

---

# **Digital Forensics and Investigation: NIST Hacking Case Solution**

---

*Solved By:*

Khubab Ahmed and Muhammad Saim

## Abstract

This digital forensics and investigation report delves into a hacking case involving a Dell Latitude CPi system owned by Greg Schardt. The investigation encompasses two primary tasks: Chain of Custody and Evidence Preservation, and Evidence Identification, Organization, Analysis, and Findings.

In Task 1, the report discusses the critical importance of maintaining the chain of custody and preserving evidence integrity throughout the investigation process. It highlights the use of tools like FTK Imager, Autopsy, and Registry Viewer to create image copies, validate images, and ensure evidence preservation.

Task 2 focuses on identifying, organizing, analyzing, and presenting key evidence related to the hacking case. This includes examining image hashes, operating system details, network configurations, user accounts, malicious programs, email communications, web activities, and deleted files.

The investigation uncovers significant findings such as the identification of malicious programs like Ethereal, Look@LAN, and Cain, email addresses associated with illicit activities, subscribed newsgroups indicating malicious intent, and executable files found in the recycle bin.

The report concludes by summarizing the findings from the system conclude it on that Greg Schardt is guilty on the basis of involving in Hacking activities.

## I. INTRODUCTION

The purpose of this project is to conduct a comprehensive digital forensics investigation on a Dell CPi notebook computer, suspected of being used for hacking. The investigation aims to uncover evidence of hacking software, their usage, and any data that might link the computer to the suspect, Greg Schardt, also known as "Mr. Evil". This report details the steps taken, the tools used, and the findings from the forensic analysis.

## II. CHAIN OF CUSTODY, VALIDATION AND EVIDENCE PRESERVATION

### A. Chain of Custody

The first people in this chain of custody are the people who collected the machine/system from the crime scene. Those investigators created an image so that the original machine doesn't go through any irreversible change (Jones, 2019). This image is further used by different investigators.

After that, the person to receive the image would be me in this case making me the second person to interact with this image/machine. The examination/work performed by me on the image is present down below but firstly we confirm that the image wasn't tampered during its movement from Acquisition person to me.

In this case, the acquisition details are missing. So we cannot maintain its chain of custody and did not validate that the image is correct or not.

### B. Image Validation

Image validation is the most important thing before starting any analysis. It ensures the integrity that image and that it isn't altered during movement and stay (Chen, 2017). In this case, we have not given any acquisition hash. So we cannot validate the image.

**Given Hash:** Not Provided

**Autopsy Calculated Hash (MD5):** aee4fcd9301c03b3b054623ca261959a

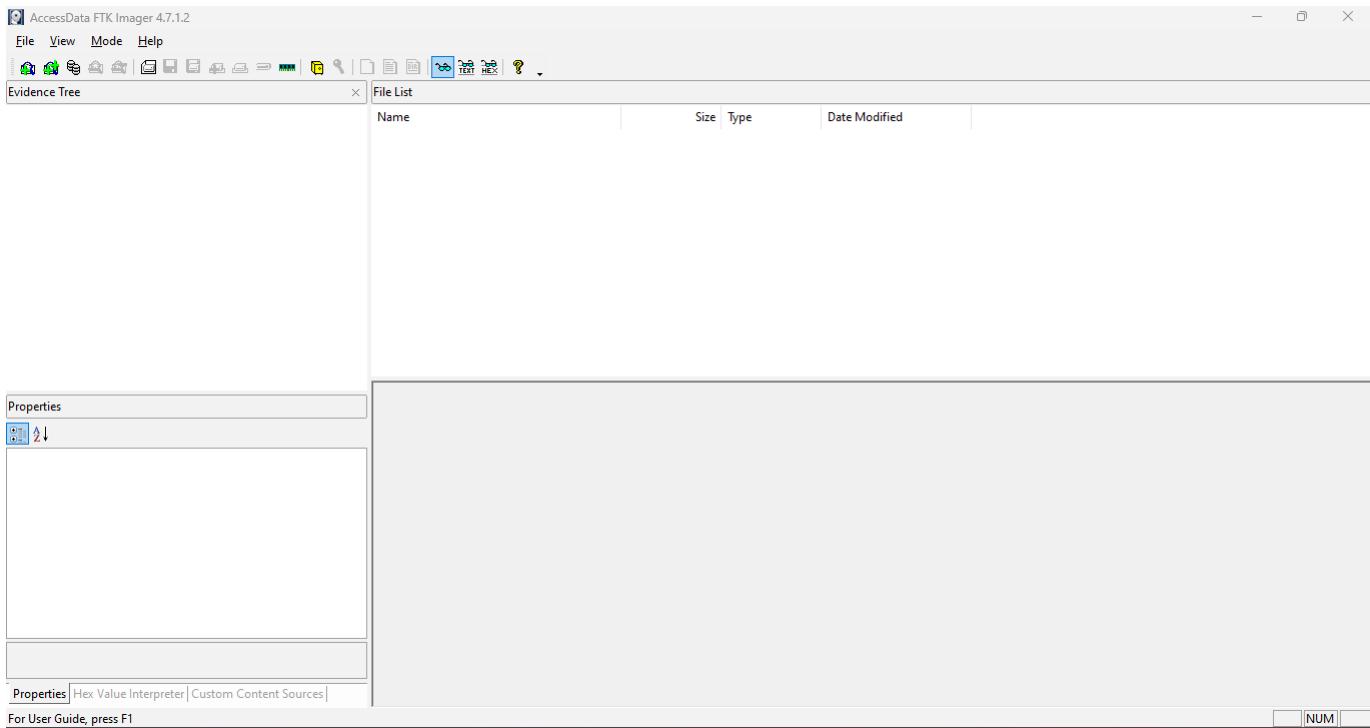
### C. Preserving Evidence

To preserve the evidence, I make a copy of the image. Match the hash. Then I worked with the copy image. This is done as sometimes we or tools can cause irreversible damage to the image, hence changing the image (Adams, 2018). This is also the reason that an image of the system was made instead of working on the physical machine. All work moving forward is done on the copy image.

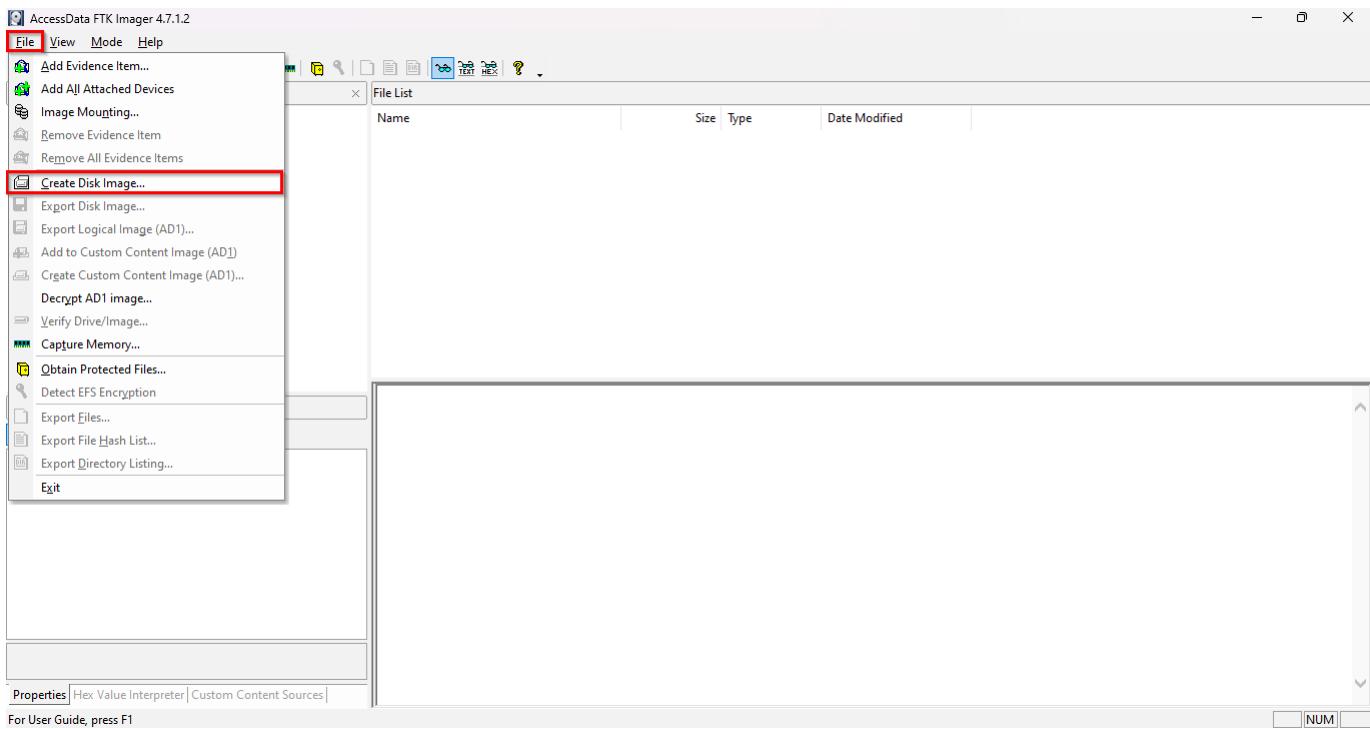
### D. Method to Preserve Evidence

To preserve the evidence, I used FTK imager tool to make a copy of the original image file.

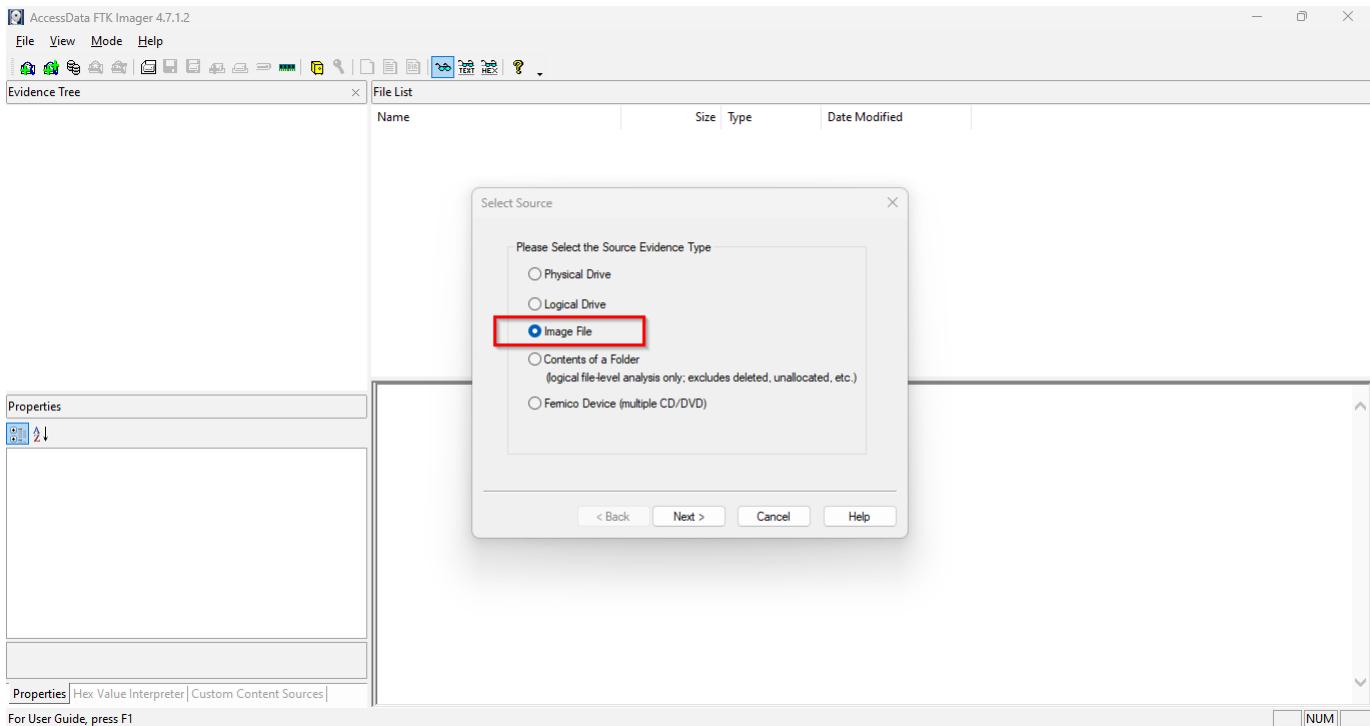
- Open FTK Imager tool.



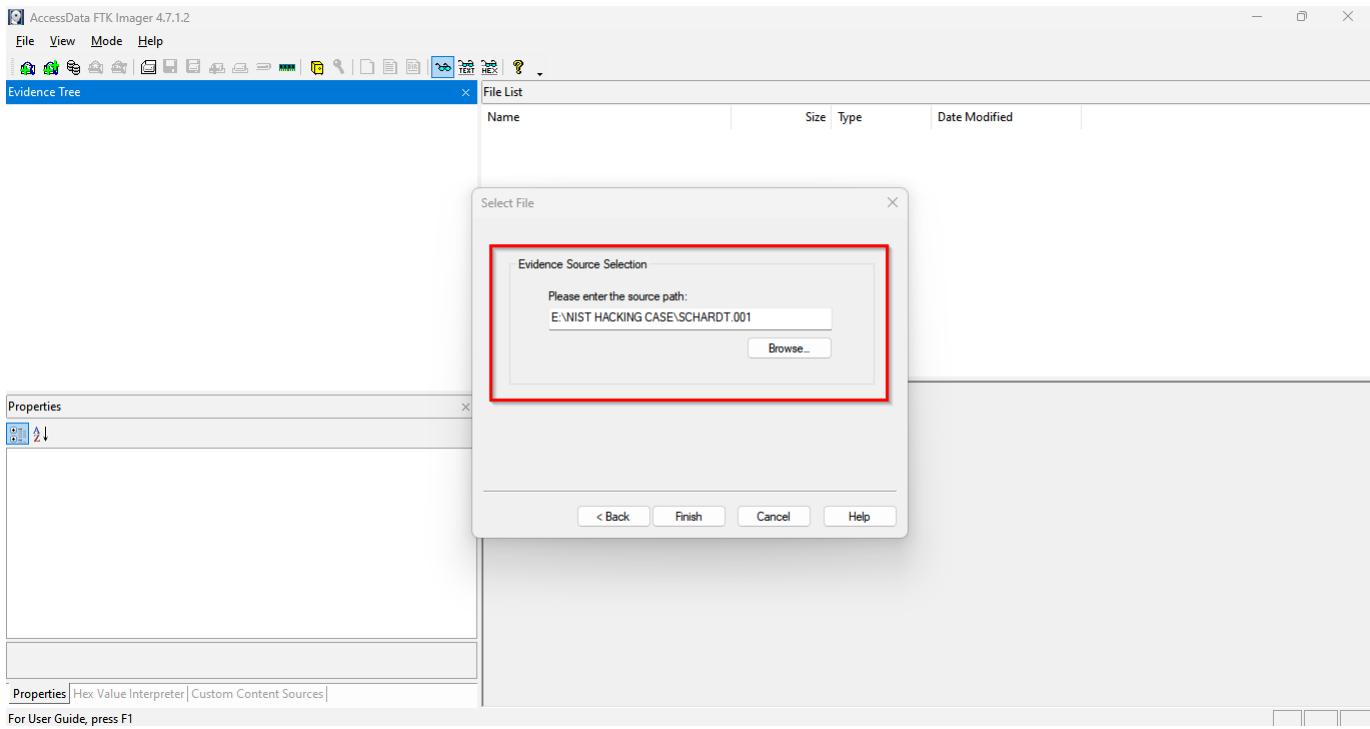
- Go to File — Create Disk Image:



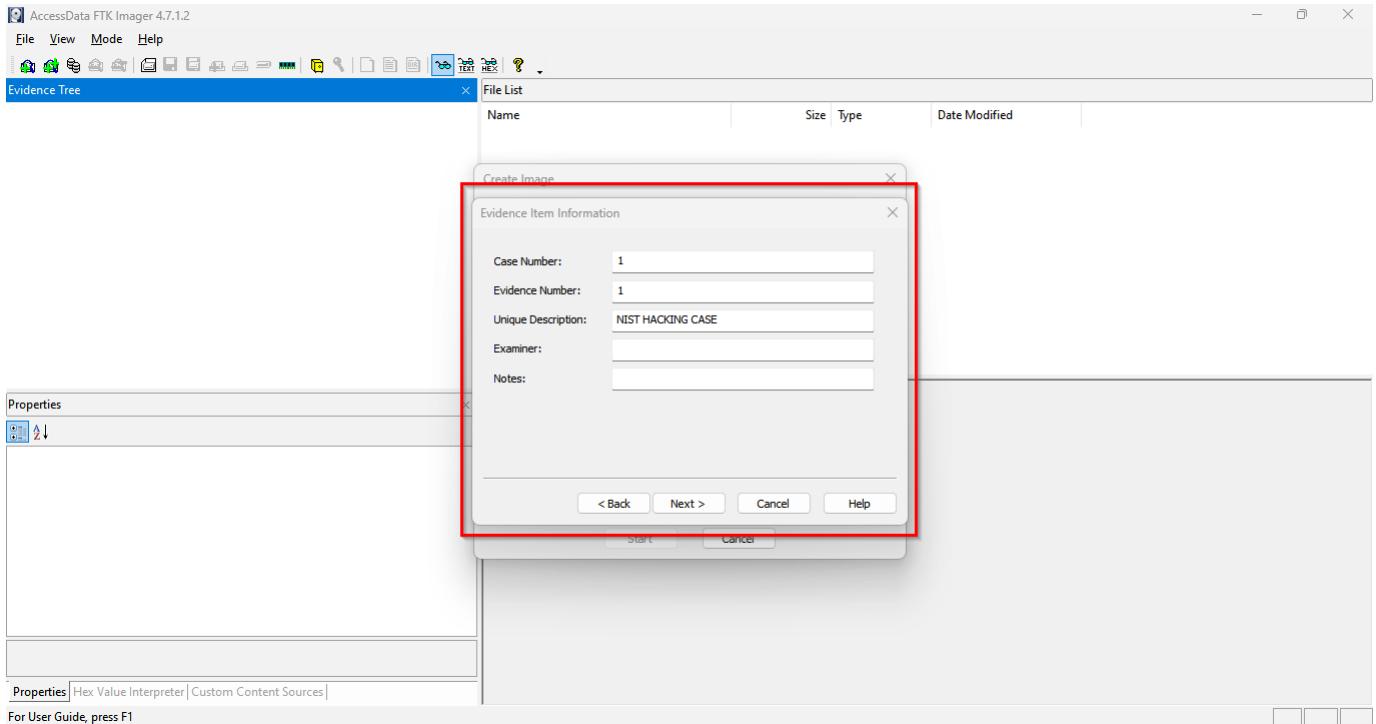
- Select Image File option.



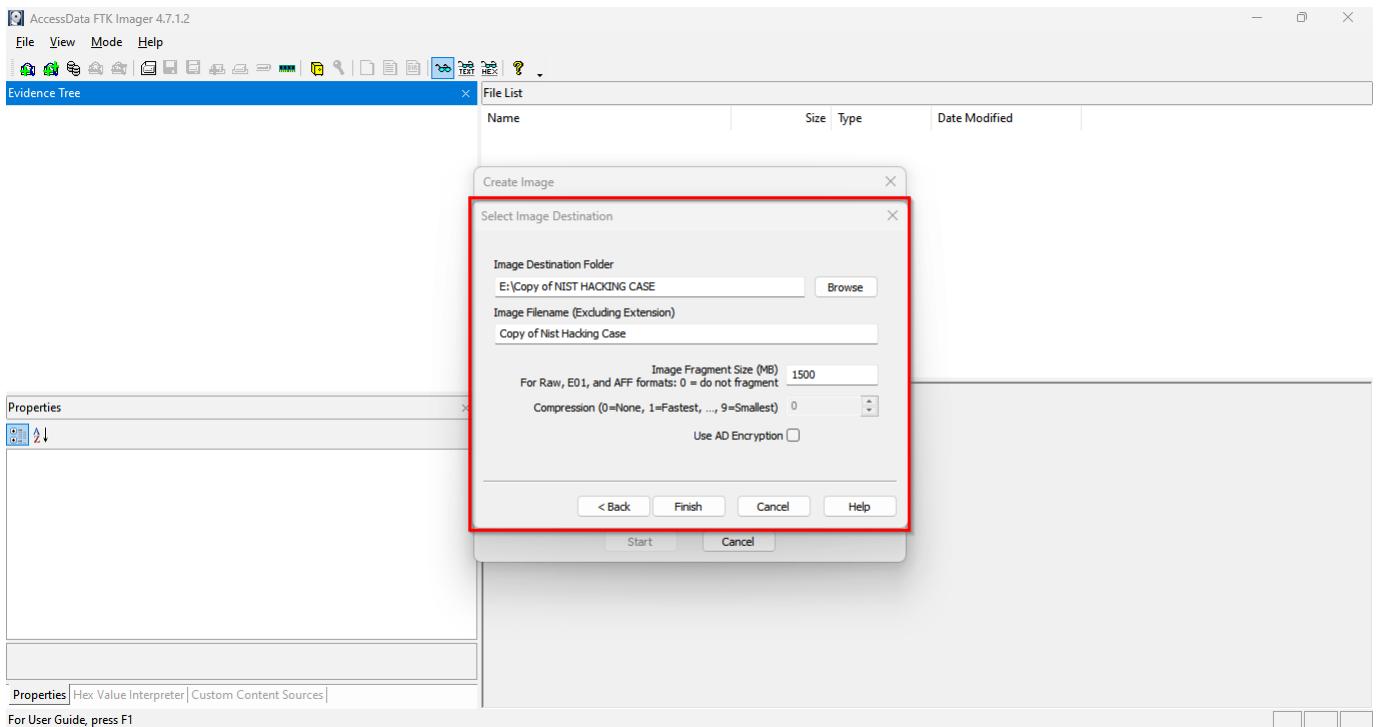
- Add the original image file.



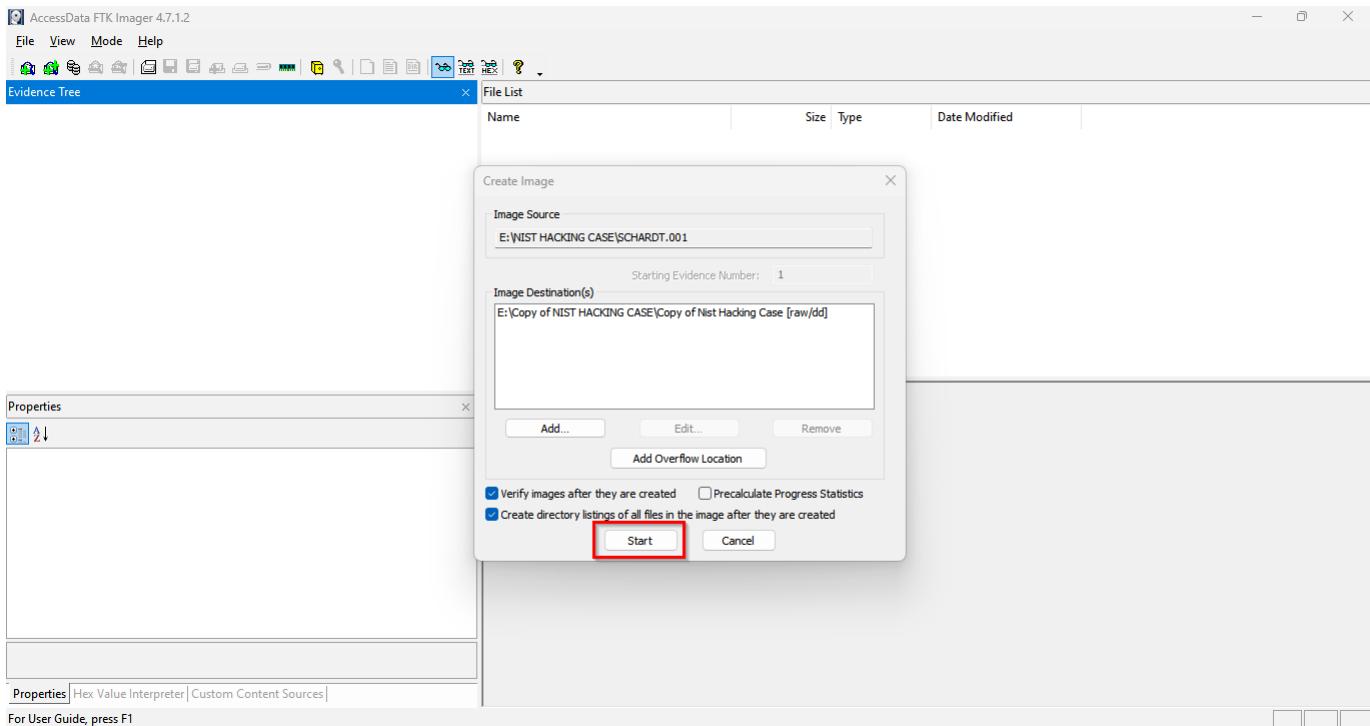
- Add the important necessary information.



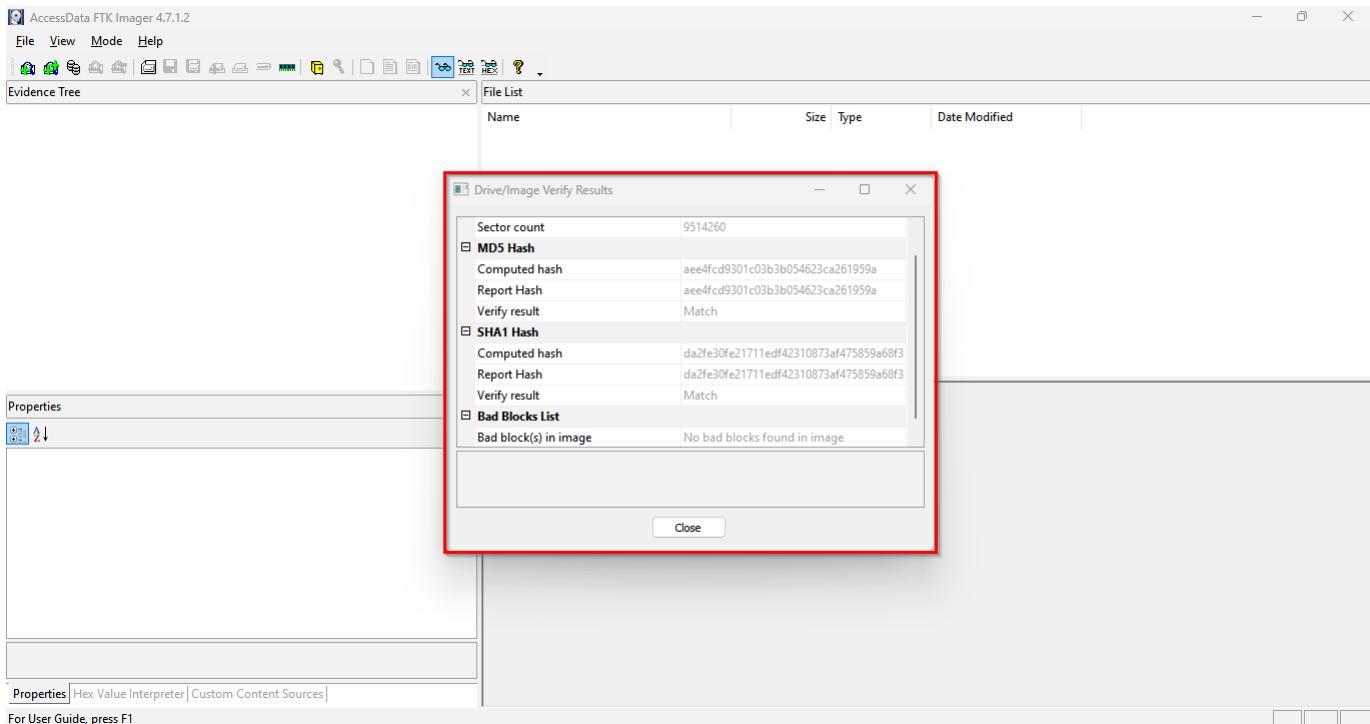
- Add image destination file.



- Start copying the image.



- Copying of the image hash file is done.



#### E. Verifying the Evidence

To verify the images, we compared both MD5 hashes of original image hash and copying image hash. Both images are the same.

**Original Image Hash:** ae4fcfd9301c03b3b054623ca261959a

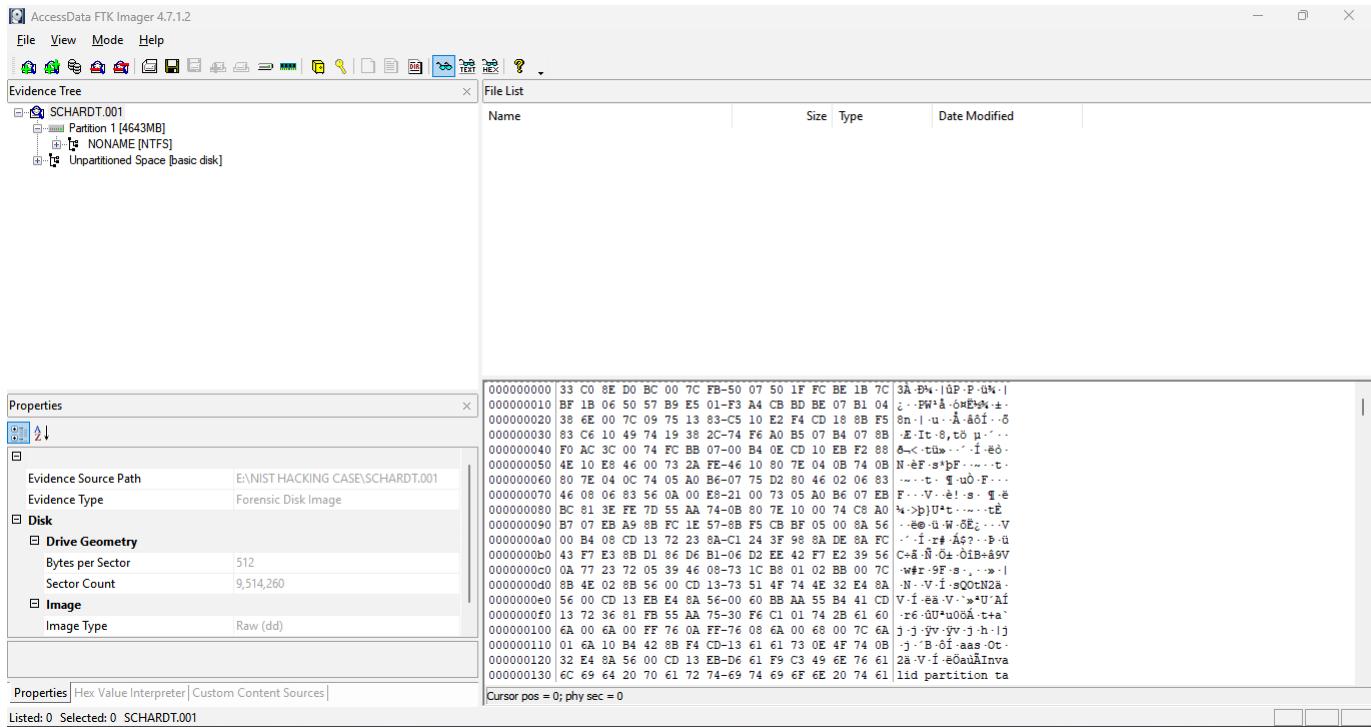
**Copying Image hash:** ae4fcfd9301c03b3b054623ca261959a

### III. TOOLS USED

The tools used are FTK imager, autopsy and registry viewer.

#### A. FTK imager

FTK Imager is a powerful tool for digital forensic investigations. It offers a wide range of tools and features to acquire, analyze, and report on digital evidence. Its capabilities make it an essential tool for law enforcement agencies, cybersecurity professionals, and forensic examiners (AccessData, 2023).



#### B. Autopsy

Autopsy is a comprehensive digital forensic tool that offers a wide range of features for acquiring, analyzing, and reporting on digital evidence. Its user-friendly interface and extensibility make it a popular choice among forensic examiners and investigators (SleuthKit, 2020).

The screenshot shows the 'Data Sources' tree on the left, with 'SCHARDT.001' selected. The main pane displays the details for 'SCHARDT.001' host, including its display name, name, device ID, and time zone. It also shows acquisition details, image type, size, unallocated space, sector size, and MD5, SHA1, SHA256 hashes. The 'File Paths' section lists the paths for each volume: E:\NIST HACKING CASE\SCHARDT.001, E:\NIST HACKING CASE\SCHARDT.002, E:\NIST HACKING CASE\SCHARDT.003, E:\NIST HACKING CASE\SCHARDT.004, E:\NIST HACKING CASE\SCHARDT.005, E:\NIST HACKING CASE\SCHARDT.006, and E:\NIST HACKING CASE\SCHARDT.007. The bottom navigation bar includes links for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

### C. Registry viewer

A registry viewer is a versatile tool that provides insights into the configuration and behavior of Windows systems, making it invaluable for system administrators, digital forensic analysts, and security professionals (Harlan, 2018).

The screenshot shows the AccessData Registry Viewer interface. The left pane displays a tree view of registry keys under 'SAM\Domains\Account\Users'. The 'Mr. Evil' key is selected. The right pane shows a table of registry values for this key. The bottom pane shows the raw binary data of the selected value.

Name	Type	Data
000001F4	REG_BINARY	02 00 01 00 00 00 00 00 A0 73 46 B2 47 8C C4 01 00 ...
000001F5	REG_BINARY	00 00 00 BC 00 00 02 00 01 00 BC 00 00 00 10 00 ...

**Key Properties**

Last Written Time	27/08/2004 15:08:23 UTC
RID unique identifier	1003
User Name	Mr. Evil
Logon Count	15
Last Logon Time	27/08/2004 15:08:23 UTC
Last Password Change Time	19/08/2004 23:03:54 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	false
Password Required	«need "SysKey" file»
Country Code	0 (System Default)
NTHash	«need "SysKey" file»
LMHash	«need "SysKey" file»

SAM\Domains\Account\Users\000003EB

Offset: 0

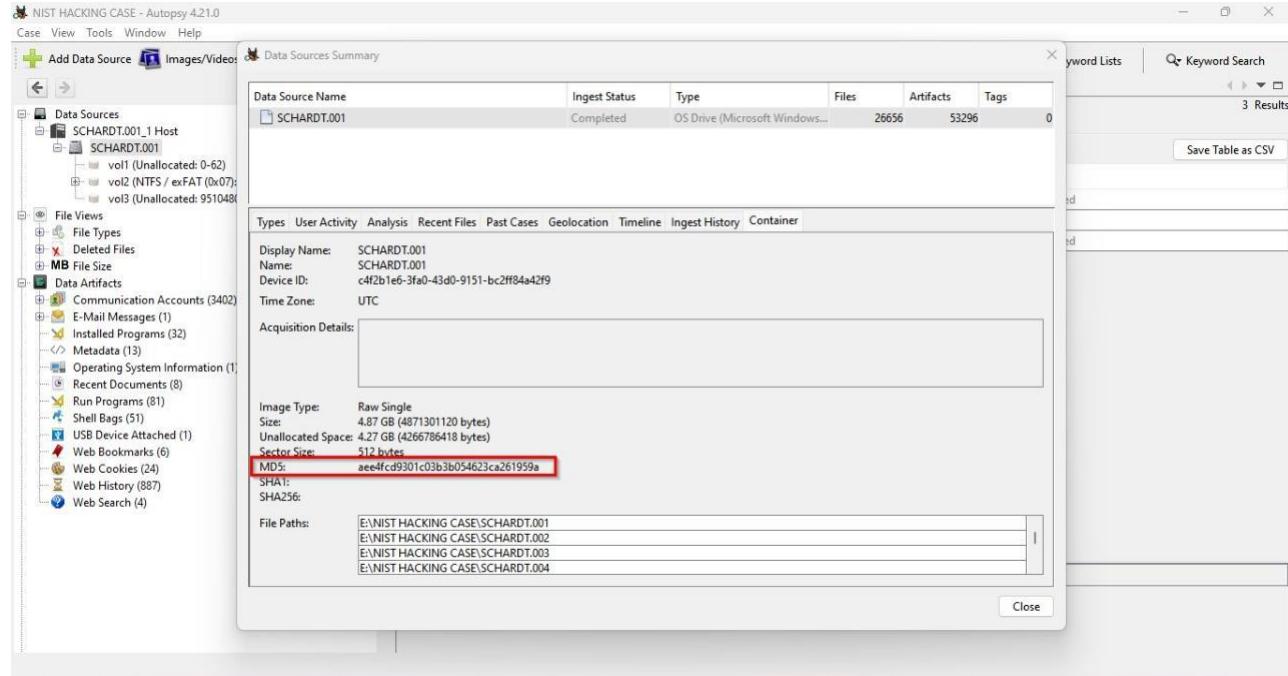
#### IV. EVIDENCE IDENTIFICATION, ANALYSIS, AND FINDINGS

##### Q1. Image Hash

**MD5:** aee4fc9301c03b3b054623ca261959a

Checking the image hash as its requirement for digital investigators to make sure the image is not altered or changed during the chain of custody. It's very important because a single change to data would make an innocent, guilty and guilty, innocent leading to many issues.

**Method:** Click on Data source - Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Right Click to View Summary Information – Container tab



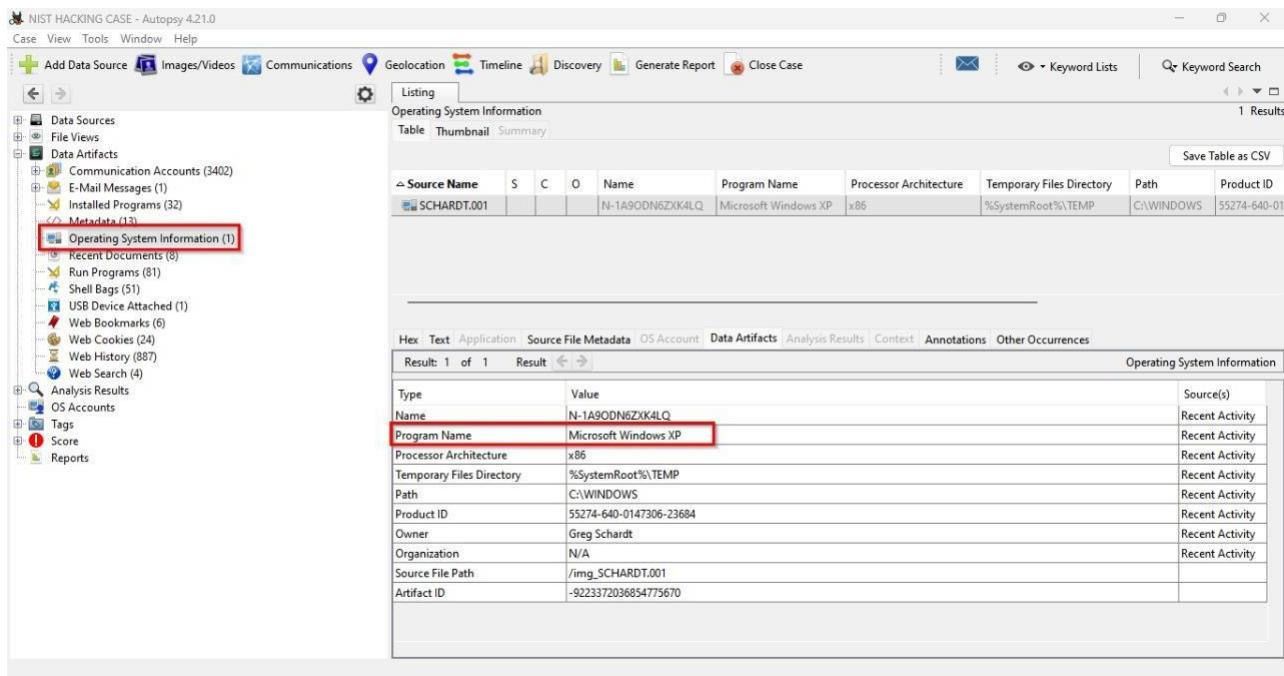
## Q2. Operating System

### Operating System: Microsoft Windows XP

Knowledge of the OS allows investigators to identify known vulnerabilities associated with that OS. This information helps in assessing potential attack vectors and understanding how the system may have been compromised.

The OS information provides insights into the file system, registry structure, user accounts, installed software, and system configurations. This data is essential for conducting forensic analysis, identifying artifacts, and reconstructing events leading to a security incident.

### Method: Click on Data Artifacts – Operating System Information



The screenshot shows the Autopsy 4.21.0 interface. The left sidebar shows a tree view of data sources, with 'Data Artifacts' expanded. Under 'Data Artifacts', 'Operating System Information (1)' is selected and highlighted with a red box. The main pane shows a table titled 'Operating System Information' with one row. The table has columns: Source Name, S, C, O, Name, Program Name, Processor Architecture, Temporary Files Directory, Path, and Product ID. The row data is: SCHRADT.001, S, C, O, N-1A90DN6ZXK4LQ, Microsoft Windows XP, x86, %SystemRoot%\TEMP, C:\WINDOWS, 55274-640-01. Below the table is a details pane titled 'Operating System Information' with a table of system properties. The 'Program Name' row is also highlighted with a red box. The details table has columns: Type, Value, and Source(s). The rows are: Name (N-1A90DN6ZXK4LQ), Program Name (Microsoft Windows XP), Processor Architecture (x86), Temporary Files Directory (%SystemRoot%\TEMP), Path (C:\WINDOWS), Product ID (55274-640-0147306-23684), Owner (Greg Schardt), Organization (N/A), Source File Path (/img\_SCHRADT.001), and Artifact ID (-9223372036854775670).

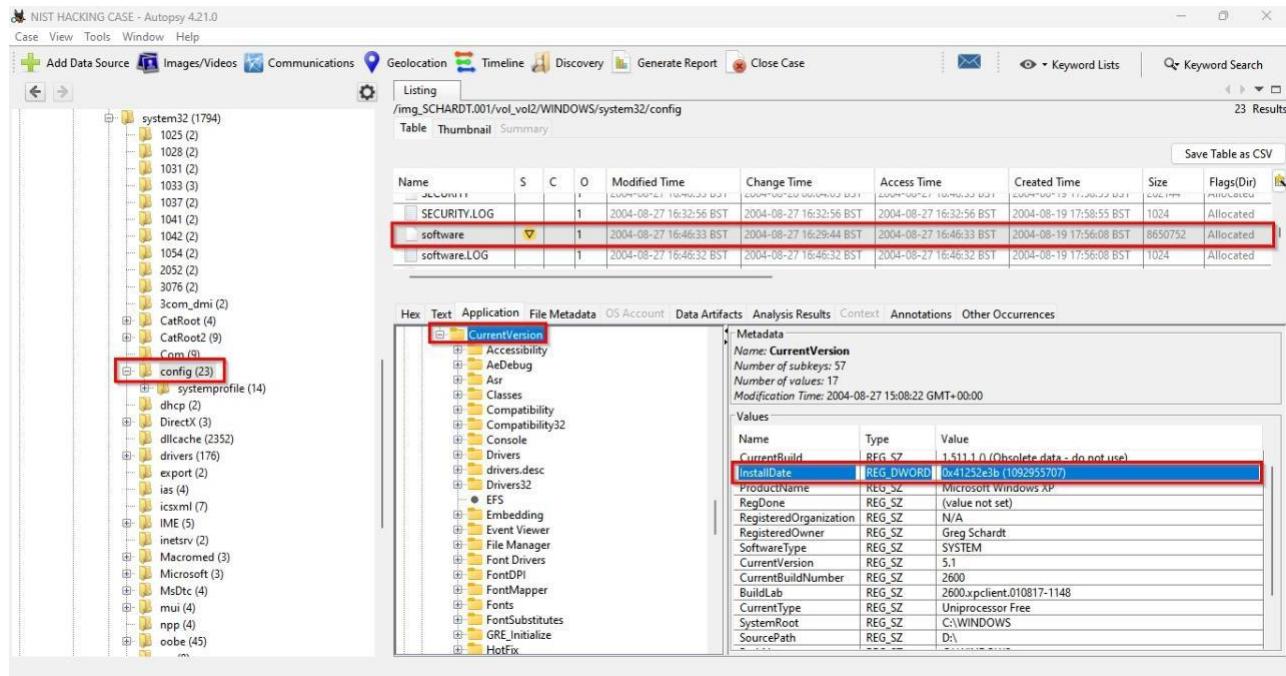
Type	Value	Source(s)
Name	N-1A90DN6ZXK4LQ	Recent Activity
Program Name	Microsoft Windows XP	Recent Activity
Processor Architecture	x86	Recent Activity
Temporary Files Directory	%SystemRoot%\TEMP	Recent Activity
Path	C:\WINDOWS	Recent Activity
Product ID	55274-640-0147306-23684	Recent Activity
Owner	Greg Schardt	Recent Activity
Organization	N/A	Recent Activity
Source File Path	/img_SCHRADT.001	
Artifact ID	-9223372036854775670	

### Q3. Operating System Install Date

#### Install Date in Registry: 0x41252e3b (1092955707)

Knowing the installation date of the OS helps establish a timeline of events related to the system. It provides a starting point for investigating when the system was initially set up and potentially compromised.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – WINDOWS – system32 – config – software – Microsoft – Windows NT – CurrentVersion

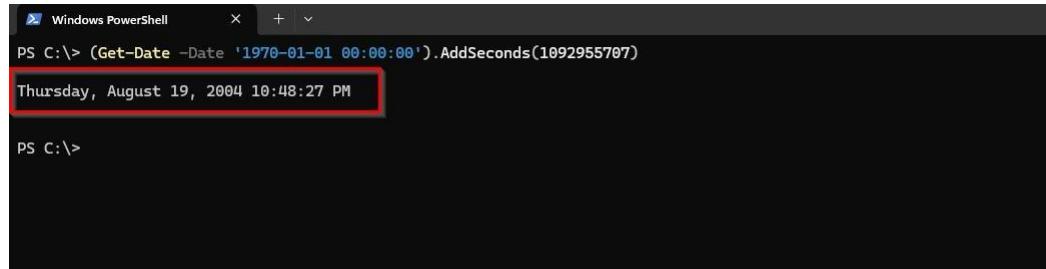


The screenshot shows the Autopsy 4.21.0 interface. The 'Data Source' tab is selected, and the 'Windows' host is chosen. The 'File System' tab is open, showing a tree view of the file system. The 'registry' section is expanded, and the 'CurrentVersion' key is selected. The 'Values' table shows a single entry for 'InstallDate' with a value of '0x41252e3b (1092955707)'. This value is highlighted with a red box.

Name	Type	Value
InstallDate	REG_DWORD	0x41252e3b (1092955707)

After converting it into UTC Standard.

**Install Date:** Thursday, August 19, 2004 10:48:27 PM



```
PS C:\> (Get-Date -Date '1970-01-01 00:00:00').AddSeconds(1092955707)
Thursday, August 19, 2004 10:48:27 PM
```

#### Q4. System Time Zone Settings

##### Time Zone: Central Standard Time (CST)

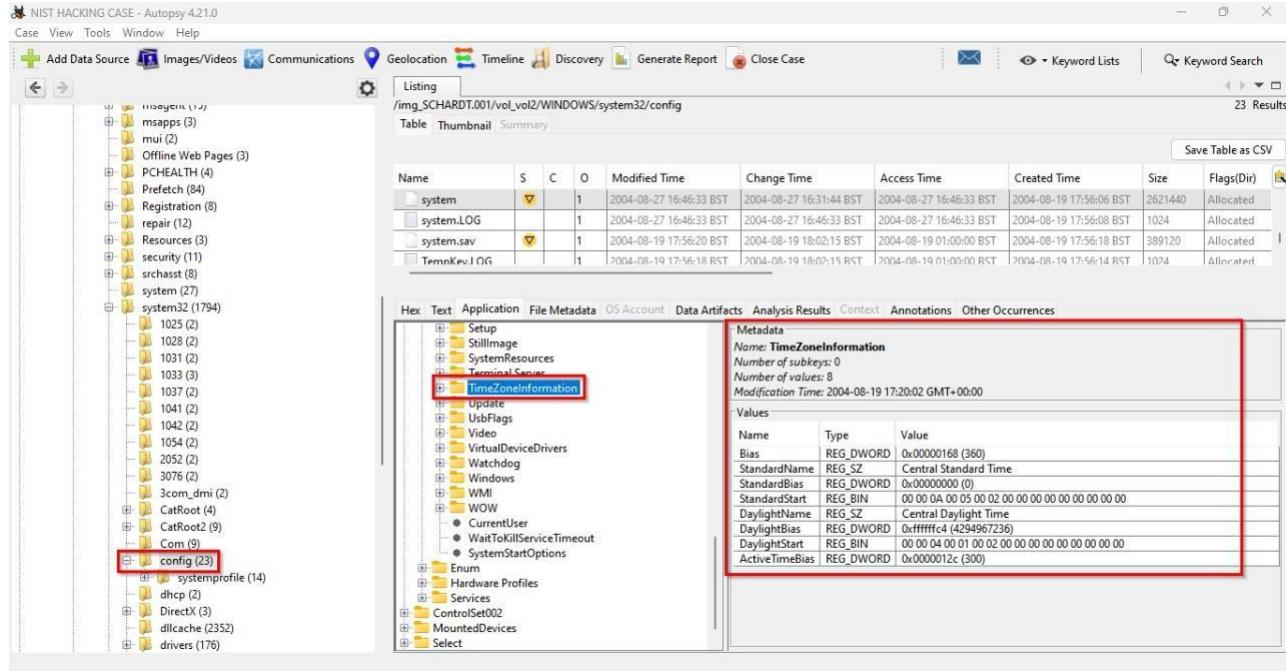
Time Zone tells the geographic location of the system where it was active.

##### Time Zone: Central Standard Time

Daylight Name: Central Daylight Time

Daylight Bias: -60

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – WINDOWS – system32 – config – system – ControlSet001 – Control – TimeZoneInformation



The screenshot shows the Autopsy 4.21.0 interface. The left pane displays a file tree with various folders and files, including 'msapps', 'mui', 'Offline Web Pages', 'PCHEALTH', 'Prefetch', 'Registration', 'repair', 'Resources', 'security', 'srchasst', 'system', and 'system32'. The 'config' folder under 'system32' is highlighted with a red box. The right pane shows a table of files in the 'system32/config' directory, with a red box highlighting the 'TimeZoneInformation' key. The details pane shows the following information for the 'TimeZoneInformation' key:

**Metadata**

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

**Values**

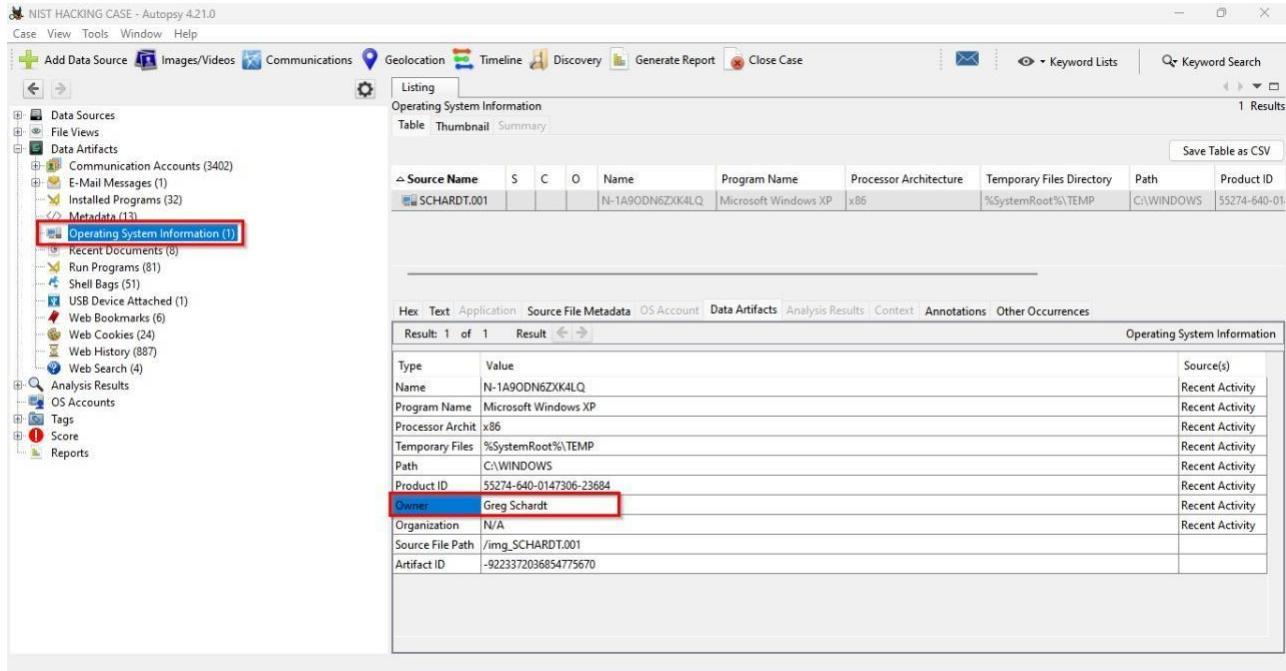
Name	Type	Value
Bias	REG_DWORD	0x00000168 (360)
StandardName	REG_SZ	Central Standard Time
StandardBias	REG_DWORD	0x00000000 (0)
StandardStart	REG_BIN	00 00 0A 00 05 00 02 00 00 00 00 00 00 00 00 00
DaylightName	REG_SZ	Central Daylight Time
DaylightBias	REG_DWORD	0xfffffc4 (4294967236)
DaylightStart	REG_BIN	00 00 04 00 01 00 02 00 00 00 00 00 00 00 00 00
ActiveTimeBias	REG_DWORD	0x0000012c (300)

## Q5. Operating System Registered Owner

**Owner:** Greg Schardt

Owner names can help identify the individual responsible for the system. This would serve as important documentation for a digital investigator. Furthermore, we can see the access each user has been provided by the owner.

**Method:** Click on results – Data Artifacts – Operating System Information



The screenshot shows the Autopsy 4.21.0 interface with the following details:

- Left Panel:** Shows a tree view of data sources, with "Operating System Information (1)" selected and highlighted with a red box.
- Top Bar:** Includes "Case", "View", "Tools", "Window", "Help" menus, and "Add Data Source", "Images/Videos", "Communications", "Geolocation", "Timeline", "Discovery", "Generate Report", "Close Case" buttons.
- Central Area:**
  - Operating System Information:** A table showing 1 result. The table has columns: Source Name, S, C, O, Name, Program Name, Processor Architecture, Temporary Files Directory, Path, and Product ID.
  - Table Data:**

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID
SCHARDT.001				N-1A90DN6ZXK4LQ	Microsoft Windows XP	x86	%SystemRoot%\TEMP	C:\WINDOWS	55274-640-01
  - Bottom Tab Bar:** Hex, Text, Application, Source File Metadata, OS Account, Data Artifacts (selected), Analysis Results, Context, Annotations, Other Occurrences.
  - Operating System Information Table:** A detailed table showing system configuration. The "Owner" row is highlighted with a red box.
  - Table Data (Operating System Information):**

Type	Value	Source(s)
Name	N-1A90DN6ZXK4LQ	Recent Activity
Program Name	Microsoft Windows XP	Recent Activity
Processor Archit	x86	Recent Activity
Temporary Files	%SystemRoot%\TEMP	Recent Activity
Path	C:\WINDOWS	Recent Activity
Product ID	55274-640-0147306-23684	Recent Activity
Owner	Greg Schardt	Recent Activity
Organization	N/A	Recent Activity
Source File Path	/img_SCHARDT.001	
Artifact ID	-9223372036854775670	

#### Q6. Computer Account Name

**Account Name:** N-1A90DN6ZXK4LQ

The computer account name serves as a fundamental identifier for network devices, facilitating management, security, and accountability within the network environment hence serves as a unique identifier in a network.

**Method:** Click on results – Data Artifacts – Operating System Information

Type	Value	Source(s)
Name	N-1A90DN6ZXK4LQ	Recent Activity
Program Name	Microsoft Windows XP	Recent Activity
Processor Archit	x86	Recent Activity
Temporary Files	%SystemRoot%\TEMP	Recent Activity
Path	C:\WINDOWS	Recent Activity
Product ID	55274-640-0147306-23684	Recent Activity
Owner	Greg Schardt	Recent Activity
Organization	N/A	Recent Activity
Source File Path	/img_SCHARDT.001	
Artifact ID	-9223372036854775670	

## Q7. Primary Domain Name

### Primary Domain Name: N-1A9ODN6ZXK4LQ

Primary Domain refers to the main domain associated with a particular entity or organization on the internet.

On our case this would be the default domain name for this computer. This would be an important piece of information as it could be used in further tracking the activities of the system.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" - Select vol2 – WINDOWS – system32 – config – software – Microsoft – WindowsNT – Current Version – Winlogon

The screenshot shows the Autopsy Forensic Browser interface. The left pane displays a file tree with various system32 and config subfolders. The 'config' folder under system32 is highlighted with a red box. The right pane shows a detailed view of the 'Winlogon' registry key. The 'DefaultDomainName' value is selected and highlighted with a red box, showing its value as 'N-1A9ODN6ZXK4LQ'. Other values listed include AutoRestartShell, DefaultUserName, LegalNoticeCaption, LegalNoticeText, PowerdownAfterShutdown, ReportBootOk, Shell, ShutdownWithoutLogon, System, Userinit, VmApplet, and WinQuota.

Name	Type	Value
DefaultDomainName	REG_DWORD	0x00000001 (1)
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"
WinQuota	REG_DWORD	0xffffffff (4294967295)

### Q8. Last recorded shutdown date/time

**Date/Time:** 2004/08/27-10:46:27

Shutdown time allows digital investigator to make a timeline of the system and it even allows the investigator to identify the system common uptime, finding this could allow us to identify each user's active time and matching this timeline with the suspicious activity. Timeline is very useful in narrowing down the suspect.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – WINDOWS – system32 – config – software – Microsoft – WindowsNT – Current Version – Prefetcher – ExitTime

The screenshot shows the Autopsy 4.21.0 interface. The left pane displays a file tree with various registry keys under 'system32\config\software'. The right pane shows a table of files and a detailed view of the 'ExitTime' key under 'Prefetcher' in the registry. The 'ExitTime' key is highlighted with a red box, and its value '2004/08/27-10:46:27' is also highlighted with a red box.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
software	1			2004-08-27 16:46:33 BST	2004-08-27 16:46:33 BST	2004-08-19 17:56:08 BST	2004-08-19 17:56:08 BST	8650752	Allocated
software.LOG	1			2004-08-27 16:46:32 BST	2004-08-27 16:46:32 BST	2004-08-19 17:56:08 BST	2004-08-19 17:56:08 BST	1024	Allocated
software.sav	1			2004-08-19 17:56:20 BST	2004-08-19 18:02:15 BST	2004-08-19 01:00:00 BST	2004-08-19 17:56:18 BST	630784	Allocated
SysEvent.Fvt	1			2004-08-27 16:46:29 RST	2004-08-27 16:46:29 RST	2004-08-19 17:59:15 RST	2004-08-19 17:59:15 RST	65536	Allocated

### Q9. Total OS Accounts

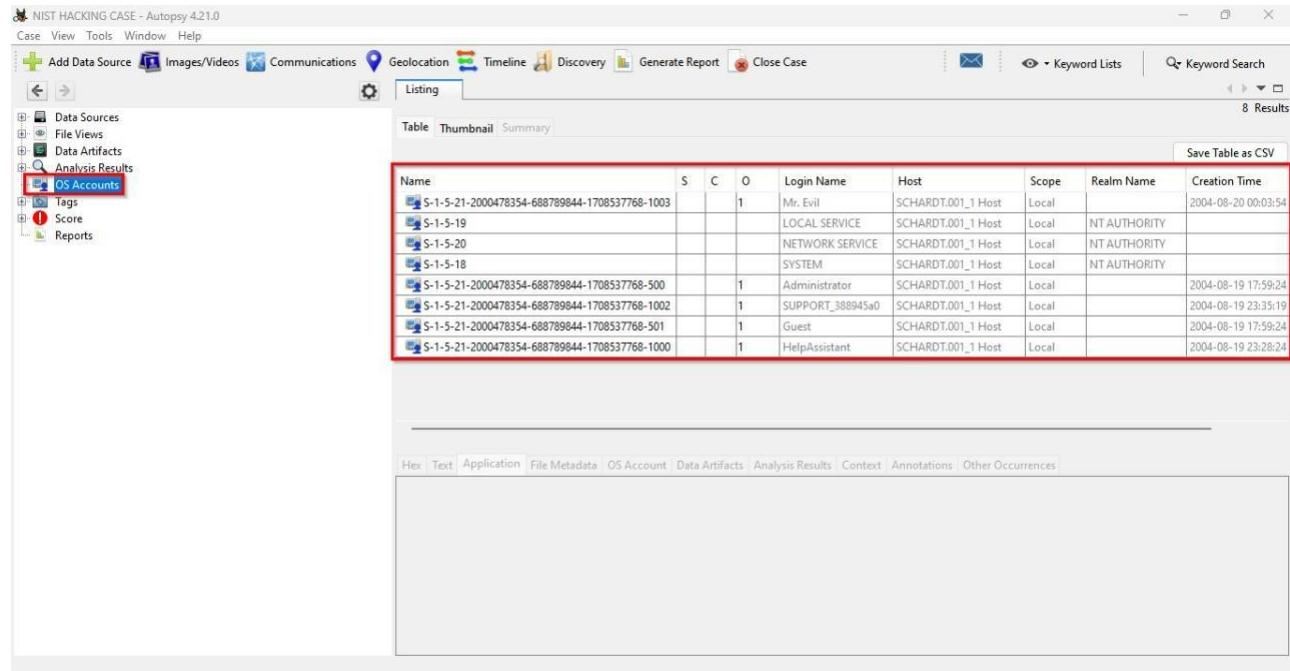
#### Accounts: 5

- 1) Guest
- 2) Administrator
- 3) Mr. Evil
- 4) Support388945a0
- 5) HelpAssistant

These OS accounts serve as entry points or starting points for a digital investigator. It tells how many potential users were active on the system. We can identify which user performed malicious activity on the system since some users will have limited access to the system hence lowering the number of suspects.

Total users present on the system or the people using the system.

#### Method: Click on OS Accounts



The screenshot shows the Autopsy 4.21.0 interface. The left sidebar has a tree view with nodes for Data Sources, File Views, Data Artifacts, Analysis Results, OS Accounts (which is selected and highlighted with a red box), Tags, Score, and Reports. The main pane is titled 'Listing' and shows a table of OS accounts. The table has columns: Name, S, C, O, Login Name, Host, Scope, Realm Name, and Creation Time. The data in the table is as follows:

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-2000478354-688789844-1708537768-1003			1	Mr. Evil	SCHARDT.001_1 Host	Local	NT AUTHORITY	2004-08-20 00:03:54
S-1-5-19				LOCAL SERVICE	SCHARDT.001_1 Host	Local	NT AUTHORITY	
S-1-5-20				NETWORK SERVICE	SCHARDT.001_1 Host	Local	NT AUTHORITY	
S-1-5-18				SYSTEM	SCHARDT.001_1 Host	Local	NT AUTHORITY	
S-1-5-21-2000478354-688789844-1708537768-500			1	Administrator	SCHARDT.001_1 Host	Local	NT AUTHORITY	2004-08-19 17:59:24
S-1-5-21-2000478354-688789844-1708537768-1002			1	SUPPORT_388945a0	SCHARDT.001_1 Host	Local	NT AUTHORITY	2004-08-19 23:35:19
S-1-5-21-2000478354-688789844-1708537768-501			1	Guest	SCHARDT.001_1 Host	Local	NT AUTHORITY	2004-08-19 17:59:24
S-1-5-21-2000478354-688789844-1708537768-1000			1	HelpAssistant	SCHARDT.001_1 Host	Local	NT AUTHORITY	2004-08-19 23:28:24

### Q10. Computer Most Frequent User

**Account Name:** Mr. Evil

Here we can see some information I gathered during my analysis. We can see that logon counts of the 5 accounts previously identified on the system. We can see that 'Mr. Evil' was active on this system, and he was the one with last logon meaning 'Mr. Evil' is the primary suspect now.

Account Name	Unique ID	Logon Count	Last Logon	Last Password Change	Invalid Logon Count
Administrator	500	0	Never	19/08/2004 17:17:29 UTC	0
Guest	501	0	Never	Never	0
HelpAssistant	1000	0	Never	19/08/2004 22:28:24 UTC	0
SUPPORT_388945a0	1002	0	Never	19/08/2004 22:35:19 UTC	0
Mr. Evil	1003	15	27/08/2004 15:08:23 UTC	19/08/2004 23:03:54 UTC	0

Table I  
LOGON INFORMATION FOR THE ACCOUNTS.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – WINDOWS – system32 – config – SAM – Sam – Domains – Account – Users

The screenshot shows the AccessData Registry Viewer interface. The left pane displays a tree view of registry keys under 'SAM\Domains\Account\Users'. A red box highlights the 'Users' key, which contains subkeys for '000001F4', '000001F5', '000003E8', '000003EA', '000003EB', 'Administrator', 'Guest', 'HelpAssistant', 'Mr. Evil', and 'SUPPORT\_388945a0'. Another red box highlights the 'Mr. Evil' key in the 'Names' subkey. The right pane shows a table of registry keys with columns 'Name', 'Type', and 'Data'. It also shows a hex dump of the registry data for the 'Mr. Evil' key, with specific bytes highlighted in red. The bottom status bar shows the path 'SAM\Domains\Account\Users\000003EB' and an offset of 0.

## Q11. Last System Logon

### Last Logon User: Mr. Evil

This serves as timeline for a digital investigator meaning this user was the last active user on this machine. Meaning the malicious activity could potentially be performed by this user. 'Mr. Evil' is the person who lastly logon into the system previously identified as our primary suspect.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – Windows – System32 – Config – Software – Microsoft – WindowsNT – CurrentVersion – Winlogon – DefaultUsername

The screenshot shows the Autopsy 4.21.0 interface. The left pane shows a file tree with various system32 and config subfolders. The central pane is a table of results with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). There are 23 results listed. The right pane is a detailed analysis view for the 'DefaultUserName' key under the 'Winlogon' section. The key's value is 'Mr. Evil'. A red box highlights the 'DefaultUserName' key in the tree view and its value in the details pane.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
software	▼	1		2004-08-27 16:46:33 BST	2004-08-27 16:46:33 BST	2004-08-19 17:56:08 BST	2004-08-19 17:56:08 BST	8650752	Allocated
software.LOG	▼	1		2004-08-27 16:46:32 BST	2004-08-27 16:46:32 BST	2004-08-19 17:56:08 BST	2004-08-19 17:56:08 BST	1024	Allocated
software.sav	▼	1		2004-08-19 17:56:20 BST	2004-08-19 18:02:15 BST	2004-08-19 01:00:00 BST	2004-08-19 17:56:18 BST	630784	Allocated
SysEvent.Evt	▼	1		2004-08-27 16:46:29 BST	2004-08-27 16:46:29 BST	2004-08-27 16:46:29 BST	2004-08-19 17:59:15 BST	65536	Allocated
system	▼	1		2004-08-27 16:46:33 BST	2004-08-27 16:46:33 BST	2004-08-27 16:46:33 BST	2004-08-19 17:56:06 BST	2621440	Allocated

## Q12. Administrator Identification

**File:** irunin.ini **Software:** Look@LAN

On the search of the owner name “Greg Schardt”, reveals multiple hits. One of the program files proves that Greg Schardt is Mr. Evil and is also the administrator of this computer.

**Program File Name:** Look@Lan

**Path:** C-Program Files-Look@LAN-irunin.ini

In the link, I found out 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 same.

**Method:** Click on Keyword Search Option – Enter Owner Name “Greg Schardt” – It lists multiple files in which “C-Program Files-Look@LAN-irunin.ini”.

The screenshot shows the Autopsy 4.21.0 interface with a keyword search for "Greg Schardt". The search results table lists several files, with "irunin.ini" highlighted. The "Text" tab of the search results pane shows the contents of "irunin.ini" with the line "%REGOWNER%=<Greg Schardt" highlighted in red.

Name	Keyword Preview	Location
Unalloc_20051_351232_1683209728	REG_SZValue data = «Greg Schardt»(On Error) User no	/img_SCHARDT.001/vol.vol2/\$Unalloc/Unalloc_20051... 0000-00-00 00h
Unalloc_20051_1684736000_3639811072	Companyil SoName=Greg Schardt+C:\WINDOWS\Syst... /img_SCHARDT.001/vol.vol2/\$Unalloc/Unalloc_20051... 0000-00-00 00h	
irunin.ini	HTTP=600%REGOWNER%=<Greg Schardt>%REGORG... /img_SCHARDT.001/vol.vol2/Program Files/Look@L... 2004-08-25 16:	
Look@LAN Setup Log.txt	REG_SZValue data = «Greg Schardt»(On Error) User n	/img_SCHARDT.001/vol.vol2/WINDOWS/Look@LAN ... 2004-08-25 16:
b0019813.ppt	Companyil SoName=Greg Schardt+C:\WINDOWS\Syst... /img_SCHARDT.001/vol.vol2/ScannedFile/b001981... 0000-00-00 00h	
drwtsn32.log	Registered Owner: «Greg Schardt»-----> Task List <----- /img_SCHARDT.001/vol.vol2/Documents and Settings... 2004-08-20 16:	
Operating System Information Artifact	306-23684Owner : «Greg Schardt»Organization : N/A SCHARDT.001	
software	0oRegisteredOwner=Greg Schardt+26008XxCurriSoft /img_SCHARDT.001/vol.vol2/Windows/repair/softw... 2004-08-19 23:	
software	Companyil SoName=Greg Schardt+C:\WINDOWS\Syst... /img_SCHARDT.001/vol.vol2/WINDOWS/system32/co... 2004-08-27 16:	
AppEvent.Evt	Registered Owner: «Greg Schardt»-----> Task List <----- /img_SCHARDT.001/vol.vol2/WINDOWS/system32/co... 2004-08-27 16:	
f0256874.txt	REG_SZValue data = «Greg Schardt»(On Error) User no /img_SCHARDT.001/vol.vol2/\$CarvedFiles/1/f0256874... 0000-00-00 00h	

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page | Matches on page: 1 of 2 Match | 100% | Reset | Text Source: Search Results

```
%REGOWNER%=<Greg Schardt
%REGORGANIZATION%=<N/A
%DATE%=<08/25/04
%CURRENTMONTH%=<8
%CURRENTDAY%=<25
%CURRENTYEAR%=<2004
%CURRENTHOUR%=<10
%CURRENTMINUTE%=<55
%CURRENTSECOND%=<24
```

### Q13. System Network Cards

- 1) Compaq WL110 Wireless LAN PC Card
- 2) Xircom Card Bus Ethernet 100 + Modem 56 (Ethernet Interface)

Knowing about the Network card used by the system allows us to understand possible network configuration of the system. Its possible network capabilities and even its potential vulnerabilities on the internet.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – WINDOWS – system32 – config – software – Microsoft – Windows NT – CurrentVersion – NetworkCards

The screenshot shows the Autopsy 4.21.0 interface with the following details:

- File Path:** /img\_SCHARDT.001/vol/vol2/WINDOWS/system32/config
- Table View:**

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
SecEvent.Evt			1	2004-08-19 17:59:15 BST	2004-08-19 18:02:15 BST	2004-08-19 17:59:15 BST	2004-08-19 17:59:15 BST	65536	Allocated
SECURITY			1	2004-08-27 16:46:33 BST	2004-08-20 00:04:03 BST	2004-08-27 16:46:33 BST	2004-08-19 17:58:55 BST	262144	Allocated
SECURITY.LOG			1	2004-08-27 16:32:56 BST	2004-08-27 16:32:56 BST	2004-08-27 16:32:56 BST	2004-08-19 17:58:55 BST	1024	Allocated
software			1	2004-08-27 16:46:33 BST	2004-08-27 16:29:44 BST	2004-08-27 16:46:33 BST	2004-08-19 17:56:08 BST	8650752	Allocated
software\OS			1	1999-09-27 16:46:33 BST	1999-09-27 16:46:33 BST	1999-09-27 16:46:33 BST	1999-09-27 16:46:33 BST	1024	Allocated
- Details View:** The 'NetworkCards' key under 'software\OS' is selected. The 'Description' value is highlighted with a red box, showing the value 'Xircom CardBus Ethernet 100 + Modem 56 (Ether...)'.

#### Q14. IP and Mac Address

**IP Address:** 192.168.1.111

**Mac Address:** 00:10:a4:93:3e:09

Since IP address identifies a system uniquely on the internet, we can see activity of this IP on the internet. We can even use IP information website/tools to identify what activity this IP has performed. We can even match this IP with any network traffic collected from the crime site. We can also pull this IP's previously active location and confirm the system location in different timelines hence adding much to our analysis. MAC address identifies the machine uniquely. We can use this to identify the manufacturer of the machine.

Combining both we can identify the system from any previously created logs of the system, e.g., router logs, network logs etc. We can use this information to piece together what activity happened first and what after hence allowing to create a better timeline for investigation

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – Program Files – Look@LAN – irunin.ini

The screenshot shows the Autopsy 4.2.1.0 interface with the following details:

- Case View:** NIST HACKING CASE - Autopsy 4.2.1.0
- Tools:** Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, Close Case.
- Search:** Keyword search 1 - Greg Schardt, 11 Results.
- Left Panel (Data Sources):**
  - Data Sources
  - File Views
  - Data Artifacts
  - Analysis Results
    - Encryption Suspected (2)
    - Extension Mismatch Detected (1862)
    - Interesting Items (1)
    - Keyword Hits (40670)
      - Single Literal Keyword Search (11)
        - greg schardt (11)
      - Single Regular Expression Search (0)
      - Email Addresses (11323)
      - IP Addresses (8243)
      - Phone Numbers (1142)
      - URLs (19951)
    - Web Categories (4)
  - OS Accounts
  - Tags
  - Score
  - Reports
- Table View:** Shows a list of files found, including 'irunin.ini' which is highlighted. The table includes columns: Source Name, S, C, O, Keyword Preview, Keyword, Modified Time, and Access Time.
- Hex View:** Shows the raw hex and ASCII dump of the 'irunin.ini' file. The IP address 192.168.1.111 and MAC address 00:10:a4:93:3e:09 are highlighted in red in the ASCII dump.

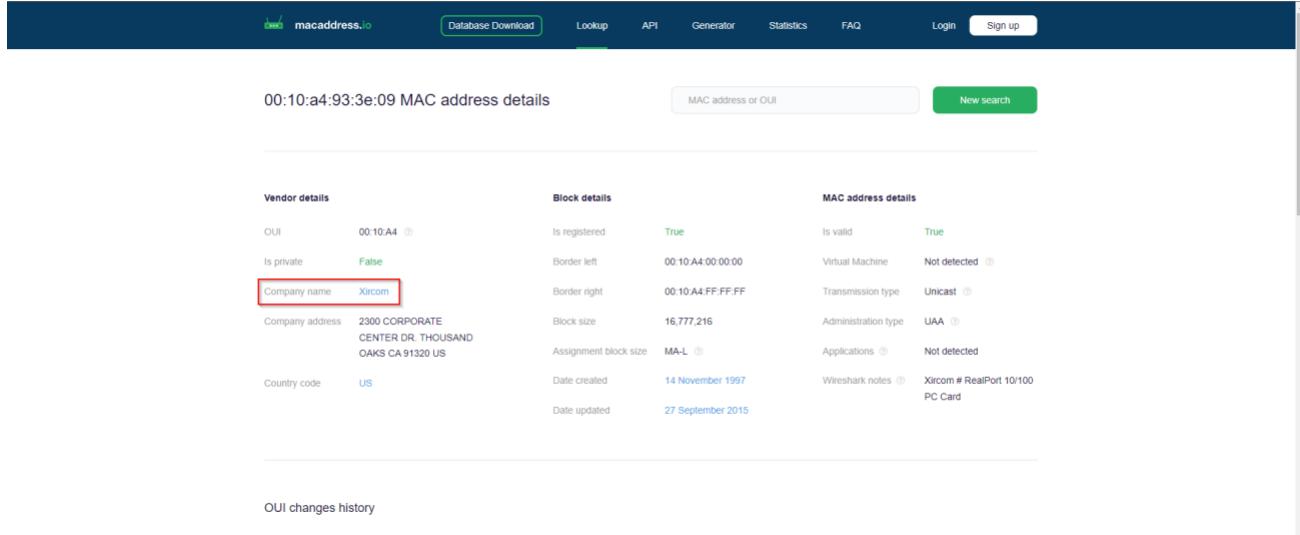
### Q15. Mac Address Vendor

#### Vendor: XIRCOM

Knowing the vendor of the MAC address allows us to identify the type of device related to the MAC address which in our case would be this system. We can even go back and start from the purchase/creation of this system if there is need for that.

The first three hex of Mac address belong to the specific vendor of Mac Address. I used an online tool Mac lookup to find its vendor.

**Method:** Any Mac lookup website.



00:10:a4:93:3e:09 MAC address details

Vendor details		Block details		MAC address details	
OUI	00:10:A4 ⓘ	Is registered	True	Is valid	True
Is private	False	Border left	00:10:A4:00:00:00	Virtual Machine	Not detected ⓘ
Company name	Xircom	Border right	00:10:A4:FF:FF:FF	Transmission type	Unicast ⓘ
Company address	2300 CORPORATE CENTER DR. THOUSAND OAKS CA 91320 US	Block size	16,777,216	Administration type	UAA ⓘ
Country code	US	Assignment block size	MA-L ⓘ	Applications	Not detected ⓘ
		Date created	14 November 1997	Wireshark notes	Xircom # RealPort 10/100 PC Card
		Date updated	27 September 2015		

OUI changes history

## Q16. Installed Programs Used in Hacking

The programs identified previously had these malicious programs.

- 1) Ethereal 0.10.6 v.0.10.6: Ethereal (now known as Wireshark) is a network protocol analyzer that captures and displays data packets transmitted over a network. It can be used for network troubleshooting, analysis, and in some cases, for unauthorized network monitoring or sniffing.
- 2) Look@LAN 2.50 Build 29: Look@LAN is a network monitoring tool that scans and analyzes network devices, IP addresses, and ports. It provides information about network topology, device status, and network traffic, which can be used for network management or potentially for network reconnaissance.
- 3) 123 Write All Stored Passwords: This tool is not well-known in the cybersecurity community. It suggests a function to extract and view stored passwords, which could be considered unethical or malicious depending on its actual functionality and usage.
- 4) Network Stumbler 0.4.0: Network Stumbler (also known as NetStumbler) is a wireless network scanner that detects and displays information about nearby Wi-Fi networks. It can be used for legitimate purposes such as network troubleshooting or mapping wireless coverage, but it can also be used for unauthorized scanning or network enumeration.
- 5) Cain & Abel v2.5 beta45: Cain & Abel is a popular password recovery tool that can recover various types of passwords, including network passwords, cached credentials, and more. It also has network sniffing capabilities, making it a versatile tool for both legitimate security testing and potentially malicious activities.
- 6) Anonymizer Bar 2.0: Anonymizer Bar is a browser toolbar that offers anonymous web browsing features, such as masking IP addresses and encrypting internet traffic. While it can be used for privacy purposes, it can also facilitate anonymous access to illicit or restricted content.
- 7) mIRC: mIRC is an internet relay chat (IRC) client used for real-time communication in chat rooms and online forums. It's not inherently a hacking tool, but it can be used by hackers or cybercriminals for communication and coordination in illegal activities.

**Method:** Click on Data Artifacts – Installed Programs

The screenshot shows the Autopsy 4.21.0 interface with the 'Installed Programs' table highlighted. The table has the following structure:

Source Name	S	C	O	Program Name	Date/Time	Data Source
software			1	Ethereal 0.10.6 v.0.10.6	2004-08-27 15:29:19 BST	SCHARDT.001
software			1	WinPcap 3.01 alpha	2004-08-27 15:15:19 BST	SCHARDT.001
software			1	Network Stumbler 0.4.0 (remove only)	2004-08-27 15:12:15 BST	SCHARDT.001
software			1	Look@LAN 2.50 Build 29	2004-08-25 15:56:11 BST	SCHARDT.001
software			1	123 Write All Stored Passwords	2004-08-20 15:10:08 BST	SCHARDT.001
software			1	Powertoys For Windows XP v.1.00.0000	2004-08-20 15:12:43 BST	SCHARDT.001
software			1	mIRC	2004-08-20 15:10:04 BST	SCHARDT.001
software			1	CuteHTML	2004-08-20 15:09:03 BST	SCHARDT.001
software			1	CuteFTP	2004-08-20 15:09:02 BST	SCHARDT.001
software			1	Forté Agent	2004-08-20 15:08:19 BST	SCHARDT.001
software			1	Faber Toys v.2.4 Build 216	2004-08-20 15:07:25 BST	SCHARDT.001
software			1	Cain & Abel v2.5 beta45	2004-08-20 15:05:58 BST	SCHARDT.001
software			1	Anonymizer Bar 2.0 (remove only)	2004-08-20 15:05:09 BST	SCHARDT.001
software			1	WebFids XP v.9.50.5318	2004-08-19 23:04:50 BST	SCHARDT.001
software			1	Microsoft NetShow Player 2.0	2004-08-19 23:04:36 BST	SCHARDT.001
software			3	MPlayer2	2004-08-19 23:04:36 BST	SCHARDT.001
software			1	Branding	2004-08-19 22:37:31 BST	SCHARDT.001
software			1	PCHealth	2004-08-19 22:32:06 BST	SCHARDT.001
software			1	DirectAnimation	2004-08-19 22:31:52 BST	SCHARDT.001
software			1	NetsMeeting	2004-08-19 22:31:52 BST	SCHARDT.001
software			3	AddressBook	2004-08-19 22:31:51 BST	SCHARDT.001

### Q17. SMTP Email Address

**Email Address:** whoknowsme@sbcglobal.net

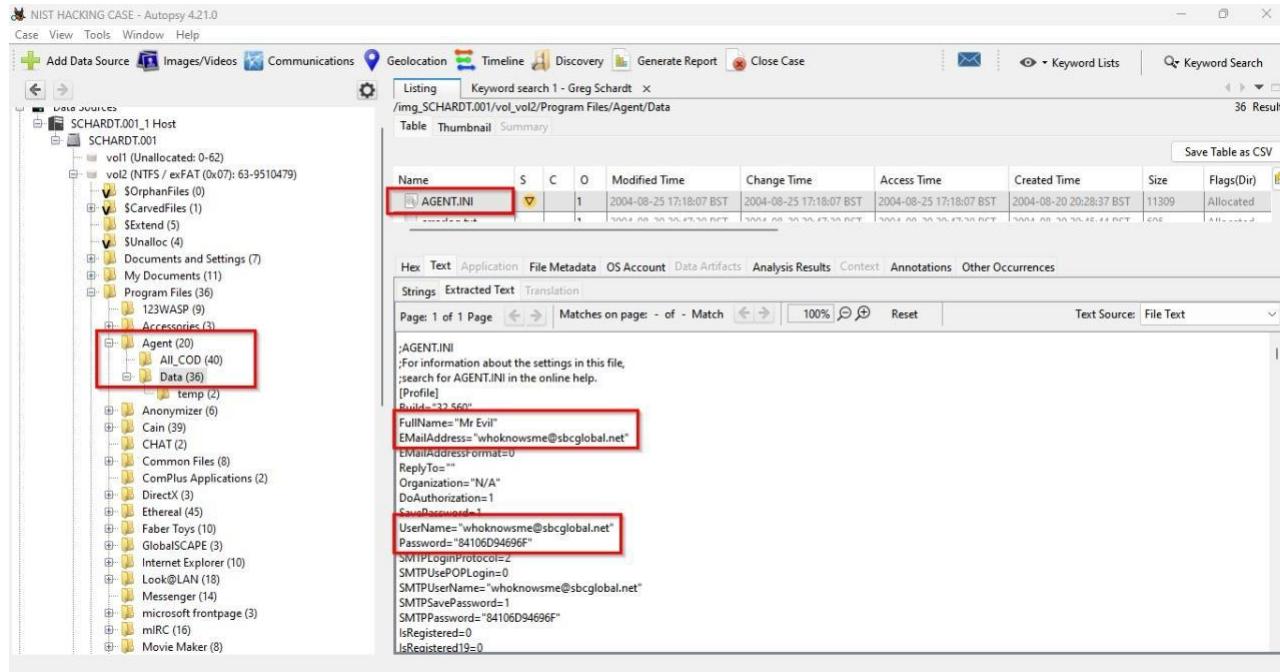
**Belongs to:** Full Name = "Mr. Evil"

**Username:** whoknowsme@sbcglobal.net

**Password:** "84106D94696F"

From the previously installed list of programs, I found a program named Forte Agent. It's an old SMTP client. From this data, I extracted the user "Mr. Evil" SMTP email address. This could serve as important evidence. We can see what users have interacted with him.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – Program Files – Agent – Data – Agent.ini



The screenshot shows the Autopsy Forensic Browser interface. The left sidebar shows a tree view of data sources, with 'SCHARDT.001\_1 Host' and 'SCHARDT.001' selected. Under 'SCHARDT.001', 'vol2' is selected, showing various file types like 'SOrphanFiles', 'SCarvedFiles', 'SExtend', 'SUnalloc', 'Documents and Settings', 'My Documents', 'Program Files', and 'Accessories'. A red box highlights the 'Accessories' folder, which contains 'Agent' (20 files), 'All\_COD' (40 files), and 'Data' (36 files). The 'Agent' folder is expanded, and a red box highlights it. The right pane shows a table of results for 'AGENT.INI'. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). One result is shown in the table, with a red box highlighting the 'Name' column. Below the table, the 'Text' tab is selected in the bottom navigation bar, showing the contents of 'AGENT.INI'. A red box highlights the entire text area. The text content includes configuration settings for the Agent application, including the user's name, email address, and password. The email address 'whoknowsme@sbcglobal.net' and password '84106D94696F' are both highlighted with red boxes.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
AGENT.INI		1		2004-08-25 17:18:07 BST	2004-08-25 17:18:07 BST	2004-08-25 17:18:07 BST	2004-08-20 20:28:37 BST	11309	Allocated

```

;AGENT.INI
;For information about the settings in this file,
;search for AGENT.INI in the online help.
[Profile]
Build="32.560"
FullName="Mr Evil"
EmailAddress="whoknowsme@sbcglobal.net"
EmailAddressFormat=0
ReplyTo=""
Organization="N/A"
DoAuthorization=1
SavePassword=1
UserName="whoknowsme@sbcglobal.net"
Password="84106D94696F"
SMTPProtocol=2
SMTPUsePPLLogin=0
SMTPUserName="whoknowsme@sbcglobal.net"
SMTPSavePassword=1
SMTPPassword="84106D94696F"
IsRegistered=0
IsRegistered19=0

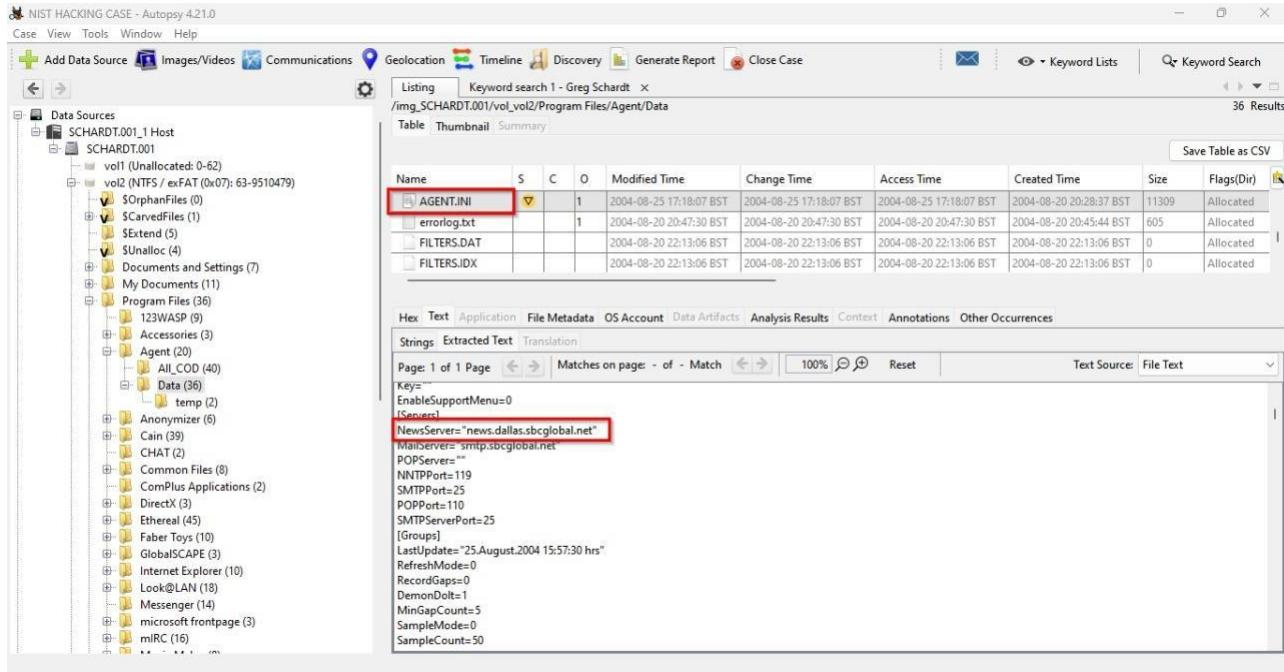
```

## Q18. NNTP Server Settings

**News Server:** news.dallas.sbcglobal.net

I found this NNTP server settings of “Mr. Evil” from the same file of Forte Agent. We can see what type of discussion this user is part of and what type of newsgroup this user interacts in since there are legal newsgroups and illegal newsgroups as well. E.g., Any criminal discussion/activity groups.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – Program Files – Agent – Agent.ini



The screenshot shows the Autopsy 4.21.0 interface. The left sidebar shows 'Data Sources' with 'SCHARDT.001\_1 Host' selected, which contains 'SCHARDT.001' and 'vol1 (Unallocated: 0-62)'. 'vol1' contains 'vol2 (NTFS / exFAT (0x07): 63-9510479)', which in turn contains 'AGENT.INI'. The main pane shows a table of files with 'AGENT.INI' selected. The 'Text' tab of the file details pane is open, showing the following configuration:

```

[NewsServer]
NewsServer="news.dallas.sbcglobal.net"

```

## Q19. NNTP Server Settings Information

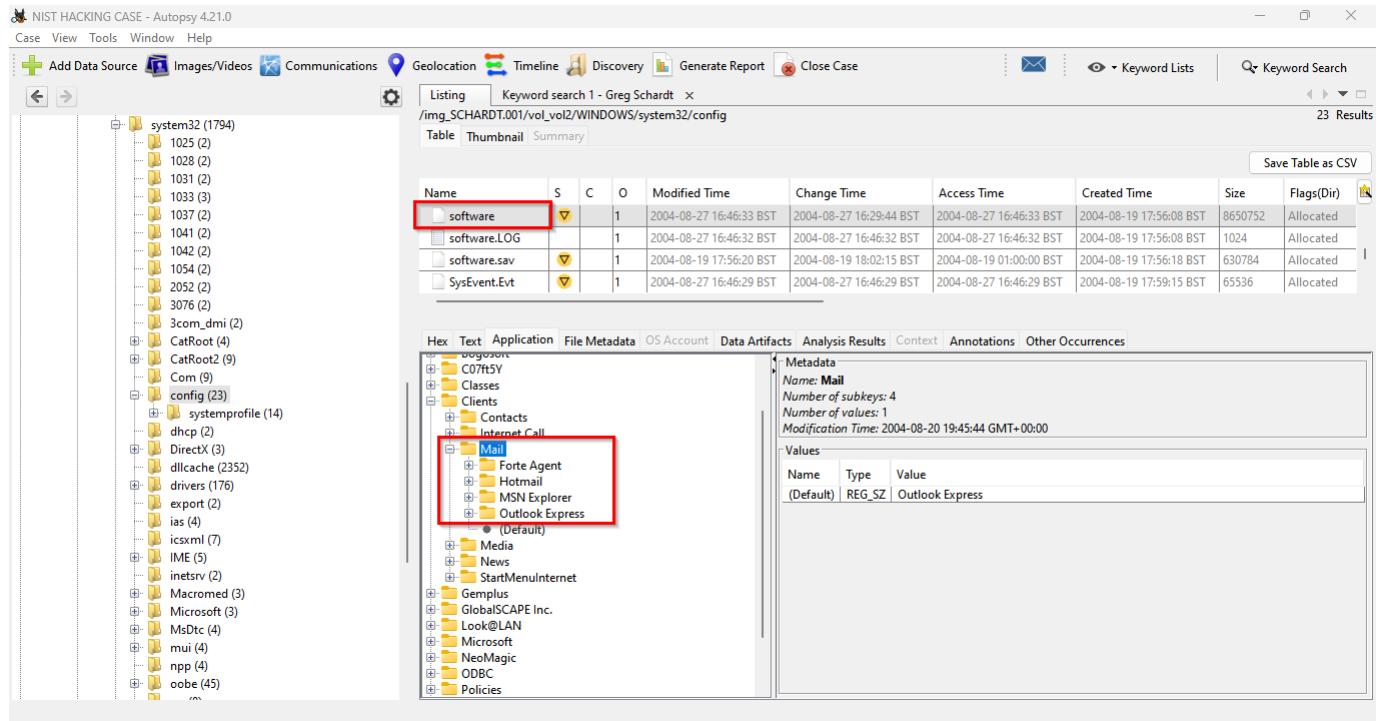
### Programs:

- 1) Forte Agent
- 2) Outlook Express

The two programs that revealed this information is Forte Agent. As you know we solve previous questions by using Data of Forte agent. After search in the autopsy, I cannot find any other program which shows these information.

Email clients can contribute to the digital footprint of a user. We can identify the user activity on these email clients. We can also use it to identify what email client was used for malicious activity.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – WINDOWS – system32 – config – software – clients – Mail



The screenshot shows the Autopsy 4.21.0 interface. The top navigation bar includes Case, View, Tools, Window, Help, Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, Close Case, Keyword Lists, and Keyword Search. The main pane displays a file tree on the left and a table and details pane on the right. The file tree shows a structure like system32 (1794) / 1025 (2) / 1028 (2) / 1031 (2) / 1033 (3) / 1037 (2) / 1041 (2) / 1042 (2) / 1054 (2) / 2052 (2) / 3076 (2) / 3com\_dmi (2) / CatRoot (4) / CatRoot2 (9) / Com (9) / config (23) / systemprofile (14) / dhcp (2) / DirectX (3) / dllcache (2352) / drivers (176) / export (2) / ias (4) / icxml (7) / IME (5) / inetsrv (2) / Macromed (3) / Microsoft (3) / MsDtc (4) / mui (4) / npp (4) / oobe (45) / ... The table in the center lists files under the 'software' folder, with the 'Mail' key highlighted. The details pane on the right shows the 'Mail' key structure, including subkeys like Forte Agent, Hotmail, MSN Explorer, and Outlook Express, and their corresponding values.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
software	1			2004-08-27 16:46:33 BST	2004-08-27 16:46:33 BST	2004-08-19 17:56:08 BST	2004-08-19 17:56:08 BST	8650752	Allocated
software.LOG	1			2004-08-27 16:46:32 BST	2004-08-27 16:46:32 BST	2004-08-19 17:56:08 BST	2004-08-19 17:56:08 BST	1024	Allocated
software.sav	1			2004-08-19 17:56:20 BST	2004-08-19 18:02:15 BST	2004-08-19 01:00:00 BST	2004-08-19 17:56:18 BST	630784	Allocated
SysEvent.Evt	1			2004-08-27 16:46:29 BST	2004-08-27 16:46:29 BST	2004-08-19 17:59:15 BST	2004-08-19 17:59:15 BST	65536	Allocated

## Q20. Subscribed Newsgroups

### Newsgroups:

- 1) Alt.2600.phreakz
- 2) Alt.2600
- 3) Alt.2600.cardz
- 4) Alt.2600codez
- 5) Alt.2600.crackz

Previously discussed that a person can be subscribed to illegal newsgroup or malicious newsgroup here we can see that Mr. Evil is subscribed to many hacking newsgroups confirming our suspicion of this individual.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – Document and Settings – Mr. Evil – Local Settings – Application Data – Identities – EF086998-1115-4ECD-9B13-9ADC067B4929 – Microsoft – Outlook Express

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2004-08-20 22:14:23 BST	2004-08-20 22:15:52 BST	2004-08-20 22:13:25 BST	2004-08-20 22:13:25 BST
[parent folder]				2004-08-20 22:13:25 BST	2004-08-20 22:13:25 BST	2004-08-20 22:13:25 BST	2004-08-20 22:13:25 BST
alt.2600.cardz.dbx	1			2004-08-20 22:27:17 BST	2004-08-20 22:27:17 BST	2004-08-20 22:27:17 BST	2004-08-20 22:18:41 BST
alt.2600.codez.dbx	1			2004-08-20 22:27:16 BST	2004-08-20 22:27:16 BST	2004-08-20 22:27:16 BST	2004-08-20 22:18:46 BST
alt.2600.crackz.dbx	1			2004-08-20 22:27:16 BST	2004-08-20 22:27:16 BST	2004-08-20 22:27:16 BST	2004-08-20 22:18:32 BST
alt.2600.dbx	1			2004-08-20 22:27:23 BST	2004-08-20 22:27:23 BST	2004-08-20 22:27:23 BST	2004-08-20 22:27:23 BST
alt.2600.hackerz.dbx	1			2004-08-20 22:27:16 BST	2004-08-20 22:27:16 BST	2004-08-20 22:27:16 BST	2004-08-20 22:25:57 BST
alt.2600.moderated.dbx	1			2004-08-20 22:19:20 BST	2004-08-20 22:19:20 BST	2004-08-20 22:19:20 BST	2004-08-20 22:19:15 BST
alt.2600.phreakz.dbx	1			2004-08-20 22:27:10 BST	2004-08-20 22:27:10 BST	2004-08-20 22:27:10 BST	2004-08-20 22:25:09 BST
alt.2600.programz.dbx	1			2004-08-20 22:27:16 BST	2004-08-20 22:27:16 BST	2004-08-20 22:27:16 BST	2004-08-20 22:24:25 BST
alt.binaries.hacking.beginner.dbx	1			2004-08-20 22:23:41 BST	2004-08-20 22:23:41 BST	2004-08-20 22:23:41 BST	2004-08-20 22:22:54 BST
alt.binaries.hacking.computers.dbx	1			2004-08-20 22:20:55 BST	2004-08-20 22:20:55 BST	2004-08-20 22:20:55 BST	2004-08-20 22:20:36 BST
alt.binaries.hacking.utilities.dbx	1			2004-08-20 22:19:24 BST	2004-08-20 22:19:24 BST	2004-08-20 22:19:24 BST	2004-08-20 22:19:22 BST
alt.binaries.hacking.websites.dbx	1			2004-08-20 22:20:50 BST	2004-08-20 22:20:50 BST	2004-08-20 22:20:50 BST	2004-08-20 22:20:42 BST
alt.dss.hack.dbx	1			2004-08-20 22:22:54 BST	2004-08-20 22:22:54 BST	2004-08-20 22:22:54 BST	2004-08-20 22:20:55 BST
alt.hacking.dbx	1			2004-08-20 22:27:07 BST	2004-08-20 22:27:07 BST	2004-08-20 22:27:07 BST	2004-08-20 22:23:41 BST
alt.nl.binaries.hack.dbx	1			2004-08-20 22:20:34 BST	2004-08-20 22:20:34 BST	2004-08-20 22:20:34 BST	2004-08-20 22:19:52 BST
alt.stupidity.hackers.malicious.dbx	1			2004-08-20 22:19:27 BST	2004-08-20 22:19:27 BST	2004-08-20 22:19:27 BST	2004-08-20 22:19:25 BST

## Q21. MIRC User Settings

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

mIRC is an IRC (Internet Relay Chat) client software for real time communication we can use it identify username for the user. It can serve as important evidence since some people use the same username on different platforms. We can also follow users chat and identify what type of discussion or what type of people user was in contact with.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – Program Files – mIRC – mirc.ini.

The screenshot shows the Autopsy 4.2.1.0 interface. The left sidebar shows a tree view of the file system, with 'Program Files (36)' expanded and 'mIRC (16)' selected. The main pane shows a table of files in the '/img\_SCHARDT.001/vol\_vol2/Program Files/mIRC' directory. The 'mirc.ini' file is highlighted with a red box. The table columns are: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The 'mirc.ini' row shows the following values: Name=mirc.ini, S=1, C=1, O=1, Modified Time=2004-08-20 16:09:56 BST, Change Time=2004-08-20 16:09:56 BST, Access Time=2004-08-20 16:09:56 BST, Created Time=2004-08-20 16:09:56 BST, Size=5483, Flags(Dir)=Allocated. Below the table, the 'Extracted Text' tab is selected, showing the contents of the mirc.ini file. The file contains the following configuration:

```

user=Mini Me
email=none@of.ya
nick=Mr
anick=mrevilrulez
host=Undernet: US, CA, LosAngeles SERVER: losangeles.ca.us.undernet.org:6660 GROUP: Undernet
[files]
servers=servers.ini
finger=finger.txt
url=url.ini
addrbk=addrbk.ini
[styles]
thin=1
font=1
hide=1
color=default
size=2
buttons=0
[chat]

```

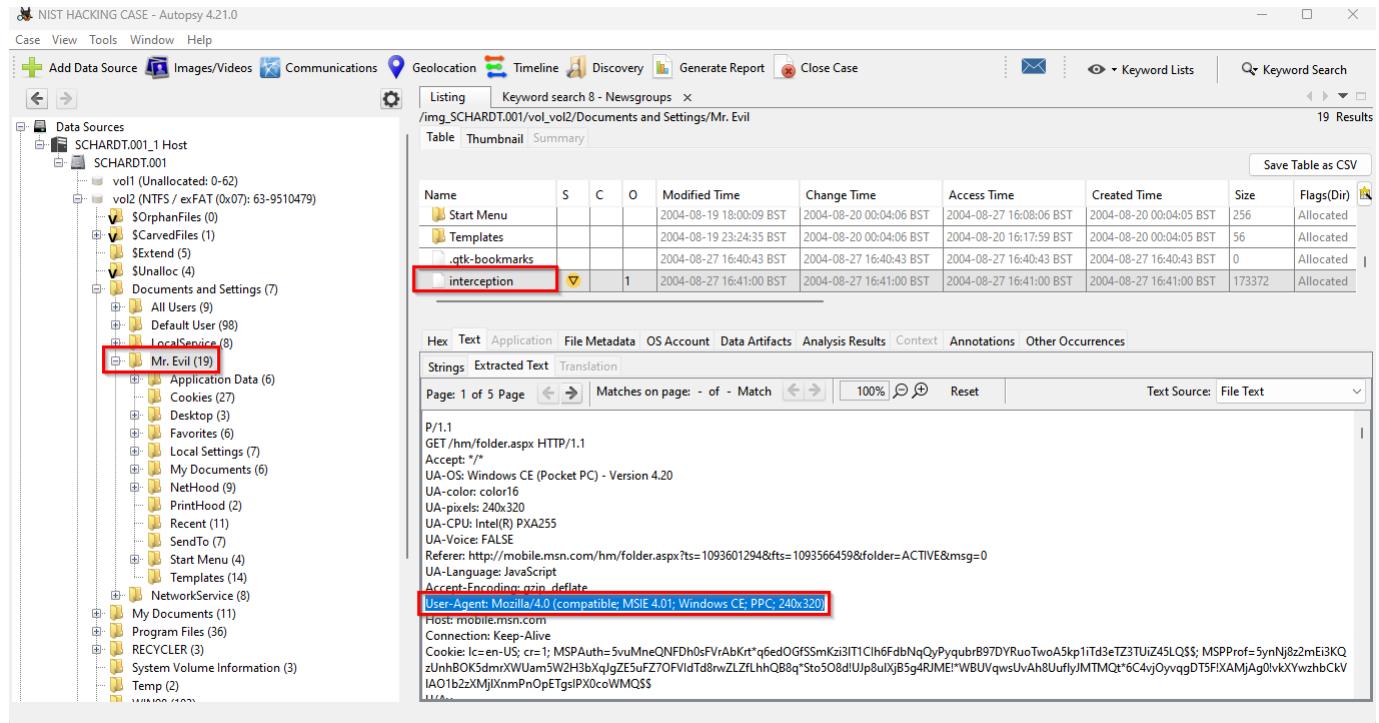
## Q22. Information Reveal from Text File

**User-Agent:** Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)

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 reassembled, the default save directory is that /users/My Documents directory. The File name is Interception.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – Document and Settings – Mr.Evil – interception.

Then scroll down and see User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)



The screenshot shows the Autopsy 4.2.10 interface. The left sidebar displays the 'Data Sources' tree, with 'SCHARDT.001\_1 Host' selected. Under 'SCHARDT.001', 'vol2 (NTFS / exFAT (0x07): 63-9510479)' is expanded, showing 'Start Menu', 'Templates', 'gtk-bookmarks', and 'interception'. The 'interception' file is highlighted with a red box. The main pane shows a table of file metadata and the 'Extracted Text' tab. The extracted text pane displays the following User-Agent header:

```
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
```

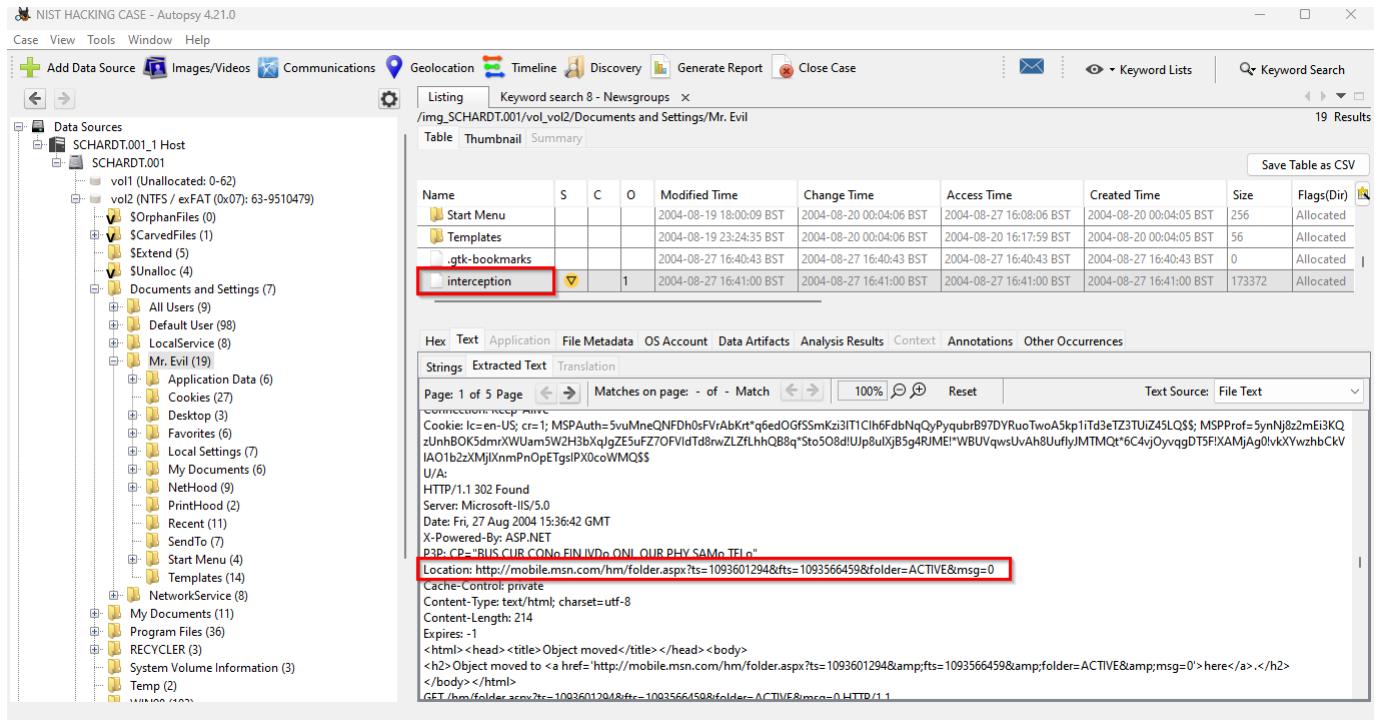
## Q23. Victims Website Accessed

### Websites:

- 1) Mobile.msn.com
- 2) Login.passport.com
- 3) Passportimages.com

Now we can see all the websites accessed by Mr. Evil. We can check which are normal and which are malicious.

**Method:** You can also copy all texts from the intercept file and search for .com it will show you the websites which were visited.



The screenshot shows the NIST Hacking CASE - Autopsy 4.21.0 interface. The 'Data Sources' tree on the left shows the 'SCHARDT.001 Host' with 'vol1' and 'vol2' volumes. The 'vol1' volume is selected. The 'Listing' tab in the center shows a search result for 'Newsgroups' in the '/img\_SCHARDT.001/vol1\_vol2/Documents and Settings/Mr. Evil' directory. The results table has 19 rows. The 'interception' file is highlighted with a red box. The 'Extracted Text' tab on the right shows the contents of the 'interception' file, which includes a redirect to a mobile.msn.com page.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Start Menu				2004-08-19 18:00:09 BST	2004-08-20 00:04:06 BST	2004-08-27 16:08:06 BST	2004-08-20 00:04:05 BST	256	Allocated
Templates				2004-08-19 23:24:35 BST	2004-08-20 00:04:06 BST	2004-08-20 16:17:59 BST	2004-08-20 00:04:05 BST	56	Allocated
.gtk-bookmarks				2004-08-27 16:40:43 BST	2004-08-27 16:40:43 BST	2004-08-27 16:40:43 BST	2004-08-27 16:40:43 BST	0	Allocated
interception			1	2004-08-27 16:41:00 BST	2004-08-27 16:41:00 BST	2004-08-27 16:41:00 BST	2004-08-27 16:41:00 BST	173372	Allocated

```

HTTP/1.1 302 Found
Server: Microsoft-IIS/5.0
Date: Fri, 27 Aug 2004 15:36:42 GMT
X-Powered-By: ASP.NET
P3P: CP="BUS CUR CONN FIN IVD ONL OUR PHY SAMo TEL"
Location: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 214
Expires: -1
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0">here</a>.</h2>
</body></html>
GET /hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0 HTTP/1.1

```

*Q24. Users Web Based Email Address*

**Email Address:** mrevilrulez@yahoo.com

From the previously identified mails this yahoo mail was used online we can also see that this mail was used and we can also see in the web history and identify what URLs/ website this user was interacting. Which looks very suspicious with a hacker in its name.

## **Method:** Click on Data Artifacts – Web History

## Q25. Yahoo File

**File:** ShowLetter[1].htm

The file ShowLetter[1].htm is the file under which yahoo saves its email copies.

**Method:** Keyword Search the Email.

NIST HACKING CASE - Autopsy 4.21.0

Case View Tools Window Help

Geolocation Timeline Discovery Generate Report Close Case

Listing Keyword search 9 - mrevirulez@ya... x

10 Results

Save Table as CSV

Name Keyword Preview Location Modified Time Change

ShowLetter[1].htm calendar | notepad «mrevirulez@yahoo.com» [sign o... /img\_SCHARDT.001/vol\_vol2/Documents and Settings... 2004-08-20 16:38:30 BST 2004-08-20 16:38:30 BST

Table Thumbnail Summary

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Download Images

Yahoo! My Yahoo! Mail

Welcome, **mrevirulez** [Sign Out, My Account]

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

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

Choose from 10 Free Cell Phones Previous | Next | Back to Messages Printable View - Full Headers

Folders [Add - Edit] Delete Reply Forward Spam Move...

- Inbox
- Draft
- Sent
- Trash[Empty]

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

Date: Fri, 20 Aug 2004 08:38:04 -0700 (PDT)

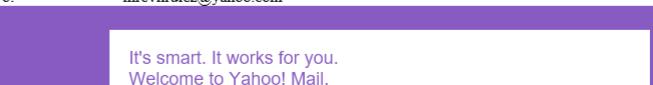
From:

Subject: Welcome to Yahoo!

To: mrevirulez@yahoo.com

Check your Credit!

It's Free.

Free Checking w/ 

## Q26. Executable files In RecycleBin

### Files:

- 1) Dc1.exe
- 2) Dc2.exe
- 3) Dc3.exe
- 4) Dc4.exe

These 4 executables were discovered in the recycle bin. Since executable is the first step in taking privileges from the user in malware activity. This could serve as important evidence for us. We can even check if these executables are dangerous or not.

**Method:** Click on Data source – Select the Host 'SCHARDT.001\_1 Host' – Select "SCHARDT.001" – Select vol2 – Recycler

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	F
[current folder]				2004-08-27 16:29:58 BST	2004-08-27 16:29:58 BST	2004-08-25 17:18:25 BST	2004-08-25 17:18:25 BST	56	Allocated	A
[parent folder]				2004-08-25 17:18:25 BST	2004-08-25 17:18:25 BST	2004-08-27 16:12:30 BST	2004-08-25 17:18:25 BST	328	Allocated	A
Dc1.exe	1			2004-08-25 16:51:23 BST	2004-08-25 17:18:25 BST	2004-08-25 16:56:08 BST	2004-08-25 16:51:24 BST	2160043	Allocated	A
Dc2.exe	1			2004-08-27 16:11:07 BST	2004-08-27 16:12:30 BST	2004-08-27 16:12:18 BST	2004-08-27 16:11:07 BST	1324940	Allocated	A
Dc3.exe	1			2004-08-27 16:14:20 BST	2004-08-27 16:15:26 BST	2004-08-27 16:15:16 BST	2004-08-27 16:14:20 BST	442417	Allocated	A
Dc4.exe	1			2004-08-27 16:24:24 BST	2004-08-27 16:29:58 BST	2004-08-27 16:29:47 BST	2004-08-27 16:24:24 BST	8460502	Allocated	A
desktop.ini				2004-08-25 17:18:25 BST	2004-08-25 17:18:25 BST	2004-08-27 16:12:30 BST	2004-08-25 17:18:25 BST	65	Allocated	A
INFO2				2004-08-27 16:46:17 BST	2004-08-27 16:46:17 BST	2004-08-27 16:46:17 BST	2004-08-25 17:18:25 BST	3220	Allocated	A

*Q27 Really Deleted*

**Conclusion:** No, the files are not actually deleted. These files can be restored from the recycle bin.

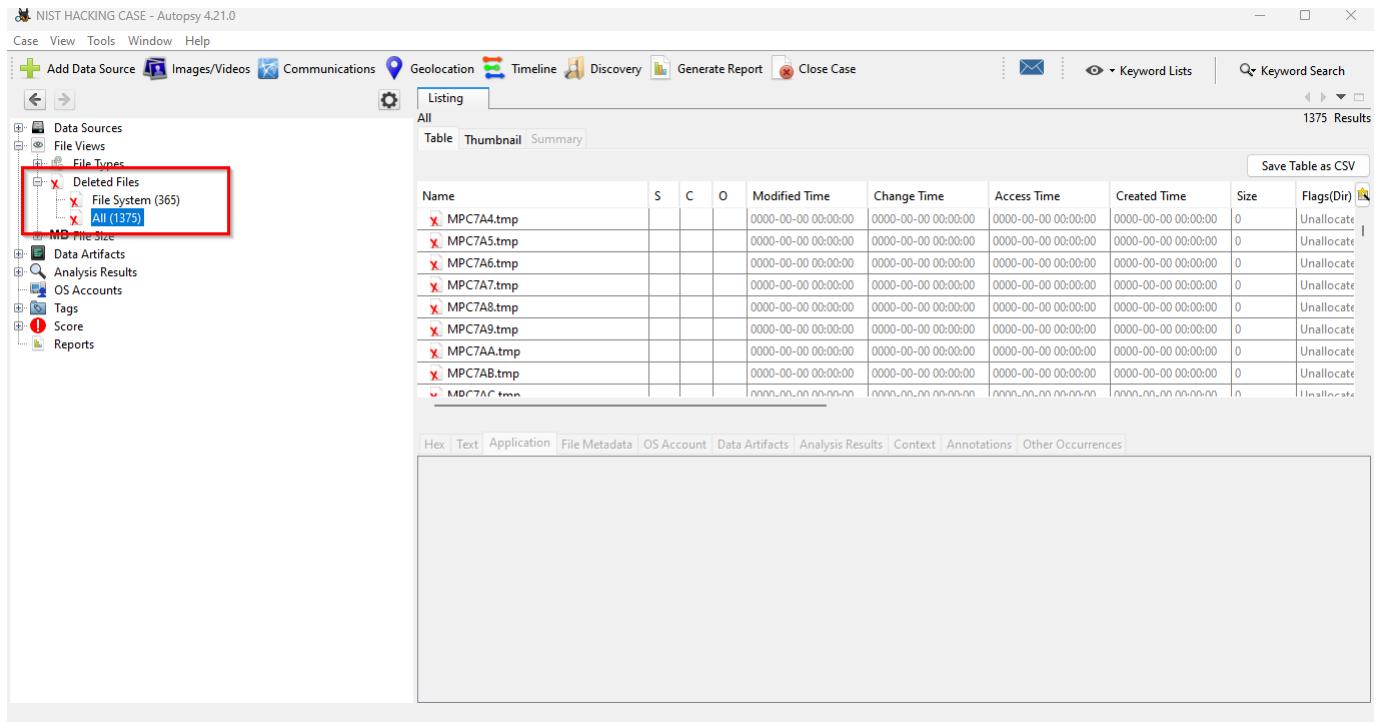
### Q28. Reportedly Deleted

**Total: 1375**

The list of files deleted on the system.

These file are important as these files could be deleted by “Mr.Evil” to hide his malicious intents or even his plans. Maybe some information that the investigator could use.

**Method:** Review file system Tree structure.



**Deleted Files**

**File System (365)**

**All (1375)**

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
MPCTA4.tmp				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	Unallocated
MPCTA5.tmp				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	Unallocated
MPCTA6.tmp				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	Unallocated
MPCTA7.tmp				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	Unallocated
MPCTA8.tmp				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	Unallocated
MPCTA9.tmp				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	Unallocated
MPCTAA.tmp				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	Unallocated
MPCTAB.tmp				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	Unallocated
MPCTAC.tmp				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	Unallocated

## V. FINDINGS/CONCLUSION

Key Findings from this investigation involve

*A. Chain of Custody and Evidence Integrity:*

The chain of custody could not be maintained due to missing acquisition details. We cannot say it that the provided image is valid and did not alter during transfer for an investigation. So its a chance that provided evidence is not valid.

*B. System Information:*

- 1) **Operating System:** Microsoft Windows XP.
- 2) **Install Date:** Thursday, August 19, 2004, 10:48:27 PM (UTC).
- 3) **Time Zone:** Central Standard Time (CST).
- 4) **Registered Owner:** Greg Schardt.
- 5) **Computer Account Name:** N-1A9ODN6ZXK4LQ.
- 6) **Primary Domain Name:** N-1A9ODN6ZXK4LQ.
- 7) **Last Shutdown Date/Time:** 2004/08/27-10:46:27.

*C. User Accounts:*

- 1) **Total OS accounts:** 5 (Guest, Administrator, Mr. Evil, Support388945a0, HelpAssistant).
- 2) The Only Active User on this system is Mr. Evil, with 15 logons and last logon on 27/08/2004 15:08:23 UTC.

*D. Network Configuration:*

- 1) **Network Cards:** Compaq WL110 Wireless LAN PC Card and Xircom Card Bus Ethernet 100 + Modem 56.
- 2) **IP Address:** 192.168.1.111.
- 3) **MAC Address:** 00:10:a4:93:3e:09.
- 4) **MAC Address Vendor:** XIRCOM.

*E. Malicious Programs:*

- 1) **Ethereal 0.10.6:** Network protocol analyzer.
- 2) **Look@LAN 2.50 Build 29:** Network monitoring tool.
- 3) **123 Write All Stored Passwords:** Password recovery tool.

*F. Other Evidence:*

- 1) **Owner Identification:** The irunin.ini file for Look@LAN indicated Greg Schardt as the registered owner and Mr. Evil as the LAN user, proving both are the same individual.
- 2) **Deleted Files:** Various executable files and suspicious programs found in the recycle bin.
- 3) **Email Communications and Web Activities:** Evidence of communication and activities related to hacking.

*G. Conclusion:*

The comprehensive forensic analysis of the Dell Latitude CPI system owned by Greg Schardt revealed substantial evidence linking Greg Schardt, operating under the alias "Mr. Evil," to hacking activities. Key findings include the presence of network monitoring and password recovery tools, suspicious user activities, and incriminating data in both active and deleted states. This evidence supports the conclusion that Greg Schardt is guilty of engaging in hacking activities.