
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

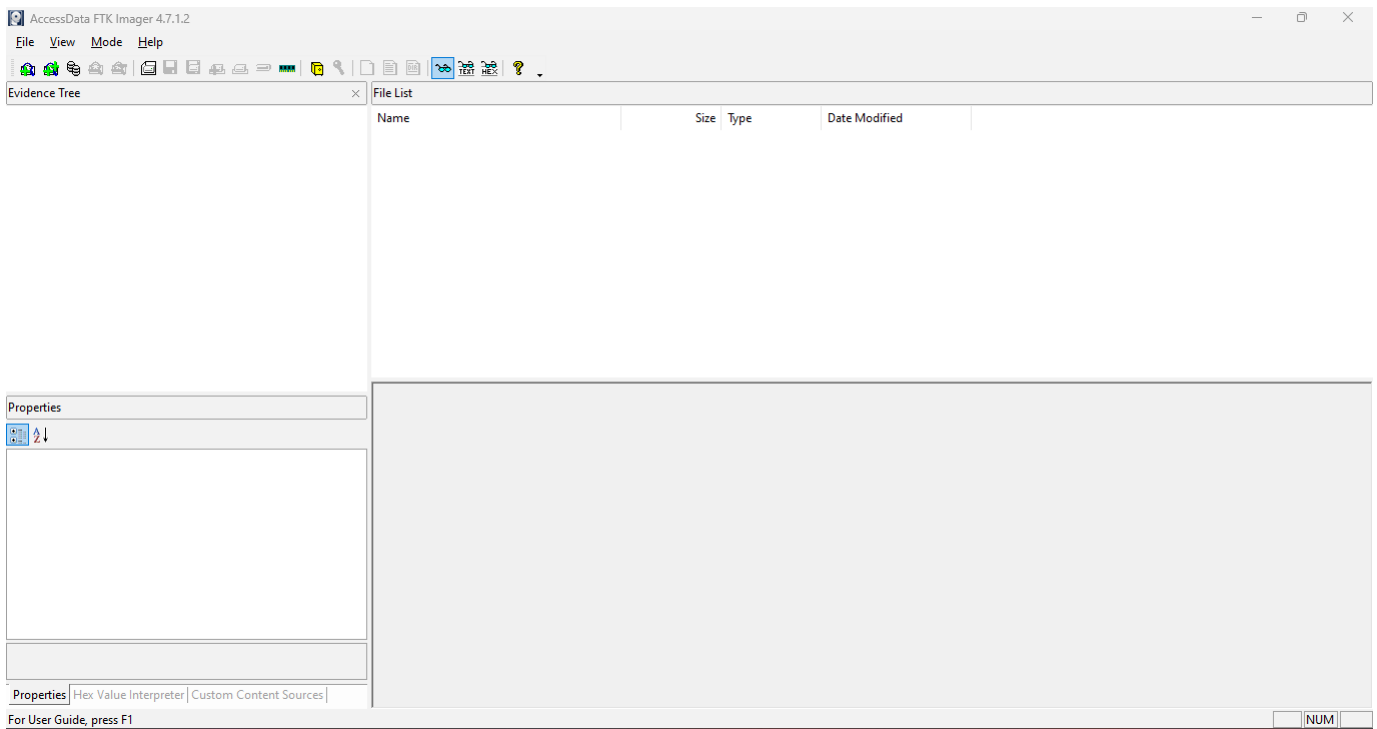
C. Preserving Evidence

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.

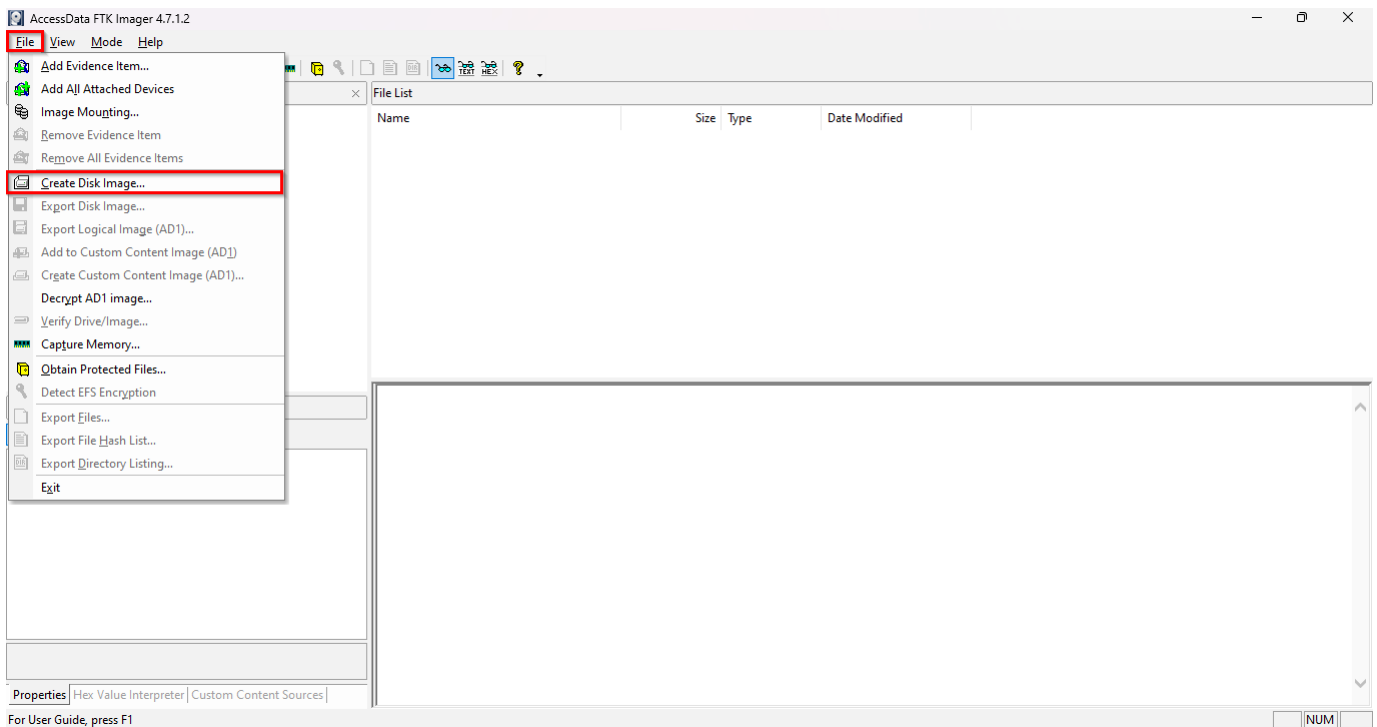
D. Method to Preserve Evidence

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

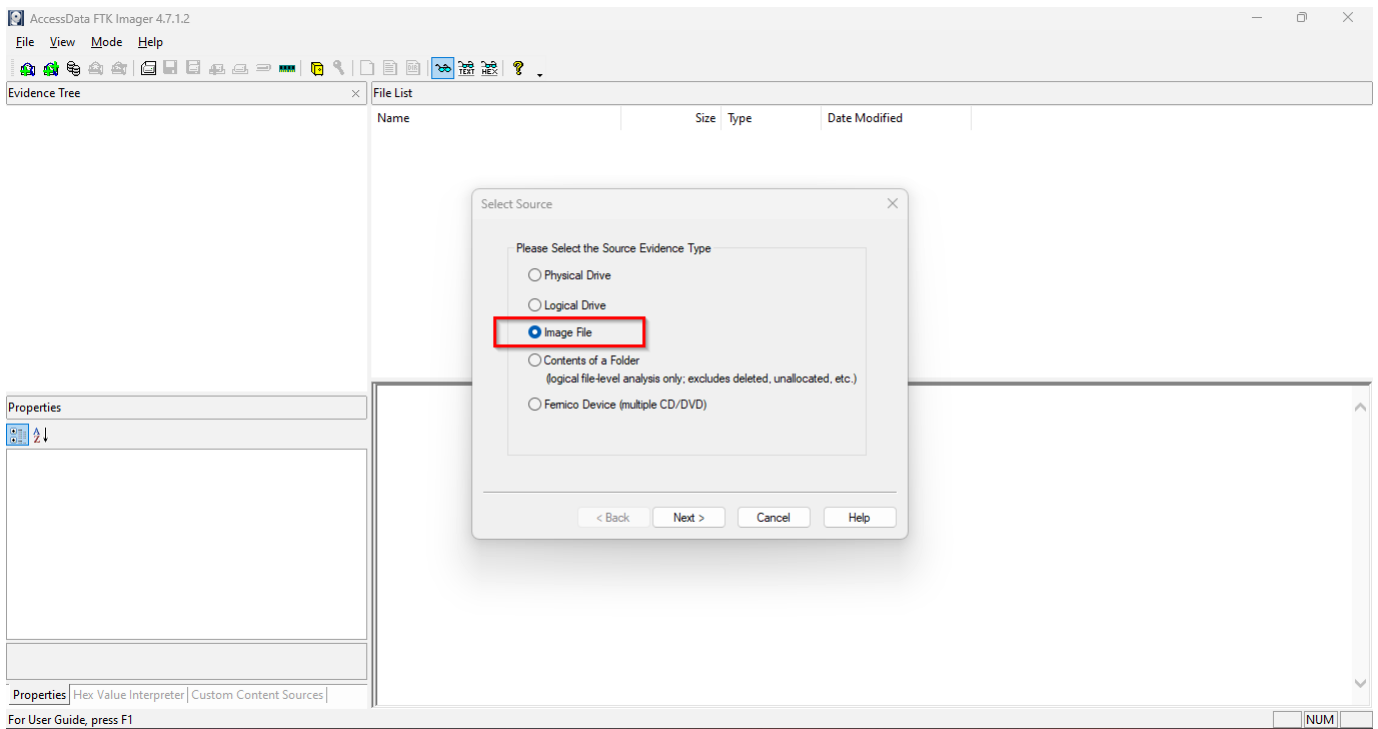
- Open FTK Imager tool.



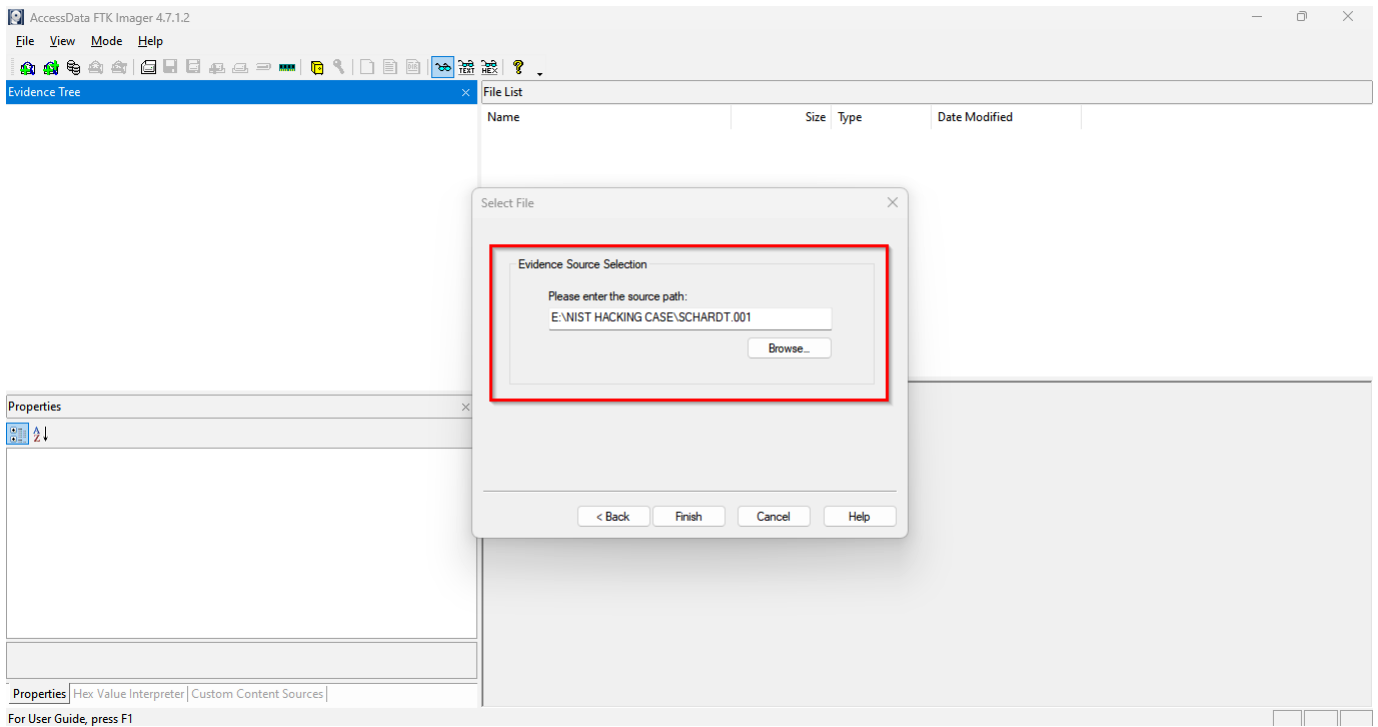
- Go to File — Create Disk Image:



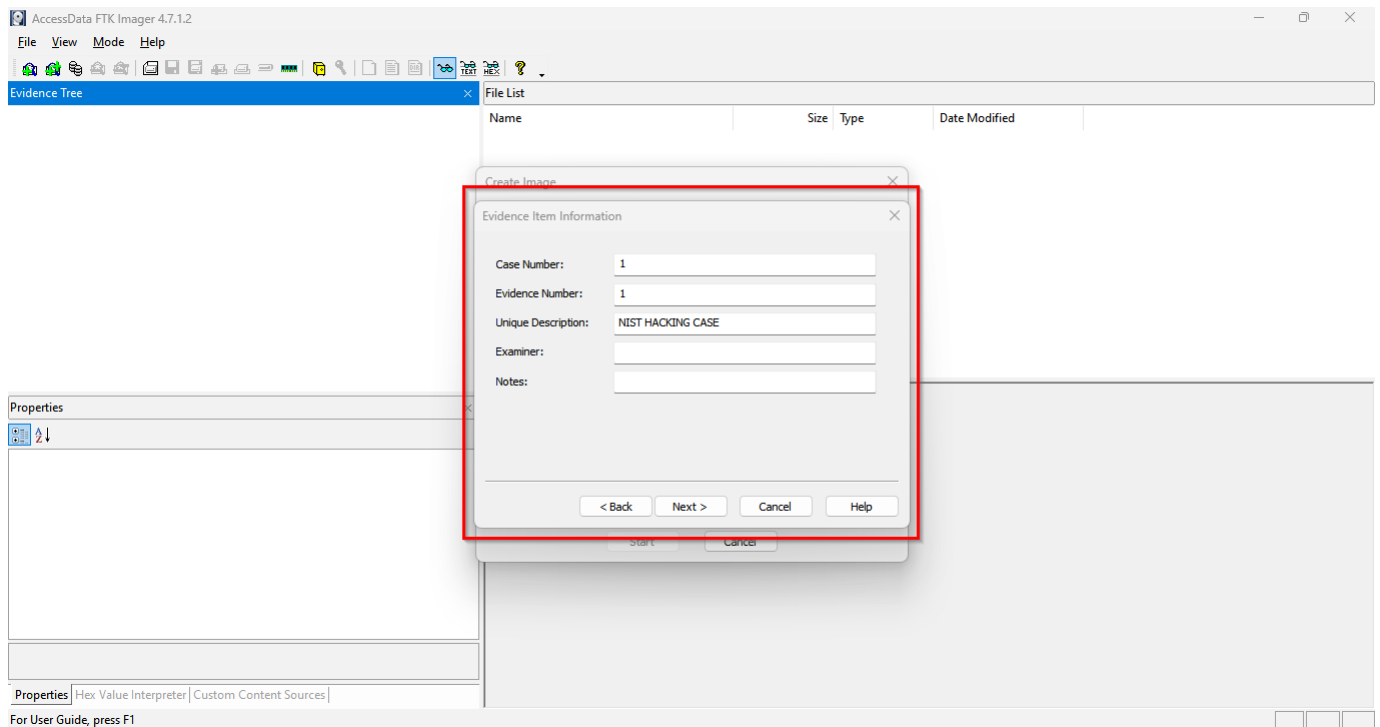
- Select Image File option.



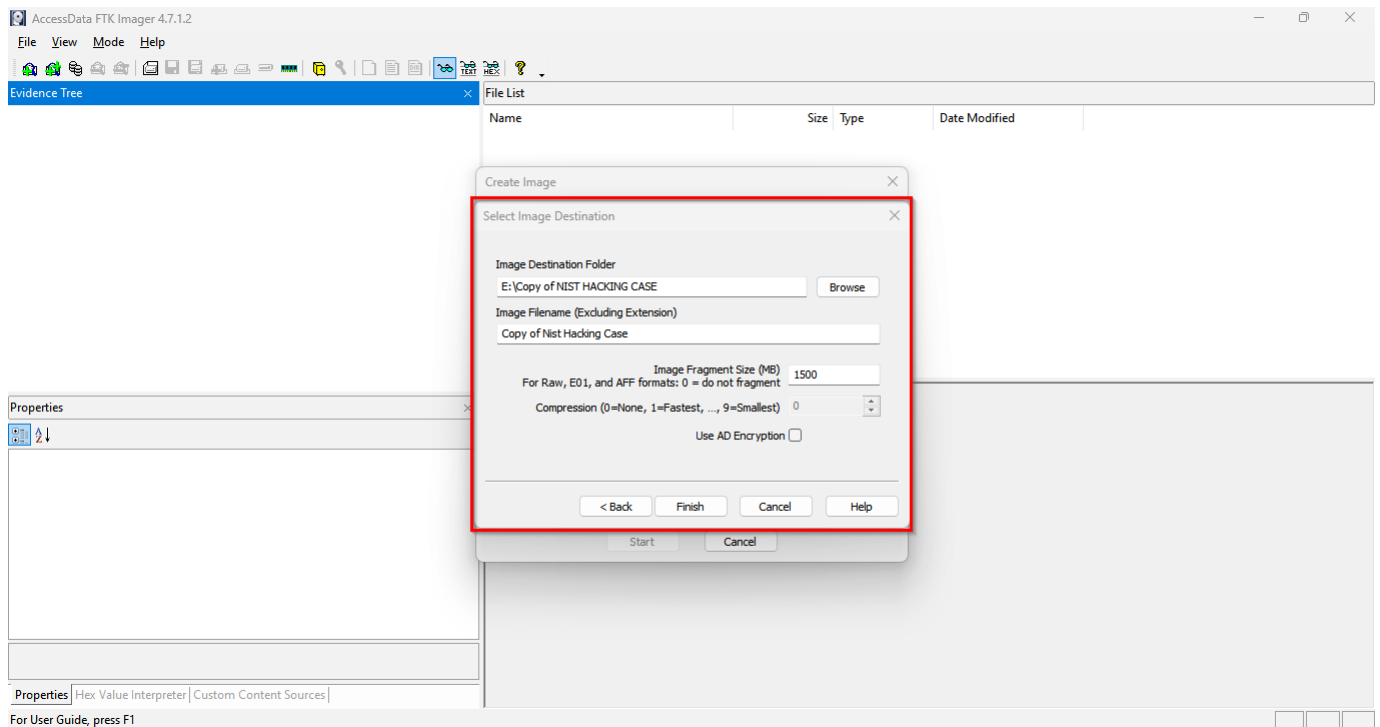
- Add the original image file.



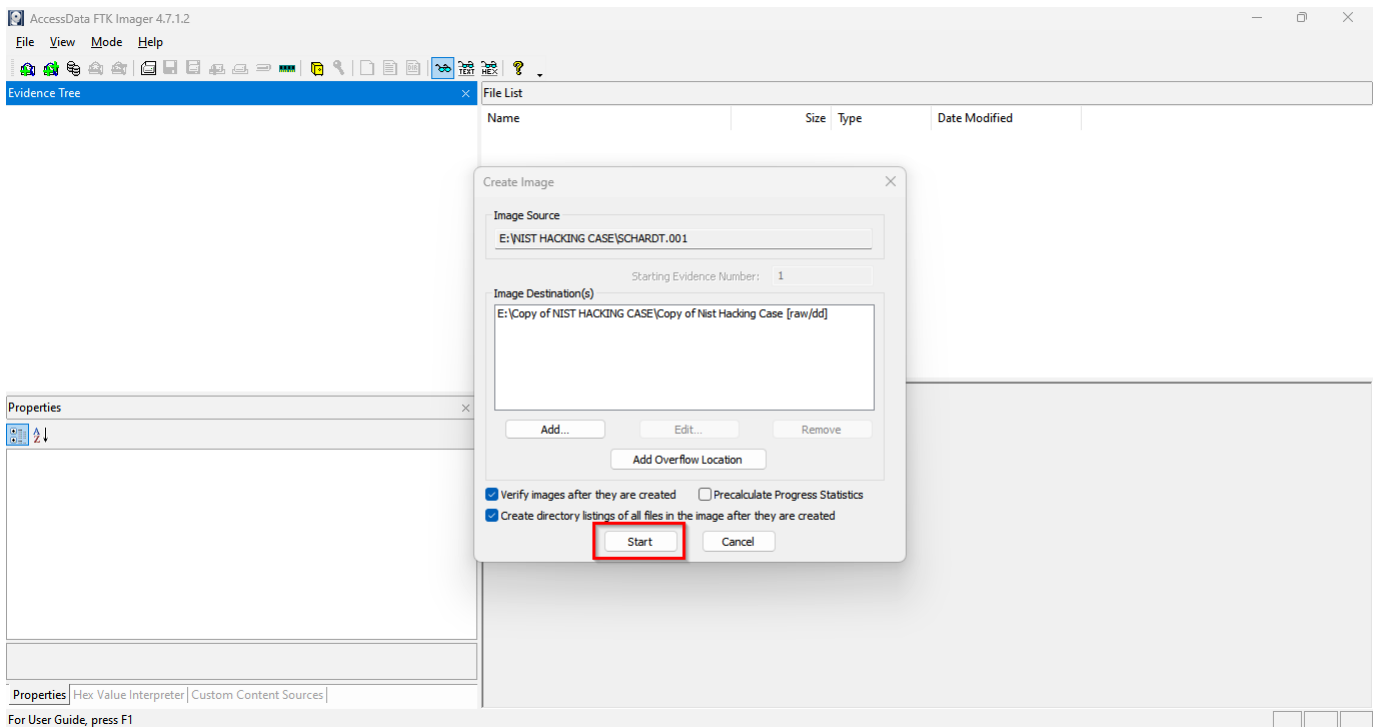
- Add the important necessary information.



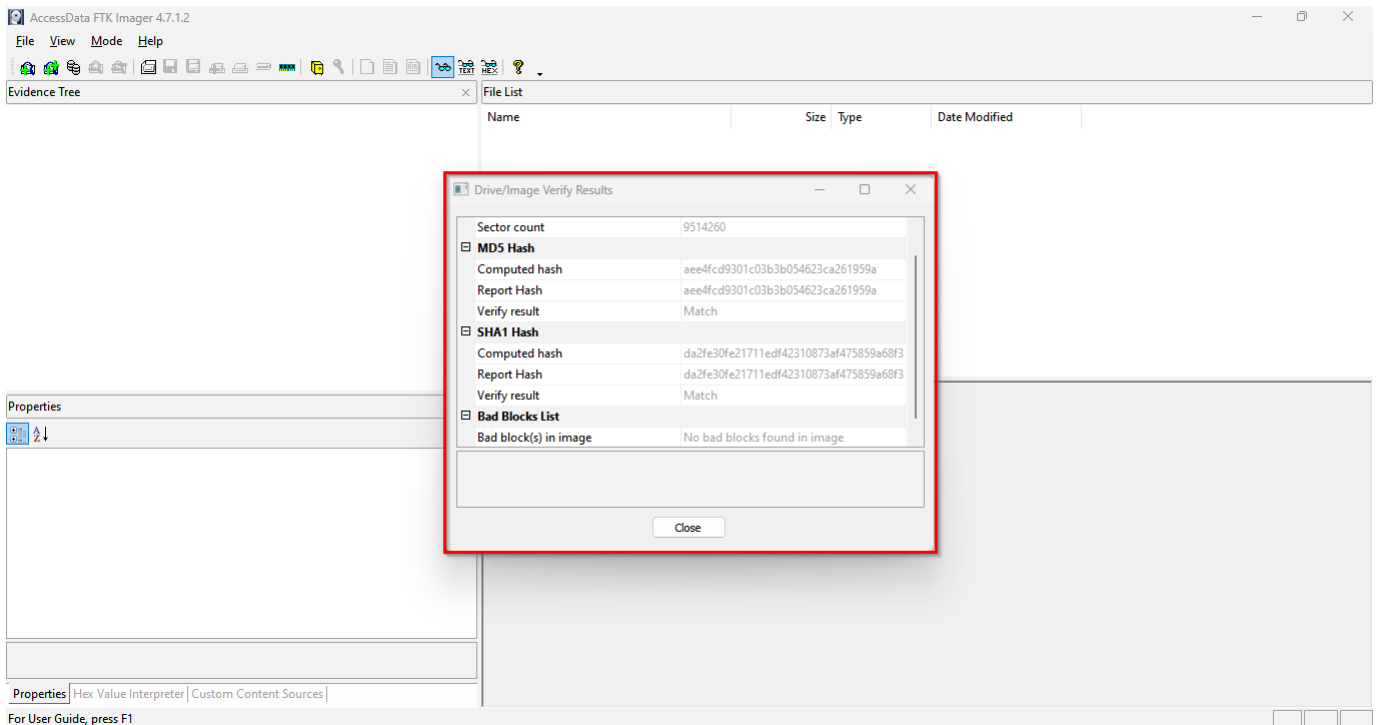
- Add image destination file.



- 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: aee4fcd9301c03b3b054623ca261959a

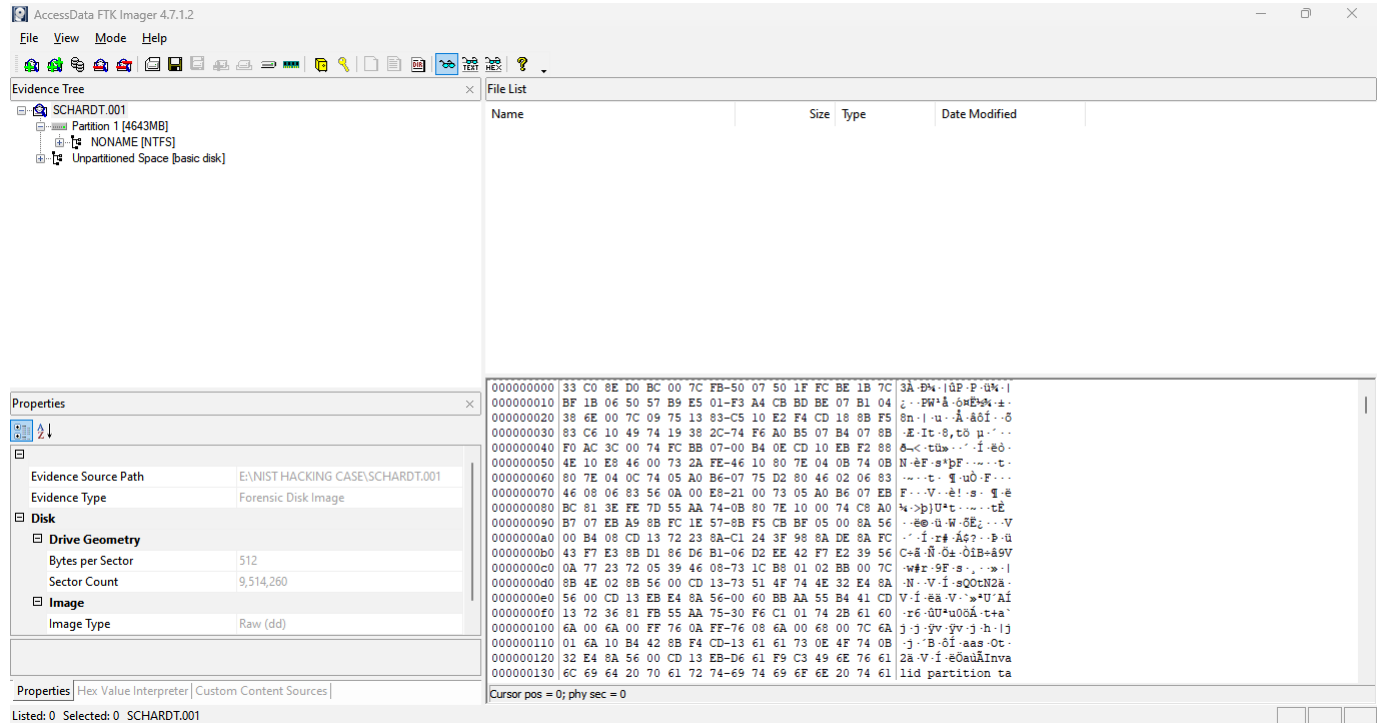
Copying Image hash: aee4fcd9301c03b3b054623ca261959a

III. TOOLS USED

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

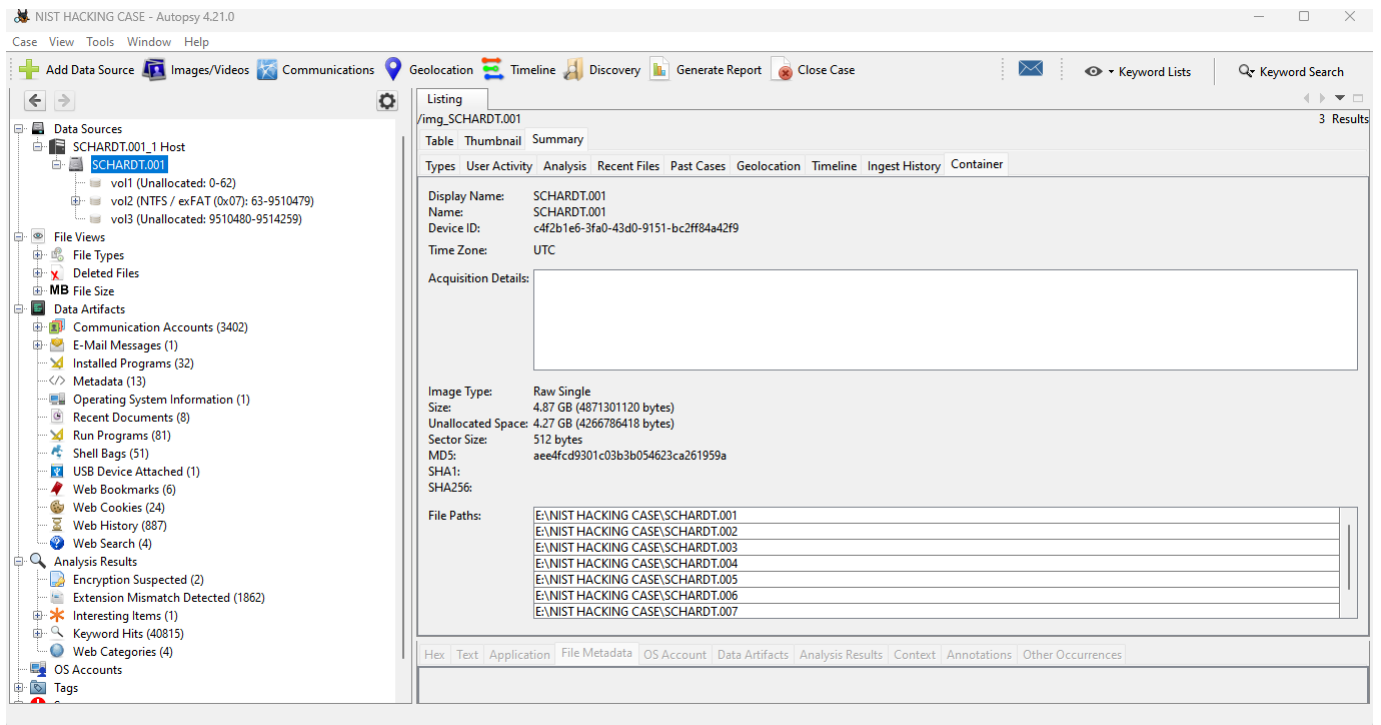
A. FTK imager

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).



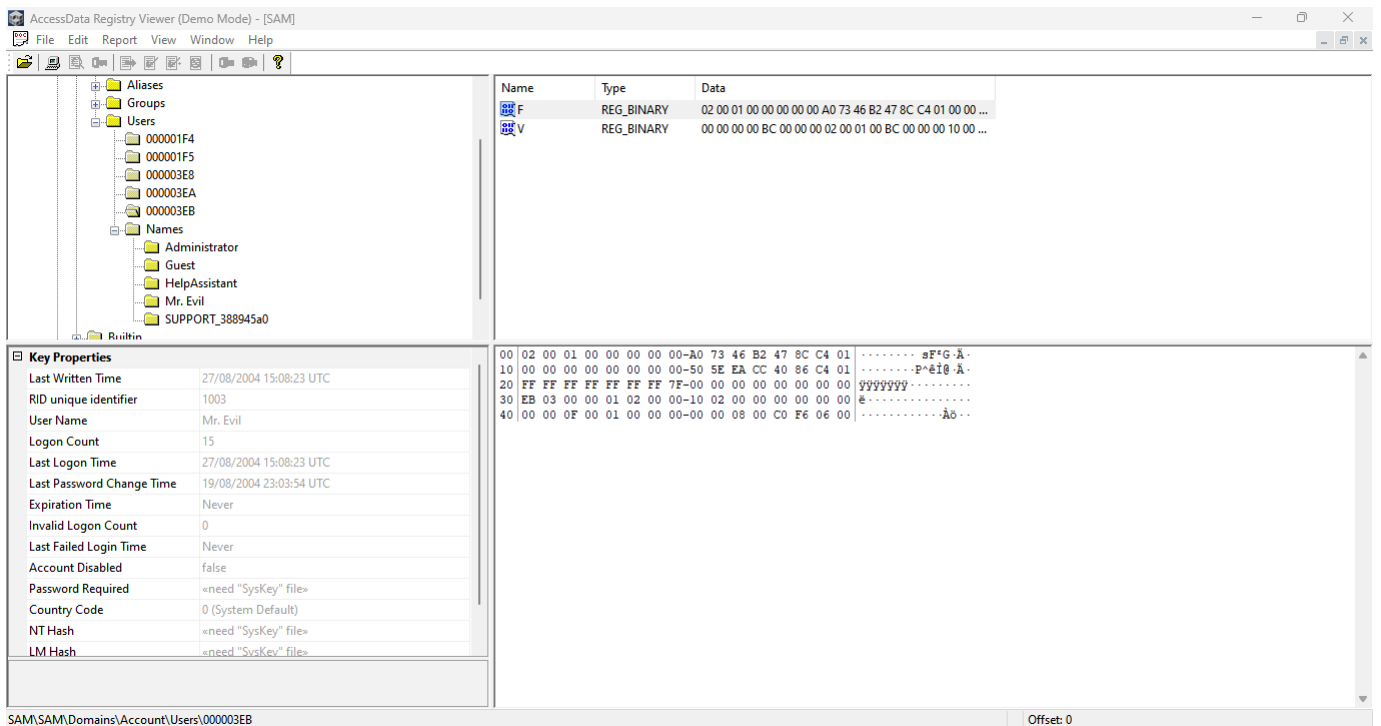
B. Autopsy

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).



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).



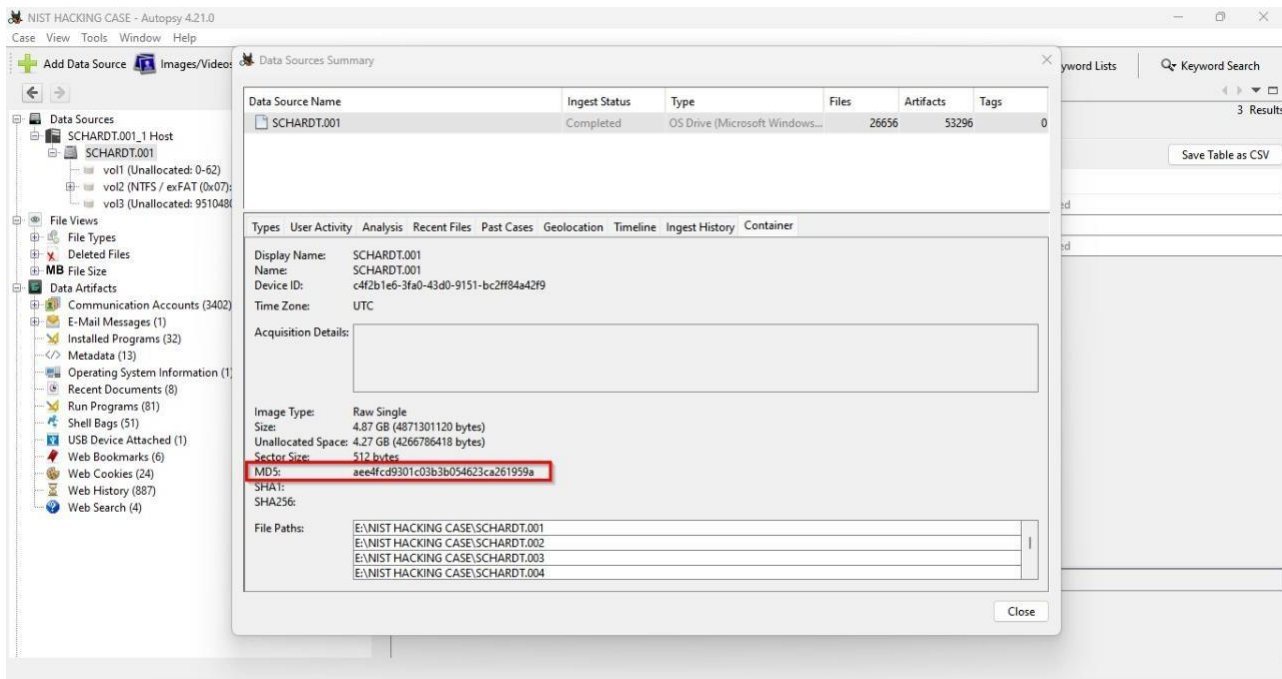
IV. EVIDENCE IDENTIFICATION, ANALYSIS, AND FINDINGS

Q1. Image Hash

MD5: aee4fcd9301c03b3b054623ca261959a

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 displays the NIST Hacking Case - Autopsy 4.21.0 interface. The left sidebar shows a tree view of data sources, with 'Operating System Information (1)' highlighted under 'Data Artifacts'. The main pane shows a table of 'Operating System Information' with one result. Below the table, a detailed view of the artifact is shown, with 'Program Name' highlighted as 'Microsoft Windows XP'.

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID
SCHARDT.001				N-1A9ODN6ZXX4LQ	Microsoft Windows XP	x86	%SystemRoot%\TEMP	C:\WINDOWS	55274-640-01

Type	Value	Source(s)
Name	N-1A9ODN6ZXX4LQ	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_SCHARDT.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 NIST Hacking Case - Autopsy 4.21.0 interface. The file system tree on the left shows the path: system32 (1794) > config (23) > software (23). The main pane displays a table of registry values for the path /img_SCHARDT.001/vol2/WINDOWS/system32/config. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The 'software' entry is highlighted, and its details are shown in the right pane. The 'CurrentVersion' key is expanded, and the 'InstallDate' value is highlighted, showing the hex value 0x41252e3b (1092955707).

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
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.LOG			1	2004-08-27 16:46:32 BST	2004-08-27 16:46:32 BST	2004-08-27 16:46:32 BST	2004-08-19 17:56:08 BST	1024	Allocated

The 'CurrentVersion' key details show the following values:

Name	Type	Value
CurrentBuild	REG_SZ	1.511.1.0 (Obsolete data - do not use)
InstallDate	REG_DWORD	0x41252e3b (1092955707)
ProductName	REG_SZ	Microsoft Windows XP
RegDone	REG_SZ	(value not set)
RegisteredOrganization	REG_SZ	N/A
RegisteredOwner	REG_SZ	Greg Schardt
SoftwareType	REG_SZ	SYSTEM
CurrentVersion	REG_SZ	5.1
CurrentBuildNumber	REG_SZ	2600
BuildLab	REG_SZ	2600.xpclient.010817-1148
CurrentType	REG_SZ	Uniprocessor Free
SystemRoot	REG_SZ	C:\WINDOWS
SourcePath	REG_SZ	D:\

After converting it into UTC Standard.

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

```
Windows PowerShell
PS C:\> (Get-Date -Date '1970-01-01 00:00:00').AddSeconds(1092955707)

Thursday, August 19, 2004 10:48:27 PM

PS C:\>
```

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 NIST Hacking Case - Autopsy 4.21.0 interface. The left pane displays a file system tree with the following structure:

- msapps (3)
- mui (2)
- Offline Web Pages (3)
- PCHEALTH (4)
- Prefetch (84)
- Registration (8)
- repair (12)
- Resources (3)
- security (11)
- srchasst (8)
- system (27)
- 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)

The right pane shows the file path `/img_SCHARDT.001/vol2/WINDOWS/system32/config` with 23 results. A table lists the files:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
system			1	2004-08-27 16:46:33 BST	2004-08-27 16:31:44 BST	2004-08-27 16:46:33 BST	2004-08-19 17:56:06 BST	2621440	Allocated
system.LOG			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 17:56:08 BST	1024	Allocated
system.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	389120	Allocated
TemnKey.LOG			1	2004-08-19 17:56:18 RST	2004-08-19 18:02:15 RST	2004-08-19 01:00:00 RST	2004-08-19 17:56:14 RST	1024	Allocated

The 'system' file is selected, and the 'TimeZoneInformation' registry value is highlighted in the 'Application' pane. The 'Metadata' pane shows the following details:

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

The 'Values' table lists the registry 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	0xffffffff (4294967295)
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 NIST Hacking Case - Autopsy 4.21.0 interface. The left sidebar displays a tree view of data sources, with 'Operating System Information (1)' highlighted. The main pane shows a table of results for 'Operating System Information'.

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	55274-640-0147306-23684

Below the table, the 'Data Artifacts' tab is selected, showing a detailed view of the 'Operating System Information' artifact. The 'Owner' field is highlighted with a red box.

Type	Value	Source(s)
Name	N-1A90DN6ZXK4LQ	Recent Activity
Program Name	Microsoft Windows XP	Recent Activity
Processor Arch	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-1A9ODN6ZXK4LQ

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

The screenshot displays the NIST Hacking Case - Autopsy 4.21.0 interface. The left sidebar shows a tree view of data sources, with 'Operating System Information (1)' highlighted under 'Data Artifacts'. The main pane shows a table of Operating System Information for source 'SCHARDT.001'. The table includes columns for Source Name, S, C, O, Name, Program Name, Processor Architecture, Temporary Files Directory, Path, and Product ID. Below the table, a detailed view of the Operating System Information is shown, with the 'Name' field highlighted, displaying 'N-1A9ODN6ZXK4LQ'.

Source Name	S	C	O	Name	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID
SCHARDT.001				N-1A9ODN6ZXK4LQ	Microsoft Windows XP	x86	%SystemRoot%\TEMP	C:\WINDOWS	55274-640-0147306-23684

Type	Value	Source(s)
Name	N-1A9ODN6ZXK4LQ	Recent Activity
Program Name	Microsoft Windows XP	Recent Activity
Processor Arch	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 displays the NIST HACKING CASE - Autopsy 4.21.0 interface. The left sidebar shows a file system tree with 'config (23)' selected. The center pane shows a table of files in the path '/img_SCHARDT.001_vol2/WINDOWS/system32/config'. The right pane shows the 'Winlogon' registry 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 16:29:44 BST	2004-08-27 16:46:33 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	2004-08-27 16:46:32 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
SvcEvent-Fut			1	2004-08-27 16:46:29 RST	2004-08-27 16:46:29 RST	2004-08-27 16:46:29 RST	2004-08-19 17:59:15 RST	65536	Allocated

Name	Type	Value
AutoRestartShell	REG_DWORD	0x00000001 (1)
DefaultDomainName	REG_SZ	N-1A9ODN6ZXK4LQ
DefaultUserName	REG_SZ	Mr. Evil
LegalNoticeCaption	REG_SZ	(value not set)
LegalNoticeText	REG_SZ	(value not set)
PowerdownAfterShutdown	REG_SZ	0
ReportBootOk	REG_SZ	1
Shell	REG_SZ	Explorer.exe
ShutdownWithoutLogon	REG_SZ	0
System	REG_SZ	(value not set)
Userinit	REG_SZ	C:\WINDOWS\system32\userinit.exe
VmApplet	REG_SZ	rundll32 shell32.Control_RunDLL "sysdm.cpl"
StcQuota	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 NIST Hacking Case - Autopsy 4.21.0 interface. The left pane displays a file system tree with the following structure:

- security (11)
- srcasht (8)
- system (27)
- 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)

The right pane shows a table of files for the path `/img_SCHARDT.001/vol2/WINDOWS/system32/config`. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The files listed are:

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 16:29:44 BST	2004-08-27 16:46:33 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	2004-08-27 16:46:32 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
SvcEvent.Fvt			1	2004-08-27 16:46:29 RST	2004-08-27 16:46:29 RST	2004-08-27 16:46:29 RST	2004-08-19 17:59:15 RST	65536	Allocated

Below the table, the 'ExitTime' registry value is highlighted in the Prefetcher folder. The metadata for 'ExitTime' is shown in a box:

```

Metadata
Name: ExitTime
Type: REG_SZ
Value
2004/08/27-10:46:27
  
```

Q9. Total OS Accounts

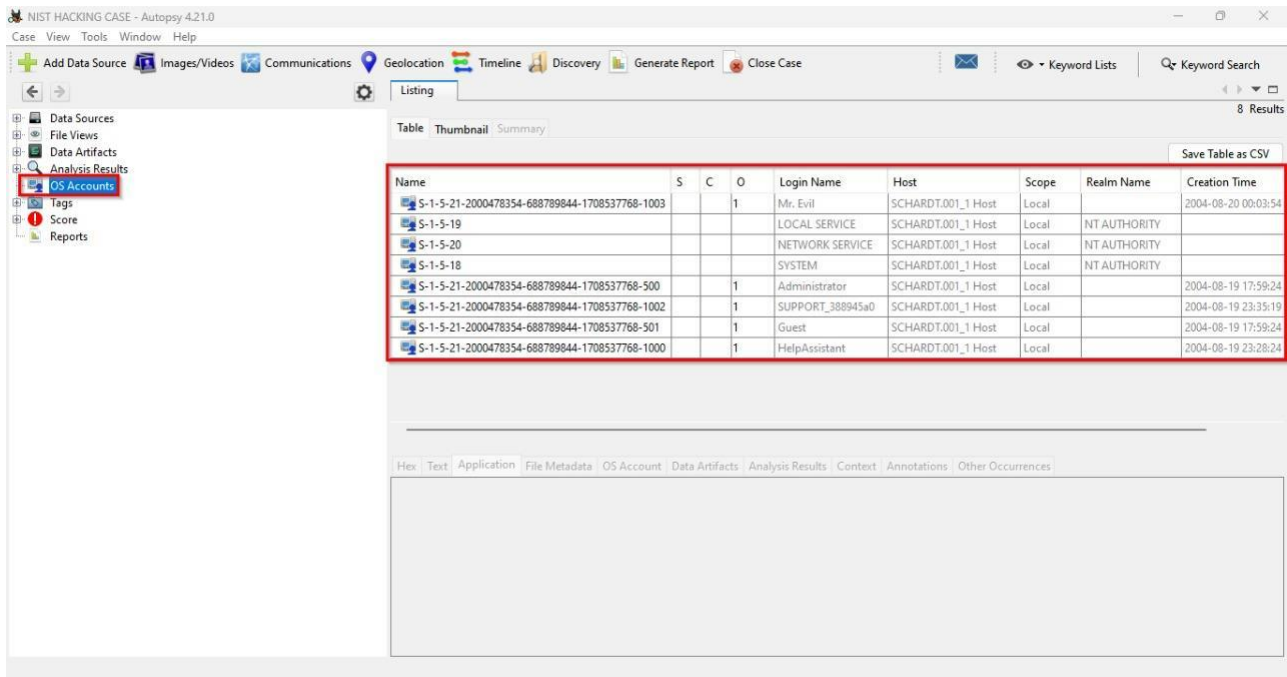
Accounts: 5

- 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 'OS Accounts' selected and highlighted with a red box. The main window displays a table of OS accounts. The table has columns: Name, S, C, O, Login Name, Host, Scope, Realm Name, and Creation Time. There are 8 results shown. The table is outlined with a red border.

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		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		2004-08-19 17:59:24
S-1-5-21-2000478354-688789844-1708537768-1002			1	SUPPORT_388945a0	SCHARDT.001_1 Host	Local		2004-08-19 23:35:19
S-1-5-21-2000478354-688789844-1708537768-501			1	Guest	SCHARDT.001_1 Host	Local		2004-08-19 17:59:24
S-1-5-21-2000478354-688789844-1708537768-1000			1	HelpAssistant	SCHARDT.001_1 Host	Local		2004-08-19 23:28:24

At the bottom of the interface, there is a tab bar with the following tabs: Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'OS Account' tab is currently selected.

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 (Demo Mode) interface. The left pane displays the tree structure of the SAM database, with the 'Users' folder expanded. The right pane shows the 'Key Properties' for the selected user, 'Mr. Evil' (RID 1003). The properties include:

- 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)
- NT Hash: <need "SysKey" file>
- LM Hash: <need "SysKey" file>

The bottom status bar shows the path: SAM\SAM\Domains\Account\Users\000003EB and the offset: 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 displays the NIST Hacking Case - Autopsy 4.21.0 interface. The left pane shows a file system tree with the path: system32 (1794) > config (23) > Software > Microsoft > WindowsNT > CurrentVersion > Winlogon. The right pane shows a table of files in the directory /img_SCHARDT.001/vol2/WINDOWS/system32/config. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The file 'DefaultUserName' is highlighted in the table, and its details are shown in the right 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 16:29:44 BST	2004-08-27 16:46:33 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	2004-08-27 16:46:32 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 16:31:44 BST	2004-08-27 16:46:33 BST	2004-08-19 17:56:06 BST	2621440	Allocated

The 'DefaultUserName' registry value is highlighted in the table, and its details are shown in the right pane:

```

Metadata
Name: DefaultUserName
Type: REG_SZ
Value
Mr. Evil
  
```


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 displays the Autopsy 4.21.0 interface with a keyword search for "Greg Schardt". The search results table is as follows:

Name	Keyword Preview	Location	Modified Time
Unalloc_20051_351232_1683209728	REG_SZValue data = «Greg Schardt«(On Error) User no	/img_SCHARDT.001/vol_vol2/\$Unalloc/Unalloc_20051...	0000-00-00 00:00
Unalloc_20051_1684736000_3639811072	Companyil SoName«Greg Schardt«C:\WINDOWS\Syst...	/img_SCHARDT.001/vol_vol2/\$Unalloc/Unalloc_20051...	0000-00-00 00:00
irunin.ini	HT%«600%REGOWNER%««Greg Schardt«%REGORGA...	/img_SCHARDT.001/vol_vol2/Program Files/Look@LA...	2004-08-25 16:16
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 16:16
b0019813.ppt	Companyil SoName«Greg Schardt«C:\WINDOWS\Syst...	/img_SCHARDT.001/vol_vol2/\$CarvedFiles/1/b001981...	0000-00-00 00:00
drwtsn32.log	Registered Owner: «Greg Schardt«*«««« Task List ««««	/img_SCHARDT.001/vol_vol2/Documents and Settings...	2004-08-20 16:16
Operating System Information Artifact	306-23684Owner: «Greg Schardt«Organization: N/A	SCHARDT.001	
software	OoRegisteredOwner«Greg Schardt«26008x«CurriSoft	/img_SCHARDT.001/vol_vol2/WINDOWS/repair/softw...	2004-08-19 23:16
software	Companyil SoName«Greg Schardt«C:\WINDOWS\Syst...	/img_SCHARDT.001/vol_vol2/WINDOWS/system32/co...	2004-08-27 16:16
AppEvent.Evt	Registered Owner: «Greg Schardt«*«««« Task List ««««	/img_SCHARDT.001/vol_vol2/WINDOWS/system32/co...	2004-08-27 16:16
f0256874.txt	REG_SZValue data = «Greg Schardt«(On Error) User no	/img_SCHARDT.001/vol_vol2/\$CarvedFiles/1/f0256874...	0000-00-00 00:00

Below the table, the extracted text from the selected file 'irunin.ini' is displayed:

```
%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

NIST HACKING CASE - Autopsy 4.21.0

Case View Tools Window Help

Keyword search 1 - Greg Schardt x

Listing: /img_SCHARDT.001/vol2/WINDOWS/system32/config

Table Thumbnail Summary

23 Results

Save Table as CSV

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

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

Image File Execution Options

IME Compatibility

IMM

IniFileMapping

LanguagePack

LastFontSweep

MCI

MCI Extensions

MCI32

Midimap

ModuleCompatibility

Network

NetworkCards

OpenGLDrivers

Perflib

PerHwldStorage

Ports

Prefetcher

Print

Metadata

Name: 2

Number of subkeys: 0

Number of values: 2

Modification Time: 2004-08-19 17:07:19 GMT+00:00

Name	Type	Value
ServiceName	REG_SZ	{6F4090C2-F4FF-499A-B575-505D71EC1049}
Description	REG_SZ	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 NIST Hacking Case - Autopsy 4.21.0 interface. The left sidebar displays a tree view of data sources, including 'Data Sources', 'File Views', 'Data Artifacts', and 'Analysis Results'. The main window shows a search for 'greg schardt' with 11 results. A table lists the search results, with the following data:

Source Name	S	C	O	Keyword Preview	Keyword	Modified Time	Access Time
Unalloc_20051_351232_1683209728				REG_SZValue data = «Greg Schardt«(On Error) User no	greg schardt	0000-00-00 00:00:00	0000-00-00
irunin.ini			1	HT%=<600%REGOWNER%=<«Greg Schardt%REGORGA...	greg schardt	2004-08-25 16:56:10 BST	2004-08-25
Unalloc_20051_1684736000_3639811072				Companyil SoName=<Greg Schardt«C:\WINDOWS\Syst...	greg schardt	0000-00-00 00:00:00	0000-00-00

Below the table, the 'Text' tab is selected, showing the contents of the 'irunin.ini' file. The file is a configuration file for 'Look@LAN' with various settings. The following lines are highlighted in red:

```
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
```

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.

The screenshot shows the 'macaddress.io' website interface. At the top, there's a navigation bar with links like 'Database Download', 'Lookup', 'API', 'Generator', 'Statistics', 'FAQ', 'Login', and 'Sign up'. Below the navigation bar, the main content area displays '00:10:a4:93:3e:09 MAC address details'. A search bar with the placeholder 'MAC address or OUI' and a 'New search' button is visible. The details are organized into three columns: 'Vendor details', 'Block details', and '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		

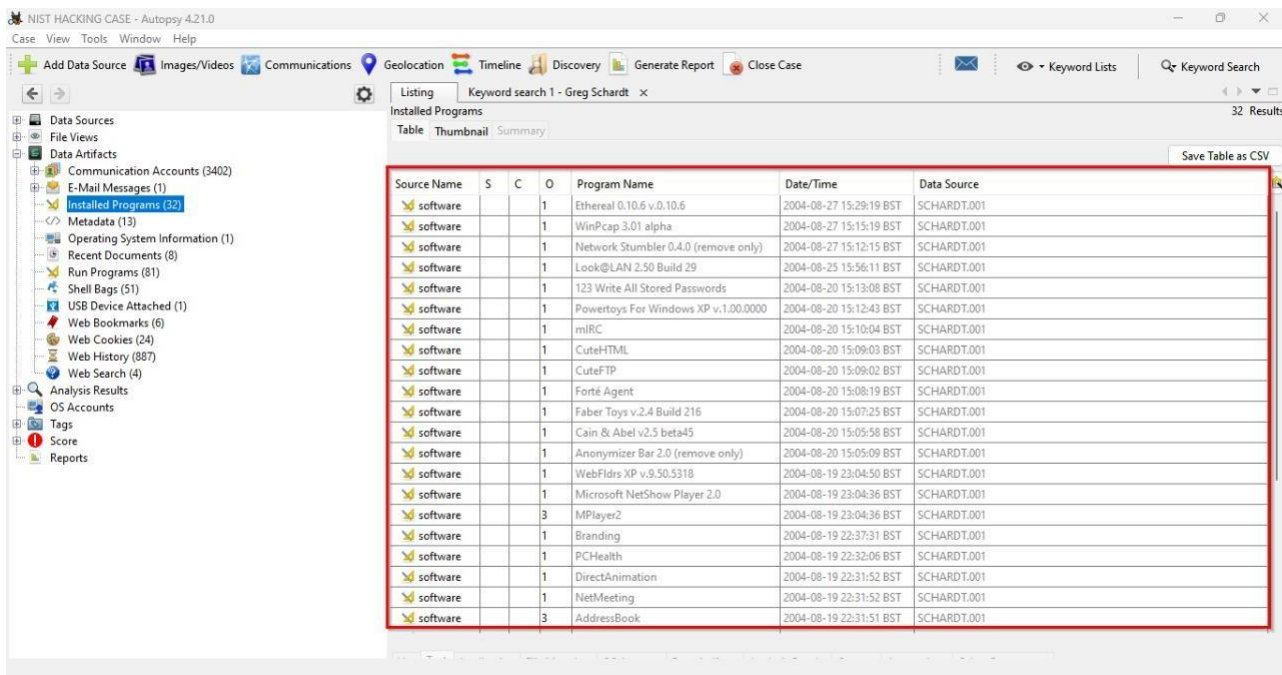
Below the details, there is a section for 'OUI changes history'.

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 selected. The table lists various software artifacts found on the system, including network tools, password recovery utilities, and communication clients. The table is filtered by the keyword 'Greg Schardt'.

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 15:13:08 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	WebFldrs 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	NetMeeting	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 NIST Hacking Case - Autopsy 4.21.0 interface. On the left, the file system tree is expanded to show the path: SCHARDT.001_1 Host > SCHARDT.001 > vol2 (NTFS / exFAT (0x07): 63-9510479) > Program Files (36) > Agent (20) > Data (36). The file 'Agent.ini' is highlighted in the tree. On the right, the 'Listing' pane shows a table of files, with 'AGENT.INI' selected. Below the table, the 'Text' pane displays the contents of 'AGENT.INI', which includes configuration details for the Forte Agent SMTP client. Red boxes highlight the following information in the text pane:

- FullNames="Mr Evil"
- EmailAddress="whoknowsme@sbcglobal.net"
- UserName="whoknowsme@sbcglobal.net"
- Password="84106D94696F"

The text pane also shows other configuration details such as SMTPLoginProtocol=2, SMTPUsePOPLogin=0, SMTPUserName="whoknowsme@sbcglobal.net", SMTPSavePassword=1, SMTPPassword="84106D94696F", and IsRegistered=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 – Data – Agent.ini

The screenshot shows the NIST Hacking Case - Autopsy 4.21.0 interface. The left pane displays the file system structure under 'SCHARDT.001_1 Host' > 'SCHARDT.001' > 'vol2' > 'Program Files' > 'Agent' > 'Data'. The file 'AGENT.INI' is highlighted. The right pane shows a table of search results for the keyword 'Greg Schardt'. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The file 'AGENT.INI' is listed with a size of 11309 bytes and is marked as 'Allocated'. Below the table, the 'Strings' tab is selected, showing the extracted text from the file. The text includes various settings for the NNTP server, with 'NewsServers="news.dallas.sbcglobal.net"' highlighted.

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
errorlog.txt			1	2004-08-20 20:47:30 BST	2004-08-20 20:47:30 BST	2004-08-20 20:47:30 BST	2004-08-20 20:45:44 BST	605	Allocated
FILTERS.DAT				2004-08-20 22:13:06 BST	2004-08-20 22:13:06 BST	2004-08-20 22:13:06 BST	2004-08-20 22:13:06 BST	0	Allocated
FILTERS.IDX				2004-08-20 22:13:06 BST	2004-08-20 22:13:06 BST	2004-08-20 22:13:06 BST	2004-08-20 22:13:06 BST	0	Allocated

Strings: Extracted Text Translation

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

Key=

EnableSupportMenu=0

ISearch=

NewsServers="news.dallas.sbcglobal.net"

MainServer= smtp.sbcglobal.net

POPServer=""

NNTPPort=119

SMTPPort=25

POPPort=110

SMTPServerPort=25

[Groups]

LastUpdate="25.August.2004 15:57:30 hrs"

RefreshMode=0

RecordGaps=0

DemonDolt=1

MinGapCount=5

SampleMode=0

SampleCount=50

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 NIST Hacking Case - Autopsy 4.21.0 interface. The left pane displays a file system tree with the path: system32 (1794) > config (23) > software. The right pane shows a table of search results for the keyword 'software' in the file 'software.LOG'. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The results show four files: software, software.LOG, software.sav, and SysEvent.Evt. The 'software' file is highlighted with a red box. Below the table, the 'Mail' folder is expanded in the file system tree, showing subfolders: Forte Agent, Hotmail, MSN Explorer, and Outlook Express. The 'Mail' folder is also highlighted with a red box. The right pane shows the metadata for the 'Mail' folder, including the name 'Mail', number of subkeys (4), number of values (1), and modification time (2004-08-20 19:45:44 GMT+00:00). The 'Values' section shows a table with columns: Name, Type, and Value. The table contains one entry: (Default), REG_SZ, Outlook Express.

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 16:29:44 BST	2004-08-27 16:46:33 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	2004-08-27 16:46:32 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

Name	Type	Value
(Default)	REG_SZ	Outlook Express

Q20. Subscribed Newsgroups

Newsletters:

- 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

The screenshot shows the NIST Hacking Case - Autopsy 4.21.0 interface. On the left, the file tree displays the hierarchy of the case, with 'Outlook Express (31)' highlighted under the 'Microsoft' folder. On the right, a table lists the files found in the Outlook Express folder. The table has columns for Name, S, C, O, Modified Time, Change Time, Access Time, and Created Time. The files listed include various .dbx files, such as 'alt.2600.cardz.dbx', 'alt.2600.codez.dbx', 'alt.2600.crackz.dbx', and others, all of which are marked as '1' in the S, C, and O columns.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2004-08-20 22:14:23 BST	2004-08-20 22:14:23 BST	2004-08-20 22:15:52 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	1	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	1	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 22:18:44 BST
alt.2600.crackz.dbx	1	1	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.dbx	1	1	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 22:18:32 BST
alt.2600.hackerz.dbx	1	1	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	1	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	1	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	1	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	1	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	1	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	1	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	1	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	1	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	1	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	1	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	1	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 4.21.0 interface. In the left sidebar, the file tree is expanded to 'Program Files (36)' > 'mIRC (16)' > 'mirc.ini'. The main pane displays a table of files with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The file 'mirc.ini' is highlighted. Below the table, the 'Strings' tab is active, showing extracted text from the file. The text includes user settings and other configuration details.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
mirc.hlp			1	2004-08-20 16:09:56 BST	2004-08-20 16:09:56 BST	2004-08-20 16:09:56 BST	2004-08-20 16:09:56 BST	224213	Allocated
mirc.ini			1	2004-08-25 17:20:55 BST	2004-08-25 17:20:55 BST	2004-08-25 17:20:55 BST	2004-08-20 16:09:56 BST	5483	Allocated

Strings | Extracted Text | Translation

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

```

other:1,1,1,1,1,1
pos=20,20
(mirc)
user=Mini Me
email=none@of.ya
nick=Mr
anick=mrevilrulez
host=Undernet: US, CA, LosAngelesSERVER:losangeles.ca.us.undernet.org:6660GROUP:Undernet
[files]
servers=servers.ini
finger=finger.txt
urls=urls.ini
addrbk=addrbk.ini
[styles]
thin=1
font=1
hide=1
color=default
size=2
buttons=0

```

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 displays the NIST Hacking Case - Autopsy 4.21.0 interface. On the left, the 'Data Sources' tree shows the hierarchy: SCHARDT.001_1 Host > SCHARDT.001 > vol2 (NTFS / exFAT) > Documents and Settings > Mr. Evil (19). The 'Mr. Evil (19)' folder is selected and highlighted with a red box. The main pane shows a table of files for 'Mr. Evil'. The file 'interception' is highlighted with a red box. Below the table, the 'Strings' tab is active, showing extracted text from the file. The 'User-Agent' string is highlighted with a red box: 'User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)'.

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

Strings: Extracted Text Translation

Page: 1 of 5 Page Matches on page: - of - Match 100% Reset Text Source: File Text

P/1,1
GET /hm/folder.aspx HTTP/1.1
Accept: */*
UA-OS: Windows CE (Pocket PC) - Version 4.20
UA-color: color16
UA-pixels: 240x320
UA-CPU: Intel(R) PXA255
UA-Voice: FALSE
Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; c=1; MSPAuth=5vuMneQNFDH0sFvAbKrt*q6edOGfSSmKzi3IT1Cih6fdbNqQyPyqubrB97DYRuoTwoA5kp1Td3eTZ3TUIz45LQ\$; MSPPProf=5ynNj8z2mEi3KQzUnhBOK5dmrXWUam5W2H3bXqJgZE5uFZ7OFVldTd8rwZLfhQ88q*Sto5O8dUjp8ulXjB5g4RjME!WBuVqwsUvAh8UuflyJMTMQT*6C4vjOyvqgDT5FIXAMjAg0vkYwzhbCKVIAO1b2zXmJIXnmPnOpETgsiPX0coWMOQ\$

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 displays the NIST Hacking Case - Autopsy 4.21.0 interface. On the left, the 'Data Sources' pane shows a file system structure for 'SCHARDT.001_1 Host'. The 'Documents and Settings' folder for 'Mr. Evil' is expanded, showing various subfolders like 'Application Data', 'Desktop', 'Favorites', etc. The main pane shows a 'Keyword search 8 - NewsGroups' results table. The table has columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The 'interception' file is highlighted in red. Below the table, the 'Text' tab is selected, showing the extracted text of the intercepted file. The text includes a 'Location' field with a URL: 'http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0'. This URL is also highlighted in red.

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

Text Source: File Text

Location: <http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0>

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

The screenshot shows the NIST Hacking Case - Autopsy 4.21.0 interface. The left sidebar displays a tree view of data sources, with 'Web History (887)' selected and highlighted by a red box. The main window shows the 'Web History' tab, which contains a table of browsing history. The table has columns for Source Name, S, C, O, Username, URL, and Date Accessed. The last row of the table is highlighted with a red box, showing a visit to 'http://us.f613.mail.yahoo.com/ym/Logout?YY=27630&first=1&inc=25&order=down&sort=date...' by 'Mr. Evil' on 2004-08-20 15:38:55. Below the table, the 'Strings' tab is active, showing a list of extracted text strings. One of the strings is 'Yahoo! Mail - mrevilrulez@yahoo.com', which is also highlighted with a red box. Other strings include various URLs and login/logout actions related to the same email address.

Source Name	S	C	O	Username	URL	Date Accessed
index.dat			2		http://us.i1.yimg.com/us.yimg.com/i/spacer.gif	2004-08-20 15:38:55
index.dat			5		http://login.yahoo.com/config/login?logout=1&src=ym&lg=us&intl=us&done=http%3a%2f...	2004-08-20 15:38:55
index.dat			2		http://us.i1.yimg.com/us.yimg.com/i/us/pim/b/mailma1.gif	2004-08-20 15:38:55
index.dat			5		http://login.yahoo.com/config/login?logout=1&src=ym&lg=us&intl=us&done=http%3a%2f...	2004-08-20 15:38:55
index.dat			5	Mr. Evil	http://us.f613.mail.yahoo.com/ym/Logout?YY=27630&first=1&inc=25&order=down&sort=date...	2004-08-20 15:38:55

Strings: Extracted Text Translation

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

URL
Visited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/login?.rand=7lrrdoi00f1k&first=1
Yahoo! Mail - mrevilrulez@yahoo.com
Visited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/ShowLetter?Search=&idx=0&YY=90802&first=1&order=down&sort=date&pos=0
URL
Visited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/ShowFolder?YY=78169&first=1&box=Inbox&YN=1
Yahoo! Mail - mrevilrulez@yahoo.com
URL
Visited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/Logout?YY=27630&first=1&inc=25&order=down&sort=date&pos=0&view=&head=&box=Inbox&YY=27630
/?!~
Visited: Mr. Evil@http://www.t50.com/extra.html
URL
Visited: Mr. Evil@http://www.elitehackers.com
== ELITEHACKERS.COM ==

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.

The screenshot displays the NIST Hacking Case - Autopsy 4.21.0 interface. The left sidebar shows a tree view of data sources, including Communication Accounts (3402), E-Mail Messages (1), and ShowLetter[1].htm. The main window shows a keyword search for 'mrevilrulez@yahoo.com' with 10 results. The first result is highlighted, showing the file 'ShowLetter[1].htm' and its location. Below the search results, a red box highlights the email content, which includes a welcome message from Yahoo Mail, a list of folders (Inbox, Draft, Sent, Trash), and a message body with the text 'It's smart. It works for you. Welcome to Yahoo! Mail.'

Keyword search 9 - mrevilrulez@yahoo.com

Name	Keyword Preview	Location	Modified Time	Change
ShowLetter[1].htm	calendar notepad «mrevilrulez@yahoo.com» [sign o...	/img_SCHARDT.001/vol_vol2/Documents and Settings...	2004-08-20 16:38:30 BST	2004-0

Download Images

Yahoo! My Yahoo! Mail

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

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

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

Choose from 10
Free Cell Phones

Folders[Add - Edit]

- Inbox
- Draft
- Sent
- Trash[Empty]

Check your Credit!

It's Free.

Free Checking w/

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

Delete Reply Forward Spam Move...

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

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

From:

Subject: Welcome to Yahoo!

To: mrevilrulez@yahoo.com

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

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

The screenshot shows the NIST Hacking Case - Autopsy 4.21.0 interface. The left sidebar displays the 'Data Sources' tree, with 'SCHARDT.001_1 Host' expanded, showing 'SCHARDT.001' and 'vol2 (NTFS / exFAT (0x07): 63-9510479)'. The 'Recycler' folder is highlighted. The main pane shows a table of files discovered in the Recycle Bin, with the following data:

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	2004-08-27 16:29:58 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			1	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			1	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.

The screenshot shows the NIST Hacking Case - Autopsy 4.21.0 interface. In the left-hand pane, under 'File Views', the 'Deleted Files' section is highlighted with a red box, showing 'File System (365)' and 'All (1375)'. The main pane displays a table of deleted files.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
✗ MPC7A4.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	Unallocate
✗ MPC7A5.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	Unallocate
✗ MPC7A6.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	Unallocate
✗ MPC7A7.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	Unallocate
✗ MPC7A8.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	Unallocate
✗ MPC7A9.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	Unallocate
✗ MPC7AA.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	Unallocate
✗ MPC7AB.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	Unallocate
✗ MPC7AC.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	Unallocate

The interface also includes a 'Save Table as CSV' button and a bottom pane with tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

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 altered during tranfer 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.