8977677889

Email: lab@gmail.com

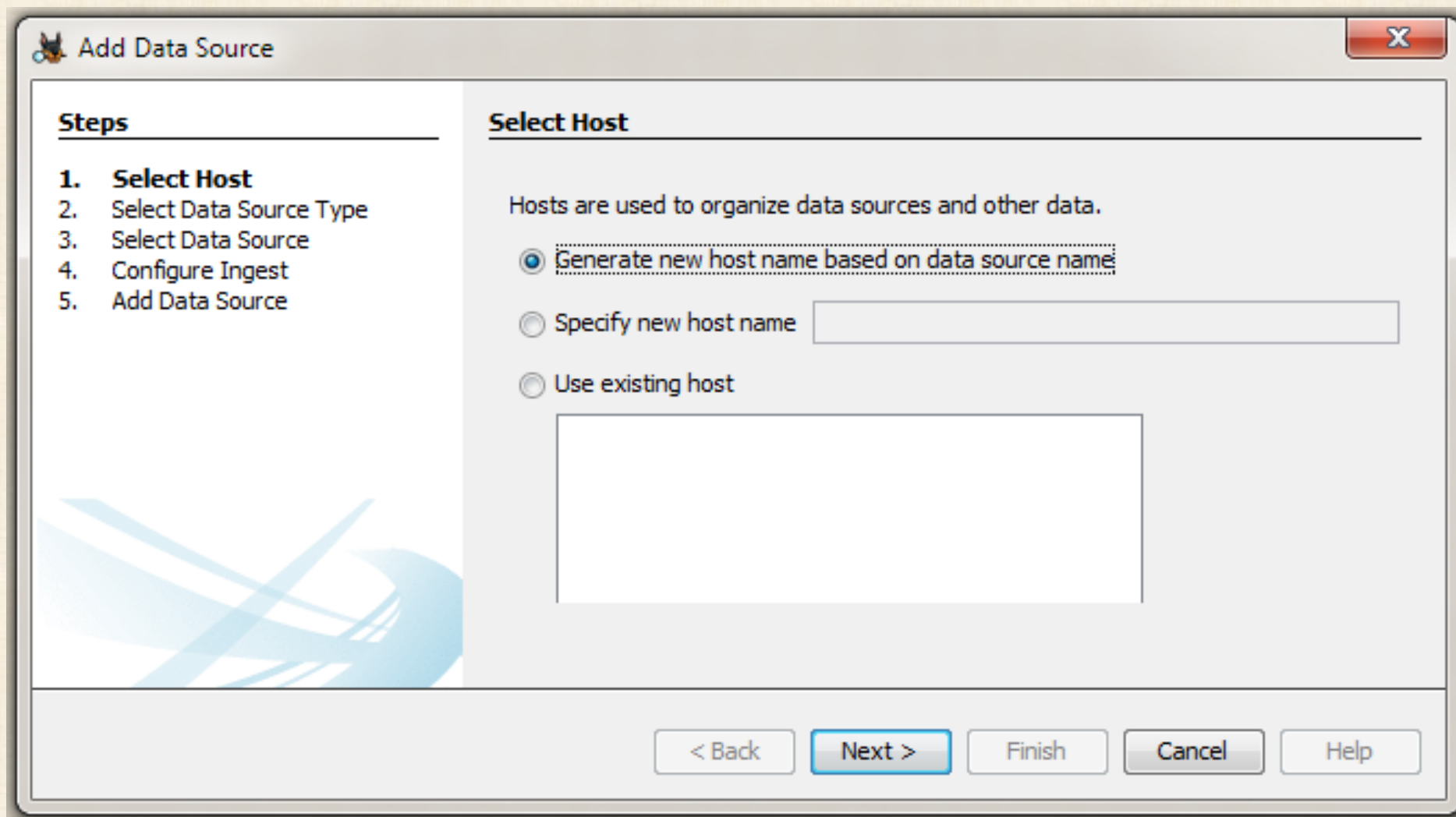
Notes:

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > Finish Cancel Help

4) Select **Host** which is used to organize data sources, in this case choose ***Generate new name based on data source name*** and click on ***Next***



The screenshot shows the 'Add Data Source' dialog box in Autopsy. The window has a title bar with a close button (X). On the left, a 'Steps' pane lists five steps: 1. Select Host, 2. Select Data Source Type, 3. Select Data Source, 4. Configure Ingest, and 5. Add Data Source. The first step, 'Select Host', is currently active. The main area is titled 'Select Host' and contains the text: 'Hosts are used to organize data sources and other data.' Below this text are three radio button options: 'Generate new host name based on data source name' (which is selected), 'Specify new host name' (with an adjacent text input field), and 'Use existing host' (with an adjacent list box). At the bottom of the dialog are five buttons: '< Back', 'Next >' (highlighted with a blue border), 'Finish', 'Cancel', and 'Help'.

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.

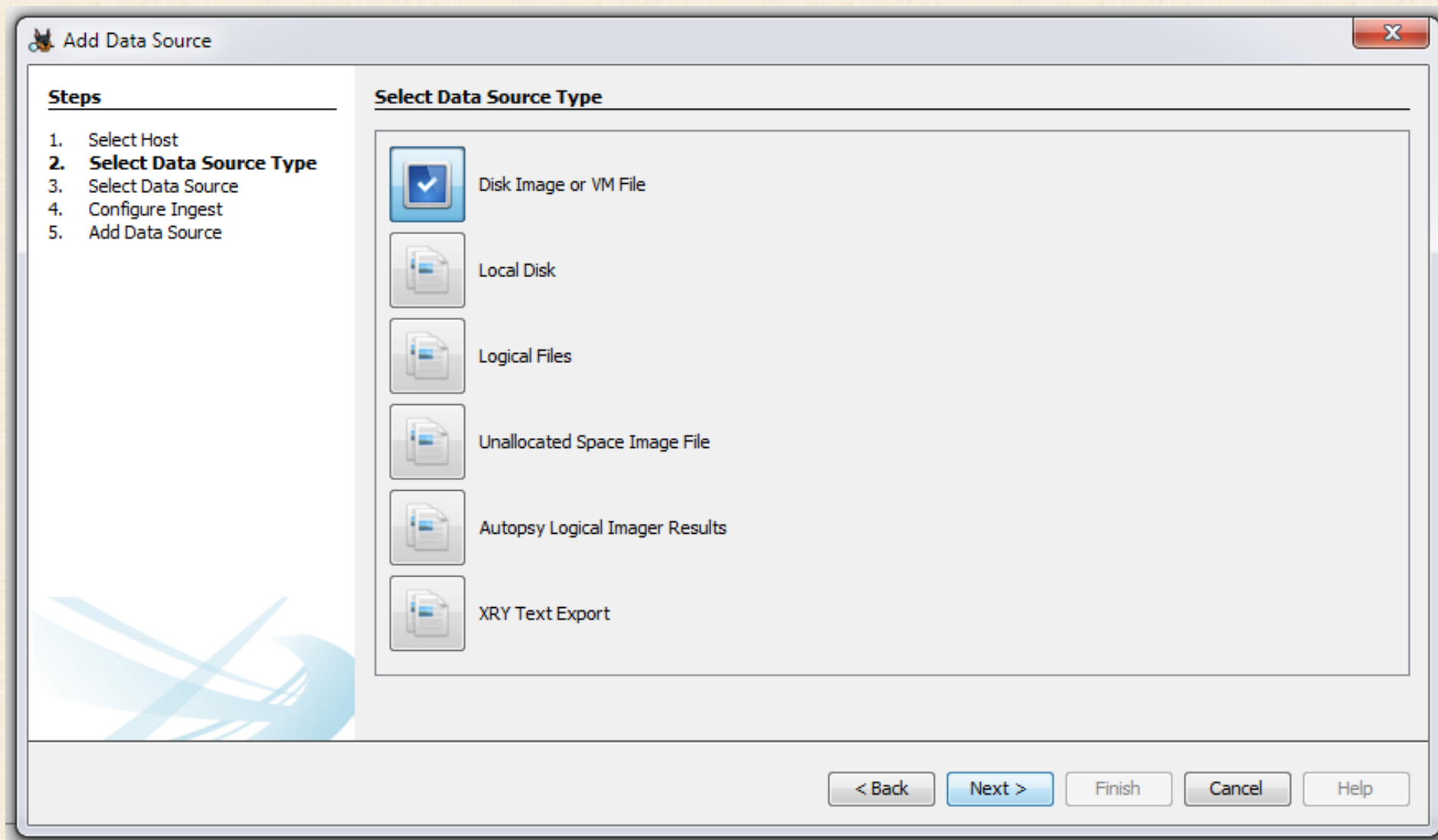
☒ Generate new host name based on data source name

☐ Specify new host name

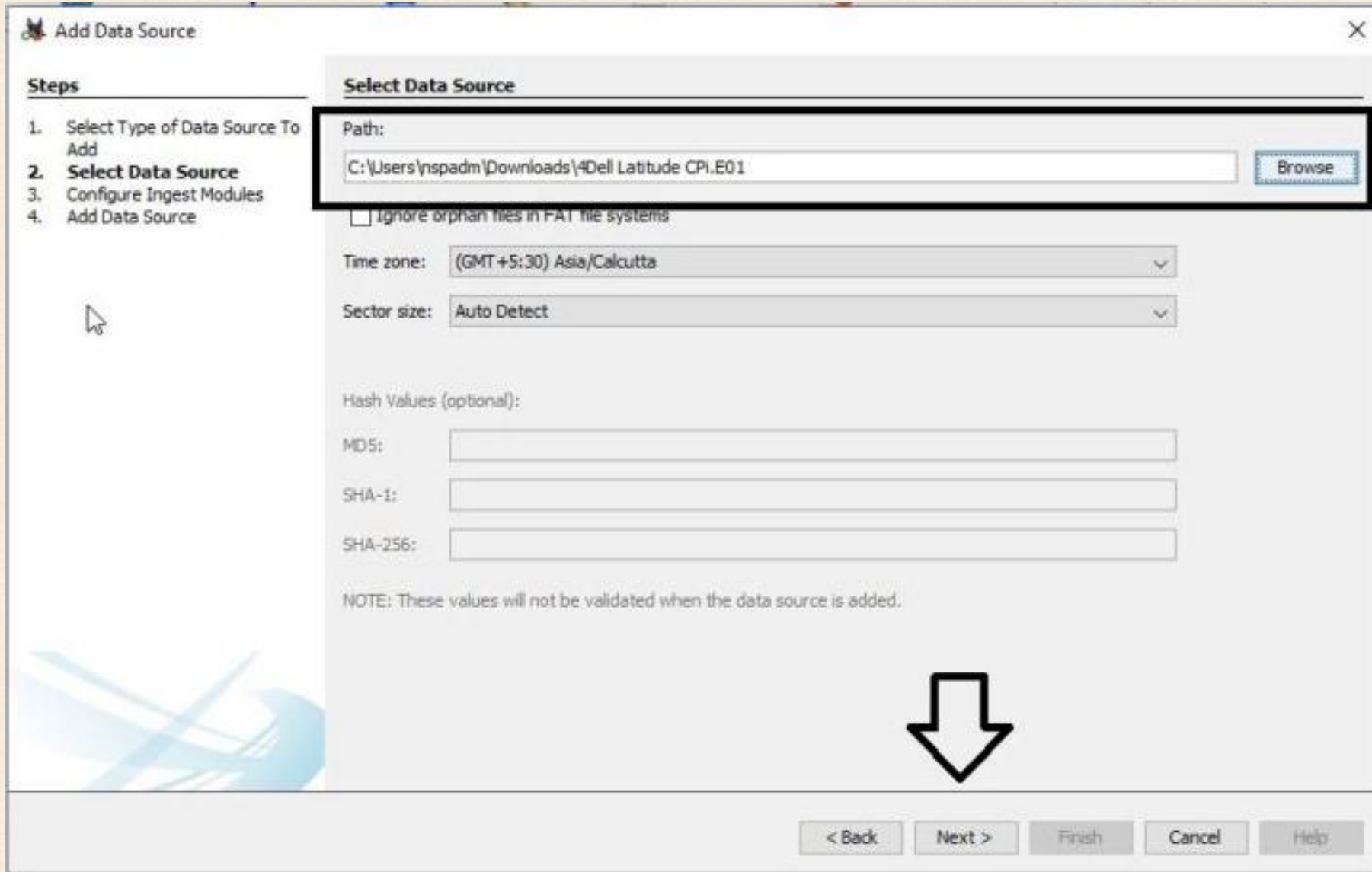
☐ Use existing host

< Back **Next >** Finish Cancel Help

5) Choose the required **data source type**, in this case ***Disk Image*** and click on ***Next***



6) Give path of the data source and click on **Next**.



Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path: C:\Users\nspadm\Downloads\4Dell Latitude CPI.E01 Browse

☐ Ignore orphan files in FAT file systems

Time zone: (GMT +5:30) Asia/Calcutta

Sector size: Auto Detect

Hash Values (optional):

MD5:

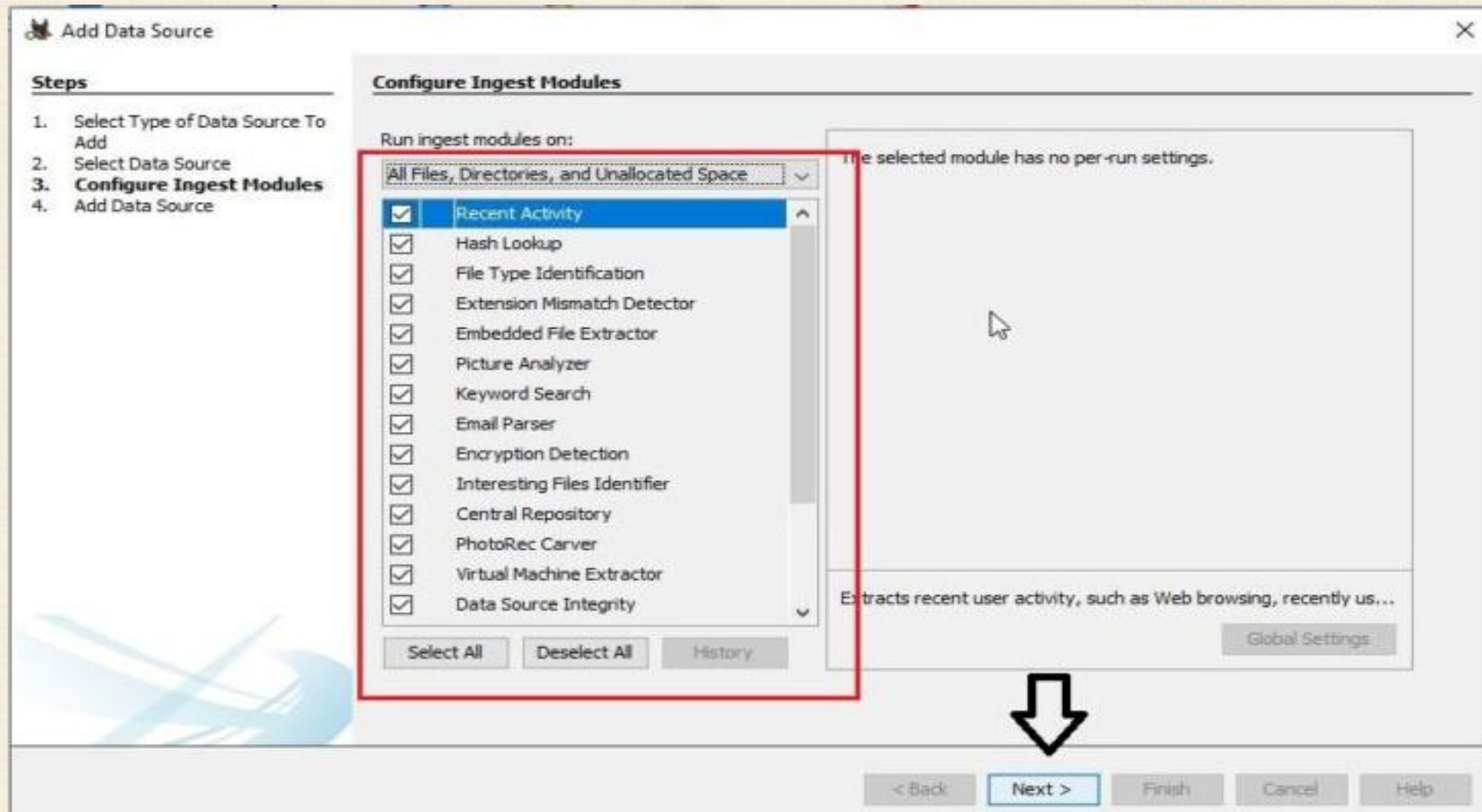
SHA-1:

SHA-256:

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

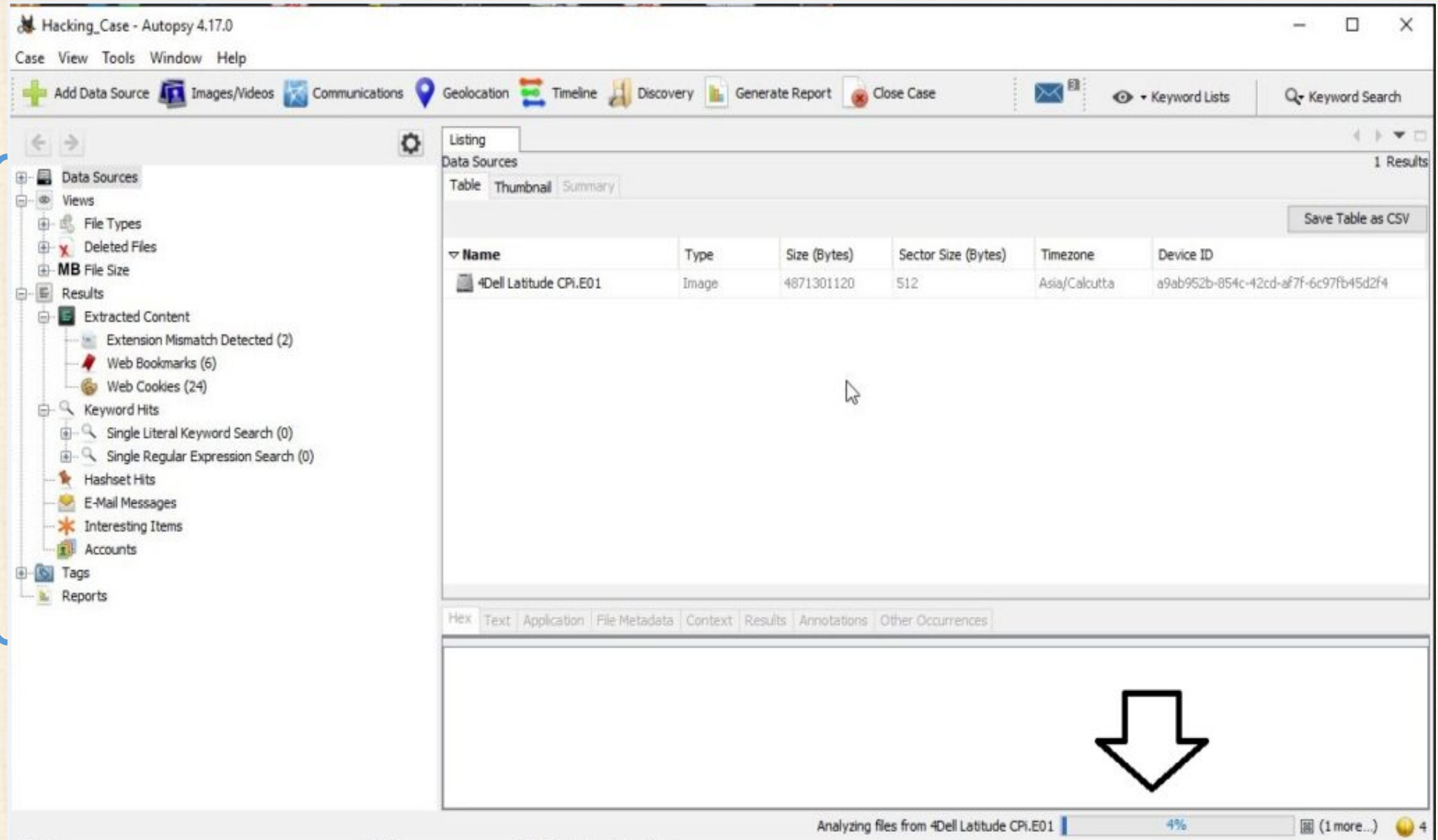
Navigation: < Back, Next >, Finish, Cancel, Help

7) Select all the **ingest modules** we want to run. Ingest modules are all the tests that can be run on the image to gather information about it. These ingest modules include tests like **hash lookup**, **email parsing** etc then click **Next**.



8) Analysis of image file is automatically launched. However, it will start displaying findings as soon as it finds them.

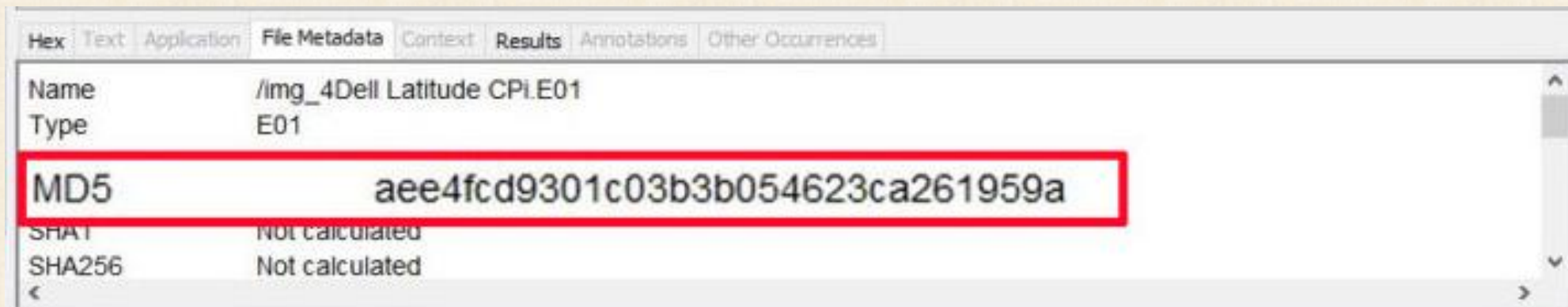
All the extracted information can be found on the left side of the Autopsy window.



9) At this stage we are ready to start our **investigation**, which is achieved across **important questions**:

Where is the image Hash?

- ✓ In Digital Forensics, as soon as an image is acquired to perform analysis on it, a **hash** is calculated to check if the file integrity is intact and not compromised.
- ✓ If the acquisition and verification hash do not match, it means our forensic analysis has changed the image which is not at all intended.
- ✓ The image hash is “**AEE4FCD9301C03B3B054623CA261959A**” . It is found in the **File Metadata** tab.



What operating system was installed on the computer ?

The operating system information can be found in the operating system information of the extracted content (in the left side panel, we go to **Results > Extracted Content > Operating System Information**).

The screenshot shows the Autopsy 4.17.0 interface. On the left sidebar, under 'Results' > 'Extracted Content', 'Operating System Information (2)' is selected and highlighted with a red box. The main panel displays a table of results for 'Operating System Information' with 2 results. The table has columns: Directory, Data Source, Program Name, Date/Time, Path, Product ID, Owner, and Organization. The first result is highlighted in blue.

Directory	Data Source	Program Name	Date/Time	Path	Product ID	Owner	Organization
TEMP	4Dell Latitude CPl.E01						
	4Dell Latitude CPl.E01	Microsoft Windows XP	2004-08-19 22:48:27 IST	C:\WINDOWS	55274-640-0147306-23684	Greg Schardt	N/A

Below the table, the 'Results' tab is active, showing a detailed view of the first result. The 'Program Name' field is highlighted with a red box and contains the text 'Microsoft Windows XP'.

Operating System Information	
Result: 1	
Type	
Program Name	Microsoft Windows XP
Date/Time	2004-08-19 22:48:27
Path	C:\WINDOWS

Who is the registered owner?

information about the registered owner of the computer is found in the same operating system info section in extracted content.

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 1 of 56 Result < >

Operating System Information

Type	Value	Source(s)
Owner	Greg Schardt	Recent Activity
Organization	N/A	Recent Activity

The install date can be found in the same operating system info section just below the OS information.

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Result: 1 of 56					Result	Operating System Information	
Date/Time					Source(s)		
2004-08-19 22:48:27					Recent Activity		
Path					Recent Activity		
C:\WINDOWS					Recent Activity		
<					>		

What is the computer account name?

The computer account name on this computer is found in the same section.

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Result: 2 of 2						Operating System Information	
Name		N-1A90DN6ZXK4LQ				Source(s)	
Domain						Recent Activity	^
Version		Windows_NT				Recent Activity	v
<						>	

How many accounts are recorded?

The information about the user accounts is found in the Operating system user account section (In the left side panel, we go to **Results > Extracted Content > Operating System User Account**)

Listing
Operating System User Account 8 Results

Source File	S	C	User ID	Username	Date Created	Count	Account Type
SAM			S-1-5-21-2000478354-688789844-1708537768-500	Administrator	9:24 IST	0	Default Admin
SAM			S-1-5-21-2000478354-688789844-1708537768-1003	Mr. Evil	3:54 IST	15	Default Admin
SAM			S-1-5-21-2000478354-688789844-1708537768-1002		5:19 IST	0	Custom Limite
SAM			S-1-5-21-2000478354-688789844-1708537768-501	SUPPORT_388945a0	9:24 IST	0	Default Guest
SAM			S-1-5-21-2000478354-688789844-1708537768-1000	Guest	8:24 IST	0	Custom Limite
software			S-1-5-18				
software			S-1-5-19				
software			S-1-5-20				

What is the account name of the user who mostly uses the computer?

In the same section, the **count** section shows how many times the user logged in.

Username	Date Created	Count
Administrator	2004-08-19 22:29:24 IST	0
Mr. Evil	2004-08-20 04:33:54 IST	15
SUPPORT_388945a0	2004-08-20 04:05:19 IST	0
Guest	2004-08-19 22:29:24 IST	0
HelpAssistant	2004-08-20 03:58:24 IST	0

Who was the last user to logon to the computer?

The information about the last user to logon to this computer can be found from the Date ***accessed column*** of the user account.

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Result: 2 of 5		Result		Operating System User Account			
						Source(s)	
Date Created	2004-08-20 04:33:54					Recent Activity	^
Date Accessed	2004-08-27 20:38:23					Recent Activity	
Count	15					Recent Activity	v

When was the last recorded computer shutdown date/time?

To find this we go to

C:\WINDOWS\system32\config\software\Microsoft\WindowNT\CurrentVersion\Prefetcher\ExitTime

The screenshot shows the Autopsy 4.17.0 interface. The left sidebar displays a file tree with the path `config (23)` expanded. The main pane shows a table of files in the `software` directory. The `software` directory is highlighted, and its contents are listed in a table. The `software` directory is highlighted, and its contents are listed in a table.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size
SecEvent.Evt			2004-08-19 22:29:15 IST	2004-08-19 22:32:15 IST	2004-08-19 22:29:15 IST	2004-08-19 22:29:15 IST	65536
SECURITY			2004-08-27 21:16:33 IST	2004-08-20 04:34:03 IST	2004-08-27 21:16:33 IST	2004-08-19 22:28:55 IST	262144
SECURITY.LOG			2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-19 22:28:55 IST	1024
software			2004-08-27 21:16:33 IST	2004-08-27 20:59:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	8650752
software.LOG			2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-19 22:26:08 IST	1024
software.sav			2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:18 IST	630784
SysEvent.Evt			2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-19 22:29:15 IST	65536
system			2004-08-27 21:16:33 IST	2004-08-27 21:01:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:06 IST	2621440
system.LOG			2004-08-27 21:16:33 IST	2004-08-27 21:16:33 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	1024
system.sav			2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:18 IST	389120

The bottom pane shows the `Prefetcher` directory. The `ExitTime` value is highlighted, showing the date and time of the last recorded shutdown: `2004/08/27-10:46:27`.

Find the installed programs that may be used for hacking ?

The programs installed on the computer system can be found out from the **Installed programs** section of the **extracted content**.

The screenshot shows the Autopsy 4.17.0 interface. On the left sidebar, under 'Results' > 'Extracted Content', the 'Installed Programs (32)' item is highlighted with a red box. The main window displays a table of installed programs. The table has columns: Source File, S, C, Program Name, Date/Time, and Data Source. The row for 'Network Stumbler 0.4.0 (remove only)' is highlighted in blue. Below the table, a detailed view of the selected program is shown.

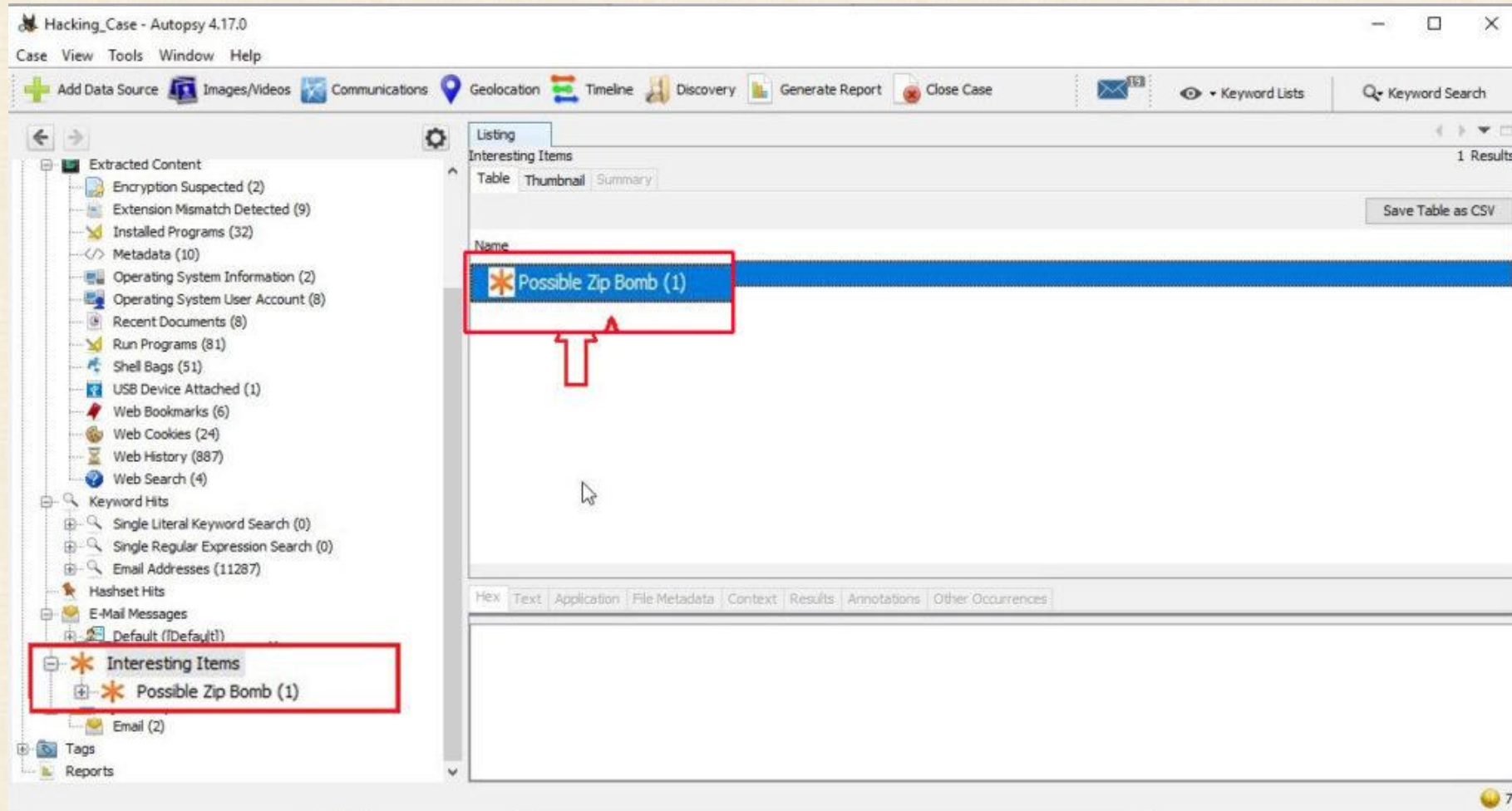
Source File	S	C	Program Name	Date/Time	Data Source
software			Ethereal 0.10.6 v.0.10.6	2004-08-27 15:29:19 IST	4Dell Latitude CPI.E01
software			WinPcap 3.01 alpha	2004-08-27 15:15:19 IST	4Dell Latitude CPI.E01
software			Network Stumbler 0.4.0 (remove only)	2004-08-27 15:12:15 IST	4Dell Latitude CPI.E01
software			Look@LAN 2.50 Build 29	2004-08-25 15:56:11 IST	4Dell Latitude CPI.E01
software			123 Write All Stored Passwords	2004-08-20 15:13:08 IST	4Dell Latitude CPI.E01
software			Powertoys For Windows XP v.1.00.0000	2004-08-20 15:12:43 IST	4Dell Latitude CPI.E01
software			mIRC	2004-08-20 15:10:04 IST	4Dell Latitude CPI.E01
software			CuteHTML	2004-08-20 15:09:03 IST	4Dell Latitude CPI.E01
software			CuteFTP	2004-08-20 15:09:02 IST	4Dell Latitude CPI.E01
software			Forté Agent	2004-08-20 15:08:19 IST	4Dell Latitude CPI.E01

Type	Value	Source(s)
Program Name	Network Stumbler 0.4.0 (remove only)	Recent Activity
Date/Time	2004-08-27 15:12:15	Recent Activity
Source File Path	/img_4Dell Latitude CPI.E01/vol_vol2/WINDOWS/system32/config/software	

From previous window there are eight programs that can be used for hacking:

1. **Cain & Abel v2.5 beta45** (password sniffer & cracker)
2. **Ethereal** (packet sniffer)
3. **123 Write All Stored Passwords** (finds passwords in registry)
4. **Anonymizer** (hides IP tracks when browsing)
5. **CuteFTP** (FTP software)
6. **Look@LAN 2.50 Build 29**(network discovery tool)
7. **Network Stumbler 0.4.0** (wireless access point discovery tool)
8. **WinPcap 3.01 alpha** (provide low-level network access and a library that is used to easily access low-level network layers.)

Perform an Anti-Virus check. Are there any viruses on the computer?
 Malicious files (if any) are found in the **Interesting** Items section of the **extracted content**.



4.4 Go further with Autopsy

A search for the name of “Greg Schardt” reveals multiple hits. One of these proves that Greg Schardt is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to?

The file that reveals all this information is:
C:\Program Files\Look@LAN\irunin.ini

The screenshot shows the Autopsy 4.17.0 interface. On the left, the file tree is expanded to 'Look@LAN (18)'. The main pane shows a listing of files in 'Look@LAN'. The file 'irunin.ini' is selected. The bottom pane shows the 'Strings' tab, displaying the contents of 'irunin.ini'. A red box highlights the following text:

```
%REGOWNER%=Greg Schardt
%REGORGANIZATION%=N/A
```

Name	S	C	Modified Time	Change Time	Access Time	Created Time
irunin.ini			2004-08-25 21:26:10 IST	2004-08-25 21:26:10 IST	2004-08-25 21:26:10 IST	2004-08-25 21:26:09 IST
irunin.lng			2004-08-25 21:25:27 IST	2004-08-25 21:25:27 IST	2004-08-25 21:26:09 IST	2004-08-25 21:26:09 IST
lalassoc.dat			2003-04-27 19:01:26 IST	2004-08-25 21:26:05 IST	2004-08-26 20:36:15 IST	2004-02-16 16:21:14 IST
lalservices.dat			2004-02-18 14:54:32 IST	2004-08-25 21:26:05 IST	2004-08-26 20:36:18 IST	2004-02-16 16:21:14 IST
License.txt			2004-02-17 16:18:00 IST	2004-08-25 21:26:11 IST	2004-02-18 15:30:03 IST	2004-02-17 16:10:55 IST
Look@LAN on the WEB.url			2004-02-17 16:01:21 IST	2004-08-25 21:26:11 IST	2004-02-18 14:49:04 IST	2004-02-17 16:01:39 IST
LookAtHost.ENG			2003-06-18 17:30:18 IST	2004-08-25 21:26:07 IST	2004-08-26 20:28:25 IST	2004-02-18 15:29:27 IST
LookAtHost.exe			2003-06-18 17:30:17 IST	2004-08-27 20:48:04 IST	2004-08-26 20:28:25 IST	2004-02-18 15:29:27 IST
LookAtLan.ENG			2004-02-18 15:21:40 IST	2004-08-25 21:26:07 IST	2004-08-26 20:28:36 IST	2004-02-18 05:05:22 IST
LookAtLan.exe			2004-02-18 15:21:39 IST	2004-08-27 20:48:04 IST	2004-08-26 20:28:49 IST	2004-02-18 05:05:21 IST

4.4 Go further with Autopsy

This same file reports the IP address and MAC address of the computer. What are they?

The IP address of this machine is 192.168.1.111 and the MAC address is 0010a4933e09. The LAN user is Mr. Evil. This confirms that Mr. Evil and Greg Schardt are one and the same.

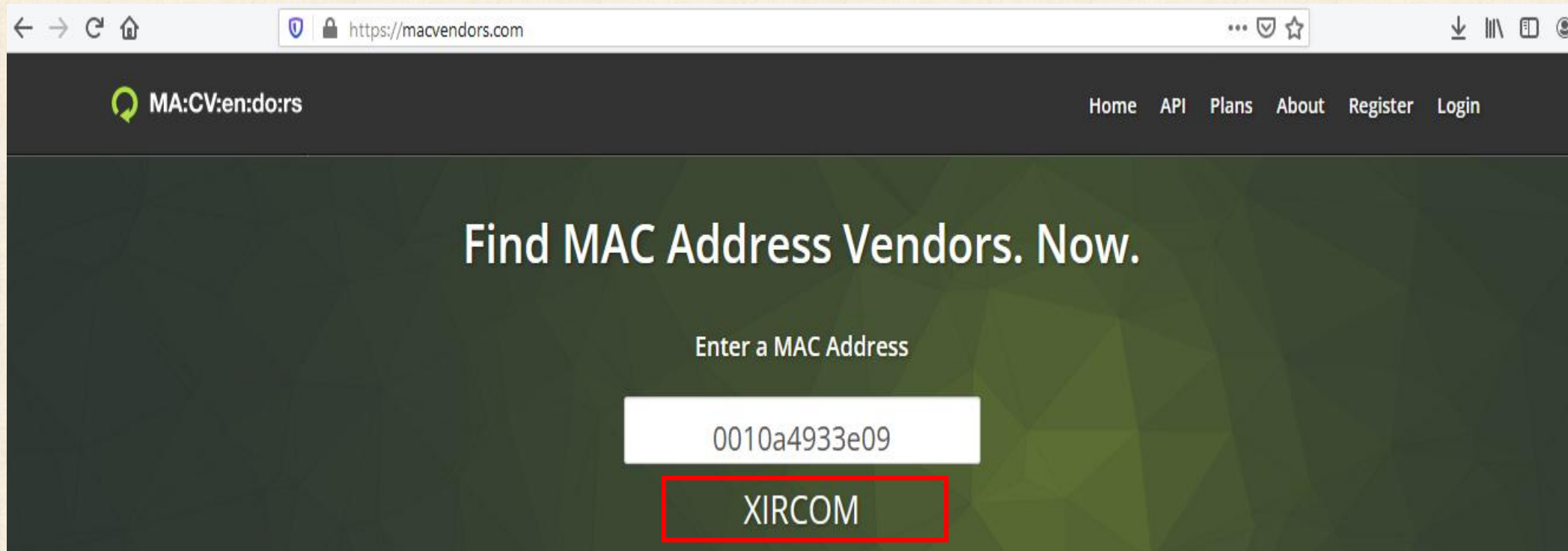
The screenshot shows the Autopsy 4.17.0 interface. The left pane displays a file tree with various folders like 'Program Files', 'Accessories', 'Agent', etc. The right pane shows a file listing for the path '/mg_4Dell Latitude CPl.E01/vol_vol2/Program Files/Look@LAN'. The file 'Look@LAN.exe' is selected. Below the listing, the 'File Metadata' tab is active, showing a table of strings. The strings include 'LANDOMAIN', 'LANUSER', 'LANIP', 'LANNIC', and 'ISWIN95'.

Name	S	C	Modified Time	Change Time	Access Time	Created Time
irunin.ini			2004-08-25 21:26:10 IST	2004-08-25 21:26:10 IST	2004-08-25 21:26:10 IST	2004-08-25 21:26:09 IST
irunin.lng			2004-08-25 21:25:27 IST	2004-08-25 21:25:27 IST	2004-08-25 21:26:09 IST	2004-08-25 21:26:09 IST
lalassoc.dat			2003-04-27 19:01:26 IST	2004-08-25 21:26:05 IST	2004-08-26 20:36:15 IST	2004-02-16 16:21:14 IST
lalservices.dat			2004-02-18 14:54:32 IST	2004-08-25 21:26:05 IST	2004-08-26 20:36:18 IST	2004-02-16 16:21:14 IST
License.txt			2004-02-17 16:18:00 IST	2004-08-25 21:26:11 IST	2004-02-18 15:30:03 IST	2004-02-17 16:10:55 IST
Look@LAN on the WEB.url			2004-02-17 16:01:21 IST	2004-08-25 21:26:11 IST	2004-02-18 14:49:04 IST	2004-02-17 16:01:39 IST
LookAtHost.ENG			2003-06-18 17:30:18 IST	2004-08-25 21:26:07 IST	2004-08-26 20:28:25 IST	2004-02-18 15:29:27 IST
LookAtHost.exe			2003-06-18 17:30:17 IST	2004-08-27 20:48:04 IST	2004-08-26 20:28:25 IST	2004-02-18 15:29:27 IST
LookAtLan.ENG			2004-02-18 15:21:40 IST	2004-08-25 21:26:07 IST	2004-08-26 20:28:36 IST	2004-02-18 05:05:22 IST
LookAtLan.exe			2004-02-18 15:21:39 IST	2004-08-27 20:48:04 IST	2004-08-26 20:28:49 IST	2004-02-18 05:05:21 IST

The 'File Metadata' tab shows the following strings:

- LANDOMAIN=N-1A9ODN6ZXK4LQ
- LANUSER=Mr. Evil
- LANIP=192.168.1.111
- LANNIC=0010a4933e09
- ISWIN95=FALSE

An internet search for MAC address vendor name/model 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 Network Interface Card was used during the installation and set-up for LOOK@LAN program?



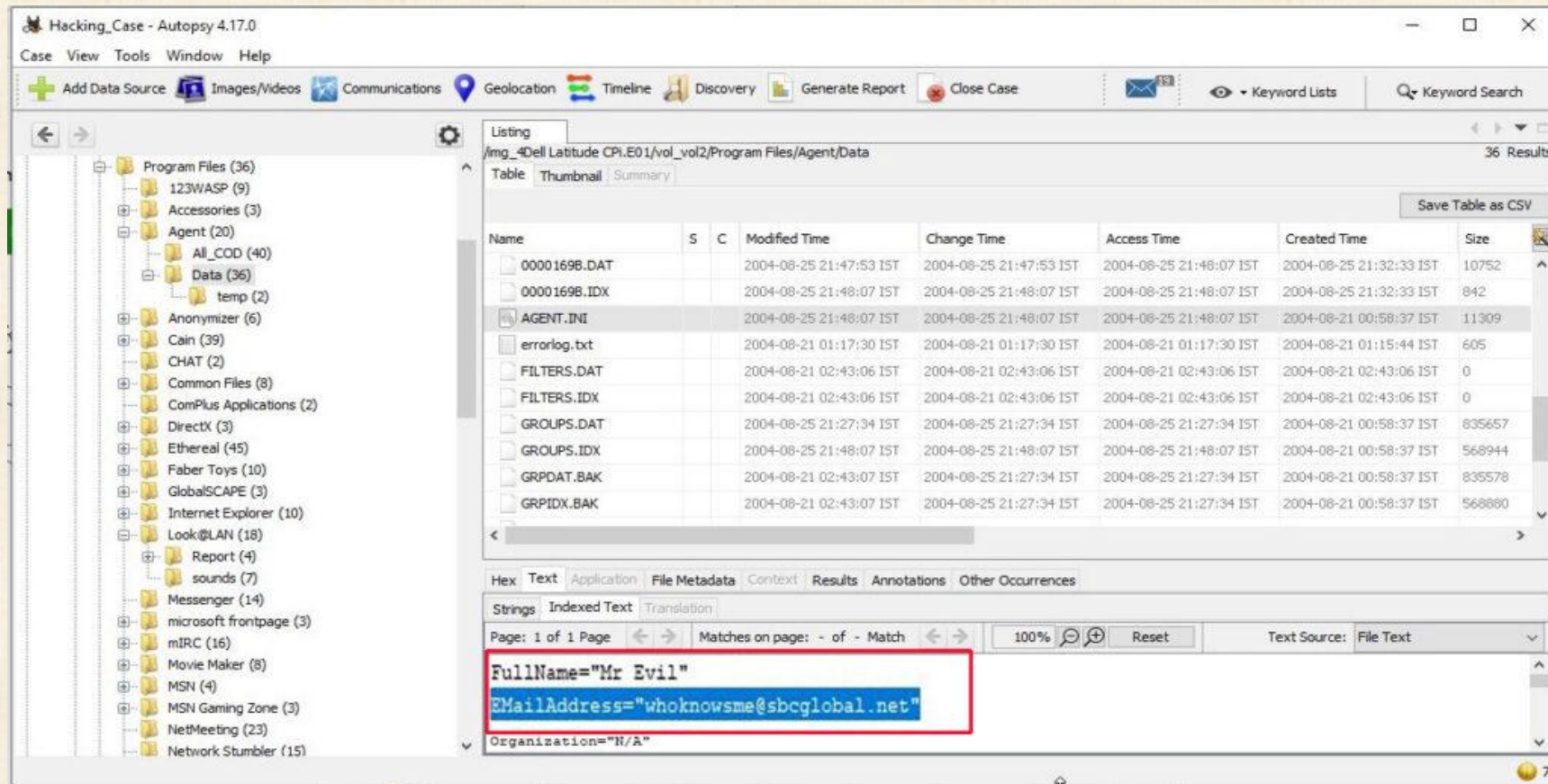
The screenshot shows a web browser window with the URL <https://macvendors.com>. The website has a dark header with the logo "MA:CV:en:do:rs" and navigation links: Home, API, Plans, About, Register, and Login. The main content area has a dark green background with the text "Find MAC Address Vendors. Now." and a form labeled "Enter a MAC Address". The form contains the MAC address "0010a4933e09" and the vendor name "XIRCOM" is displayed below it, highlighted with a red rectangular box.

The Vendor of this Network Card is **XIRCOM**.

4.4 Go further with Autopsy

What is the SMTP email address for Mr. Evil ?

SMTP or Simple Mail Transfer Protocol is a protocol used to send emails. The SMTP email address if present on the system can be found in `C:\Program Files \Agent\Data\AGENT.INI`.



The screenshot shows the Autopsy 4.17.0 interface. On the left, the file tree is expanded to 'Program Files (36)' > 'Agent (20)' > 'Data (36)' > 'temp (2)'. The main pane shows a listing of files in the directory `/img_4Dell Latitude CPl.E01/vol2/Program Files/Agent/Data`. The file `AGENT.INI` is selected. Below the listing, the 'Strings' tab is active, showing the contents of the file. The string `EEmailAddress="whoknowsme@sbcglobal.net"` is highlighted with a red box.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size
0000169B.DAT			2004-08-25 21:47:53 IST	2004-08-25 21:47:53 IST	2004-08-25 21:48:07 IST	2004-08-25 21:32:33 IST	10752
0000169B.IDX			2004-08-25 21:48:07 IST	2004-08-25 21:48:07 IST	2004-08-25 21:48:07 IST	2004-08-25 21:32:33 IST	842
AGENT.INI			2004-08-25 21:48:07 IST	2004-08-25 21:48:07 IST	2004-08-25 21:48:07 IST	2004-08-21 00:58:37 IST	11309
errorlog.txt			2004-08-21 01:17:30 IST	2004-08-21 01:17:30 IST	2004-08-21 01:17:30 IST	2004-08-21 01:15:44 IST	605
FILTERS.DAT			2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	0
FILTERS.IDX			2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	2004-08-21 02:43:06 IST	0
GROUPS.DAT			2004-08-25 21:27:34 IST	2004-08-25 21:27:34 IST	2004-08-25 21:27:34 IST	2004-08-21 00:58:37 IST	635657
GROUPS.IDX			2004-08-25 21:48:07 IST	2004-08-25 21:48:07 IST	2004-08-25 21:48:07 IST	2004-08-21 00:58:37 IST	568944
GRPDAT.BAK			2004-08-21 02:43:07 IST	2004-08-25 21:27:34 IST	2004-08-25 21:27:34 IST	2004-08-21 00:58:37 IST	835578
GRPIDX.BAK			2004-08-21 02:43:07 IST	2004-08-25 21:27:34 IST	2004-08-25 21:27:34 IST	2004-08-21 00:58:37 IST	568880

Strings: Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

FullName="Mr Evil"

EEmailAddress="whoknowsme@sbcglobal.net"

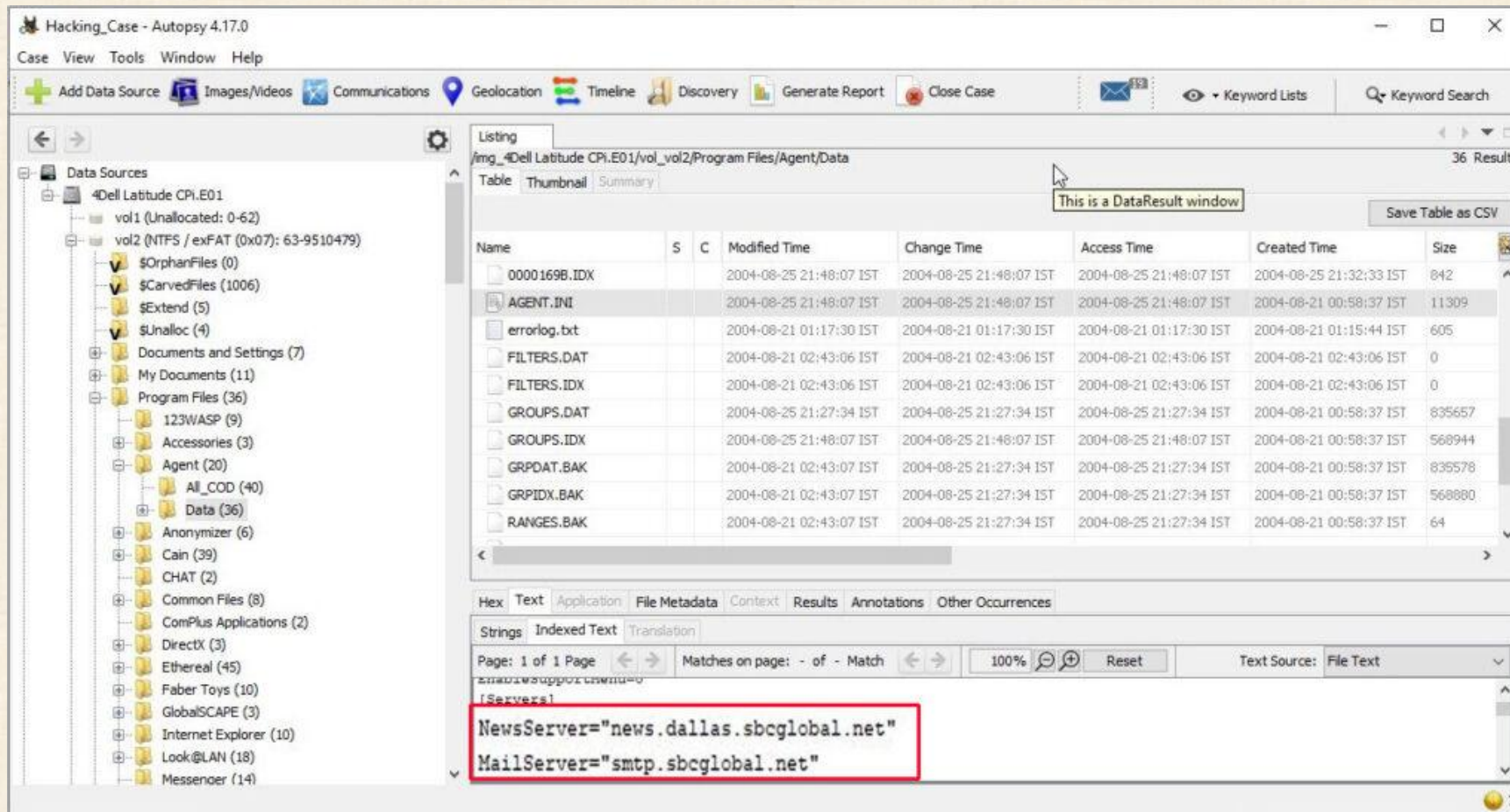
Organization="N/A"

The SMTP email address is "whoknowsme@sbcglobal.net".

4.4 Go further with Autopsy

What are the NNTP (News Servers or netNews) settings for Mr. Evil?

This information can be found in the same file as above.



The screenshot shows the Autopsy 4.17.0 interface. On the left, the 'Data Sources' tree is expanded to 'Program Files (36)' > 'Agent (20)' > 'Data (36)'. The main pane shows a listing of files in the directory '/img_4Dell Latitude CPl.E01/vol2/Program Files/Agent/Data'. The file 'AGENT.INI' is selected. A tooltip indicates 'This is a DataResult window'. Below the file listing, the 'Strings' tab is active, showing the contents of 'AGENT.INI'. The text is as follows:

```

[Servers]
NewsServer="news.dallas.sbcglobal.net"
MailServer="smtp.sbcglobal.net"
  
```

The Network News Transfer Protocol Server being used is “news.dallas.sbcglobal.net”.

What the installed program that shows this information ?

We searched for local settings of all programs and found the information about this news server in the local settings of Outlook Express.

The screenshot shows the Autopsy 4.17.0 interface. On the left, the file tree is expanded to show the path: `/img_4Dell Latitude CPI.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/`. The file `alt.2600.cardz.dbx` is selected. The main pane displays a table of files with columns: Name, S, C, Modified Time, Change Time, Access Time, and Created Time. The file `alt.2600.cardz.dbx` is highlighted. Below the table, the search results for the selected file are shown, displaying the text: `news.dallas.sbcglobal.net000000002`.

Name	S	C	Modified Time	Change Time	Access Time	Created Time
[current folder]			2004-08-21 02:44:23 IST	2004-08-21 02:44:23 IST	2004-08-21 02:45:52 IST	2004-08-21 02:45:52 IST
[parent folder]			2004-08-21 02:43:25 IST	2004-08-21 02:43:25 IST	2004-08-21 02:43:25 IST	2004-08-21 02:43:25 IST
alt.2600.cardz.dbx			2004-08-21 02:57:17 IST	2004-08-21 02:57:17 IST	2004-08-21 02:57:17 IST	2004-08-21 02:57:17 IST
alt.2600.codez.dbx			2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST
alt.2600.crackz.dbx			2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST
alt.2600.dbx			2004-08-21 02:57:23 IST	2004-08-21 02:57:23 IST	2004-08-21 02:57:23 IST	2004-08-21 02:57:23 IST
alt.2600.hackerz.dbx			2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST
alt.2600.moderated.dbx			2004-08-21 02:49:20 IST	2004-08-21 02:49:20 IST	2004-08-21 02:49:20 IST	2004-08-21 02:49:20 IST
alt.2600.phreakz.dbx			2004-08-21 02:57:10 IST	2004-08-21 02:57:10 IST	2004-08-21 02:57:10 IST	2004-08-21 02:57:10 IST
alt.2600.programz.dbx			2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST

Search Results for `alt.2600.cardz.dbx`:

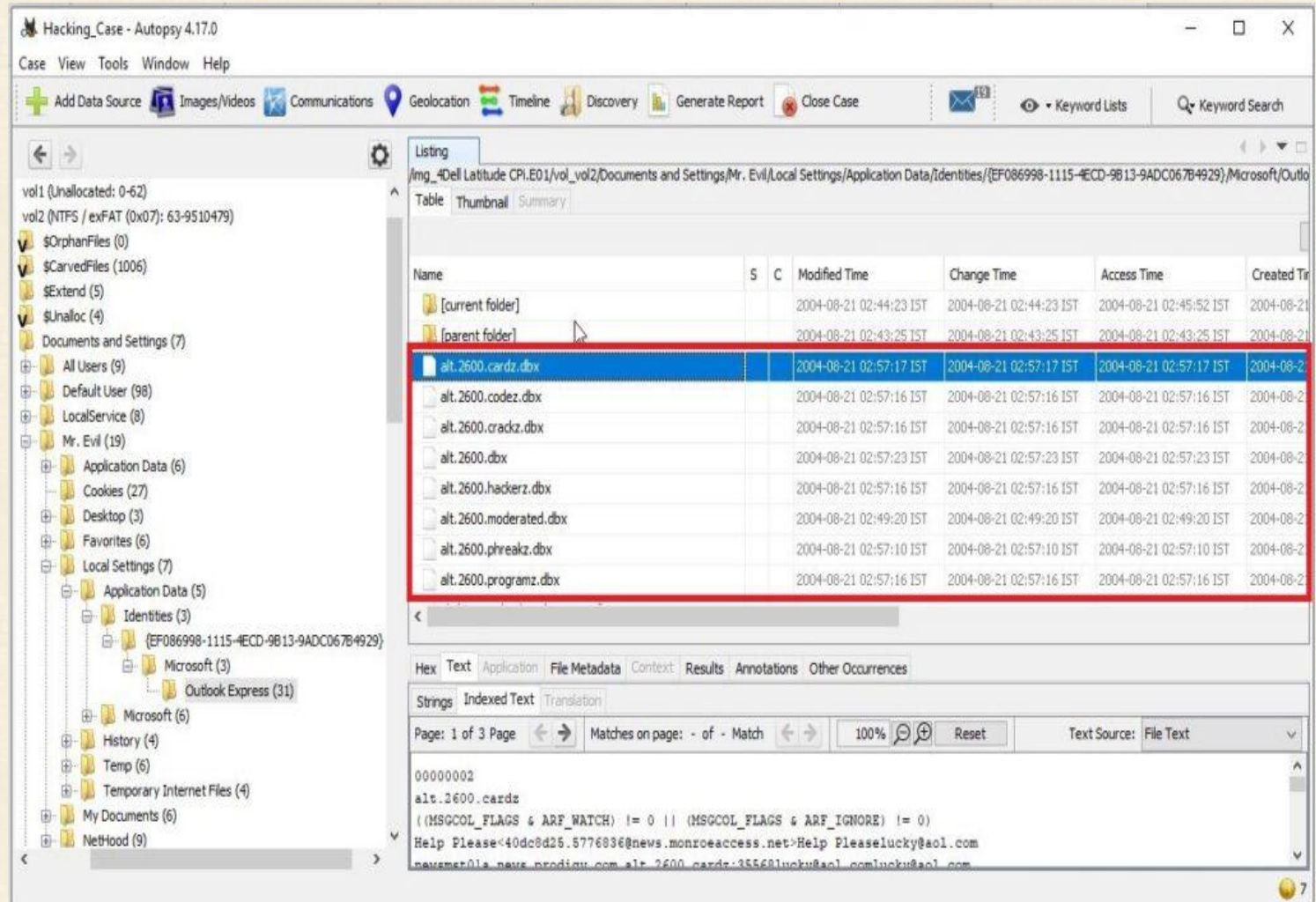
Page: 1 of 3 Page Matches on page: - of - Match 100% Reset Text Source: File Text

news.dallas.sbcglobal.net000000002

List 5 newsgroups that Mr. Evil has subscribed to? We can find this information in the same file as above.

User Mr. Evil subscribed to over 23 news groups :

1. Alt.2600.phreakz 2. Alt.2600 3. Alt.2600.cardz
4. Alt.2600codez 5. Alt.2600.crackz 6. Alt.2600.moderated
7. Alt.binaries.hacking.utilities
8. Alt.stupidity.hackers.malicious 9. Free.binaries.hackers.malicious
10. alt.nl.binaries.hack 11. Free.binaries.hacking.talentless.troll_haven
12. alt.hacking 13. free.binaries.hacking.beginner 14. alt.2600.programz
15. Free.binaries.hacking.talentless.troll-haven 16. alt.dss.hack
17. free.binaries.hacking.computers 18. free.binaries.hacking.utilities
19. alt.binaries.hacking.websites 20. alt.binaries.hacking.computers
21. alt.binaries.hacking.websites 22. alt.binaries.hacking.beginner
23. alt.2600.hackerz



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

We can find this information in the .ini file of the installed program mIRC. The path to this program is in "C:\Program Files\mIRC\mirc.ini"

The user settings that were shown when the user was online and in a chat channel are :

user = Mini Me
email = none@of.ya
nick = Mr
anick = mrevilrulez

The screenshot shows the Autopsy 4.17.0 interface. The left pane displays a file tree with 'Program Files' expanded, showing 'mIRC (16)'. The right pane shows a table of files in the directory 'C:\Program Files\mIRC'. The file 'mirc.ini' is selected, and its contents are displayed in the bottom pane, showing user settings.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size
aliases.ini			2004-08-20 20:39:56 IST	2004-08-25 21:50:34 IST	2004-08-25 21:50:34 IST	2004-08-20 20:39:56 IST	287
ircintro.hlp			2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	69423
mirc.exe			2004-08-20 20:39:55 IST	2004-08-27 20:44:45 IST	2004-08-25 21:50:27 IST	2004-08-20 20:39:55 IST	1867776
mirc.hlp			2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	224213
mirc.ini			2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST	2004-08-20 20:39:56 IST	5483
popups.ini			2004-08-20 20:39:56 IST	2004-08-25 21:50:34 IST	2004-08-25 21:50:34 IST	2004-08-20 20:39:56 IST	2568
readme.txt			2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	1104
servers.ini			2004-08-21 00:46:33 IST	2004-08-25 21:50:34 IST	2004-08-25 21:50:34 IST	2004-08-20 20:39:56 IST	31500
urls.ini			2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST	2004-08-20 20:39:56 IST	355
versions.txt			2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	22410

The contents of the selected file 'mirc.ini' are displayed in the bottom pane:

```

user=Mini Me
email=none@of.ya
nick=Mr
anick=mrevilrulez
server=losangeles.ca.us.undernet.org:6660GROUP:Undernet
  
```

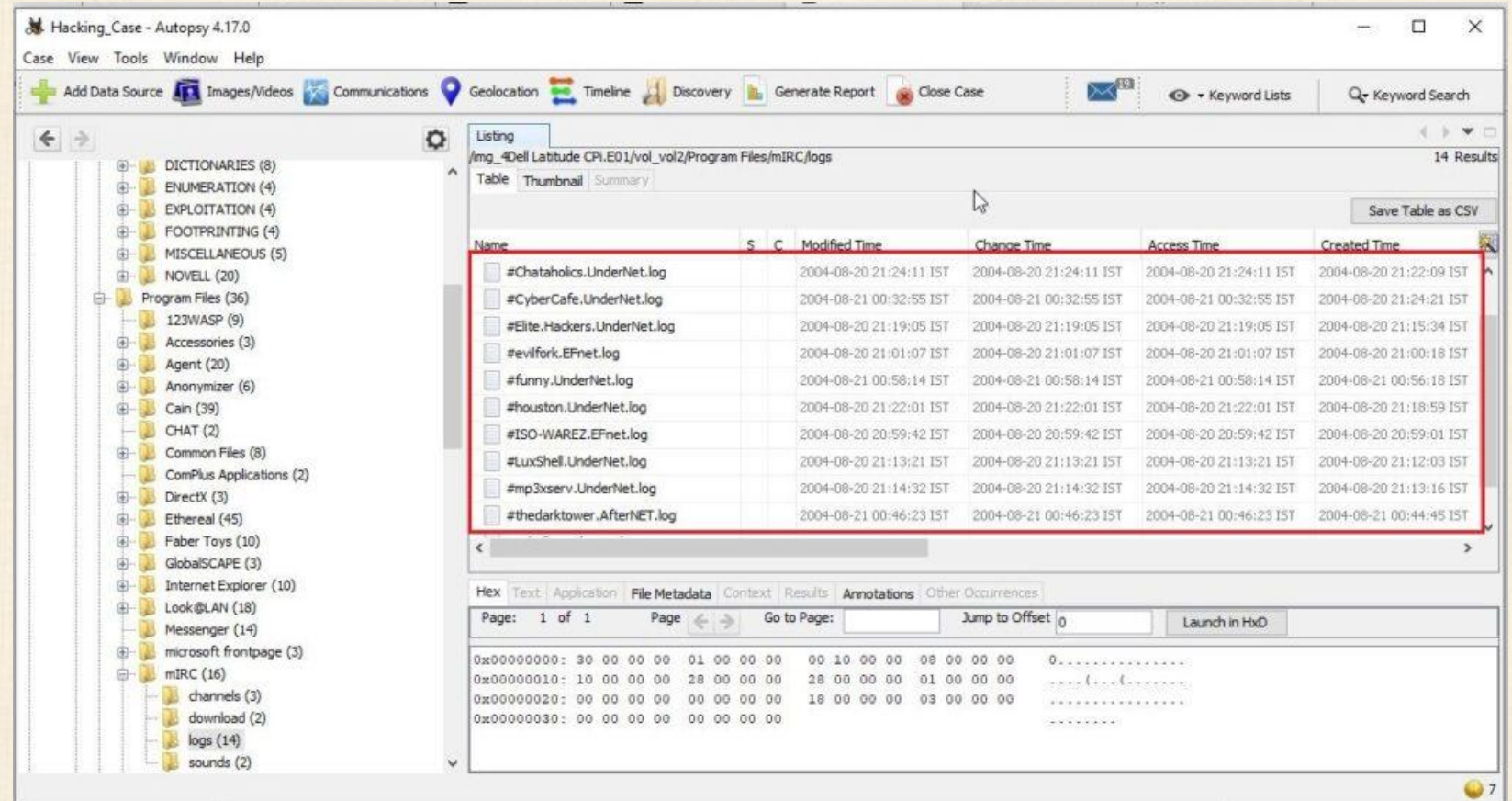
4.4 Go further with Autopsy

This IRC program has the capability to log chat sessions. What are IRC channels that the user of this computer accessed?

This information can be accessed from C:\Program Files\mIRC\logs file.

The IRC channels that this user accessed are :

Ushells.undernet.log
 Elite.hackers.undernet.log
 Mp3xserv.undernet.log
 Chataholics.undernet.log
 Cybercafé.undernet.log
 M5tar.undernet.log
 Thedarktower.afternet.log
 Funny.undernet.log
 Luxshell.undernet.log
 Evilfork.efnet.log
 Iso-warez.efnet.log
 Houston.undernet.log



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?

After going through the Documents folder, we found the file that contains the intercepted data. It’s name is “interception” which is a packet capture file.

The screenshot shows the Autopsy forensic tool interface. On the left, the 'Data Sources' tree is expanded to show the 'Documents and Settings' folder for 'Mr. Evil'. The 'interception' file is highlighted in the list. The main pane shows a table of files in the 'Documents and Settings/Mr. Evil' directory. The 'interception' file is selected, and its metadata is displayed at the bottom.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size
My Documents			2004-08-20 04:34:51 IST	2004-08-20 20:56:37 IST	2004-08-27 20:38:06 IST	2004-08-20 04:34:05 IST	56
Nethood			2004-08-26 20:38:15 IST	2004-08-26 20:38:15 IST	2004-08-26 20:38:15 IST	2004-08-20 04:34:05 IST	56
PrintHood			2004-08-19 22:30:09 IST	2004-08-20 04:34:06 IST	2004-08-26 20:37:44 IST	2004-08-20 04:34:05 IST	48
Recent			2004-08-26 20:38:14 IST	2004-08-26 20:38:14 IST	2004-08-27 20:44:40 IST	2004-08-20 04:34:05 IST	56
SendTo			2004-08-20 04:34:15 IST	2004-08-20 04:34:15 IST	2004-08-20 20:47:59 IST	2004-08-20 04:34:05 IST	56
Start Menu			2004-08-19 22:30:09 IST	2004-08-20 04:34:06 IST	2004-08-27 20:38:06 IST	2004-08-20 04:34:05 IST	256
Templates			2004-08-20 03:54:35 IST	2004-08-20 04:34:06 IST	2004-08-20 20:47:59 IST	2004-08-20 04:34:05 IST	56
interception			2004-08-27 21:11:00 IST	2004-08-27 21:11:00 IST	2004-08-27 21:11:00 IST	2004-08-27 21:11:00 IST	173372
			2004-08-27 21:16:23 IST	2004-08-27 21:16:13 IST	2004-08-27 21:16:23 IST	2004-08-20 04:34:05 IST	786432

The metadata for the 'interception' file is shown below:

Type	File System
MIME Type	applicat
Size	173372
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2004-08-27 21:11:00 IST

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) was using: Viewing the file “interception” in text format revealed that the victim was using Windows CE Pocket PC wireless computer.

The screenshot shows the Autopsy 4.17.0 interface. On the left, the file tree is expanded to 'Mr. Evil (19)' > 'Application Data (6)' > 'interception'. The main pane displays a table of files with columns 'Name', 'S', 'C', 'Modified Time', and 'Change'. The 'interception' file is selected. Below the table, the 'Text' tab is active, showing the contents of the intercepted file. A red box highlights the 'UA-OS: Windows CE (Pocket PC) - Version 4.20' line in the text. A red arrow points from this line in the interface to a larger, detailed view of the text on the right.

Listing
/img_4Dell Latitude CPl.E01/vol_vol2/Documents and Settings/Mr. Evil

Name	S	C	Modified Time	Change
PrintHood			2004-08-19 22:30:09 IST	2004-08-19 22:30:09 IST
Recent			2004-08-26 20:38:14 IST	2004-08-26 20:38:14 IST
SendTo			2004-08-20 04:34:15 IST	2004-08-20 04:34:15 IST
Start Menu			2004-08-19 22:30:09 IST	2004-08-19 22:30:09 IST
Templates			2004-08-20 03:54:35 IST	2004-08-20 03:54:35 IST
.gtk-bookmarks			2004-08-27 21:10:43 IST	2004-08-27 21:10:43 IST
interception			2004-08-27 21:11:00 IST	2004-08-27 21:11:00 IST
NTUSER.DAT			2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST
ntuser.dat.LOG			2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST
ntuser.ini			2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST

Text

Page: 1 of 5 Page

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=ACTI

VE&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*q6edOGfSSmKzi3lTlCIh6FdbNqQyPyqubrB97DYRuoTwoA5

lnliTd3eT73THi745LOSS.

4.4 Go further with Autopsy

What websites was the victim accessing?

Even this information can be obtained from the same file “interception”. We found two websites the victim was accessing, **Mobile.msn.com** and **MSN Hotmail Email**.

```
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=ACTI
VE&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*q6edOGfSSmKzi3lTlCIh6FdbNqQyPyqubrB97DYRuoTwoA5
kn1iTd3eT73THi745LOSS.
```

How many executable files are in the recycle bin?

The screenshot shows the Autopsy 4.17.0 interface. In the left sidebar, the 'RECYCLER (3)' folder is selected and highlighted with a red box. The main pane displays a listing of files in the RECYCLER folder, also highlighted with a red box. The files are Dc1.exe, Dc2.exe, Dc3.exe, and Dc4.exe. The table below shows the details of these files.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]			2004-08-27 20:59:58 IST	2004-08-27 20:59:58 IST	2004-08-27 20:59:58 IST	2004-08-25 21:48:25 IST	56
[parent folder]			2004-08-25 21:48:25 IST	2004-08-25 21:48:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:48:25 IST	328
Dc1.exe			2004-08-25 21:21:23 IST	2004-08-25 21:48:25 IST	2004-08-25 21:26:08 IST	2004-08-25 21:21:24 IST	2160043
Dc2.exe			2004-08-27 20:41:07 IST	2004-08-27 20:42:30 IST	2004-08-27 20:42:18 IST	2004-08-27 20:41:07 IST	1324940
Dc3.exe			2004-08-27 20:44:20 IST	2004-08-27 20:45:26 IST	2004-08-27 20:45:16 IST	2004-08-27 20:44:20 IST	442417
Dc4.exe			2004-08-27 20:54:24 IST	2004-08-27 20:59:58 IST	2004-08-27 20:59:47 IST	2004-08-27 20:54:24 IST	8460502
			2004-08-25 21:48:25 IST	2004-08-25 21:48:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:48:25 IST	65
			2004-08-27 21:16:17 IST	2004-08-27 21:16:17 IST	2004-08-27 21:16:17 IST	2004-08-25 21:48:25 IST	3220

4.4 Go further with Autopsy

How many files are actually reported to be deleted by the file system?

This information can be found out from the INFO2 file.

The screenshot shows the Autopsy 4.17.0 interface. On the left, the file tree shows the 'INFO2' file selected under the 'vol3 (Unallocated: 9510480-9514259)' volume. The main pane displays a table of files with columns: Name, S, C, Modified Time, Change Time, Access Time, Created Time, and Size. The 'INFO2' file is highlighted. Below the table, the 'Text' tab is active, showing the contents of the INFO2 file. The text is a list of file paths, with 'Evil\Desktop\netstumblerinstaller_0_4_0.exe' and 'Evil\Desktop\netstumblerinstaller_0_4_0.exe' highlighted by a red box.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]			2004-08-27 20:59:58 IST	2004-08-27 20:59:58 IST	2004-08-27 20:59:58 IST	2004-08-25 21:48:25 IST	56
[parent folder]			2004-08-25 21:48:25 IST	2004-08-25 21:48:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:48:25 IST	328
Dc1.exe			2004-08-25 21:21:23 IST	2004-08-25 21:48:25 IST	2004-08-25 21:26:08 IST	2004-08-25 21:21:24 IST	2160043
Dc2.exe			2004-08-27 20:41:07 IST	2004-08-27 20:42:30 IST	2004-08-27 20:42:18 IST	2004-08-27 20:41:07 IST	1324940
Dc3.exe			2004-08-27 20:44:20 IST	2004-08-27 20:45:26 IST	2004-08-27 20:45:16 IST	2004-08-27 20:44:20 IST	442417
Dc4.exe			2004-08-27 20:54:24 IST	2004-08-27 20:59:58 IST	2004-08-27 20:59:47 IST	2004-08-27 20:54:24 IST	8460502
desktop.ini			2004-08-25 21:48:25 IST	2004-08-25 21:48:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:48:25 IST	65
INFO2			2004-08-27 21:16:17 IST	2004-08-27 21:16:17 IST	2004-08-27 21:16:17 IST	2004-08-25 21:48:25 IST	3220

Text View Content:

```

C:\Documents and Settings\Mr. Evil\Desktop\netstumblerinstaller_0_4_0.exe
C:\Documents and Settings\Mr. Evil\Desktop\netstumblerinstaller_0_4_0.exe
C:\Documents and Settings\Mr. Evil\Desktop\netstumblerinstaller_0_4_0.exe
C:\Documents and Settings\Mr. Evil\Desktop\netstumblerinstaller_0_4_0.exe
C:\Documents and Settings\Mr. Evil\Desktop\netstumblerinstaller_0_4_0.exe

```


4.5 Case Study conclusion

On being asked to find out any evidence that this laptop was used for hacking, we found in our **forensic investigation** that this laptop belonged to **Greg Schardt** who also has a online persona **“Mr. Evil”**. We found his operating system as **Windows XP** and he was running **Ethereal**, a packet interception program to capture network traffic. Apart from Ethereal, his system **had six other programs** which were used for **hacking**. He was active among many **hacking related IRC** channels and **news groups**. Binding this evidence with what his **associates** said about him, we can come to a conclusion that this laptop belonged to Greg Schardt and he was involved in **hacking activities**. This case can be closed now.