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

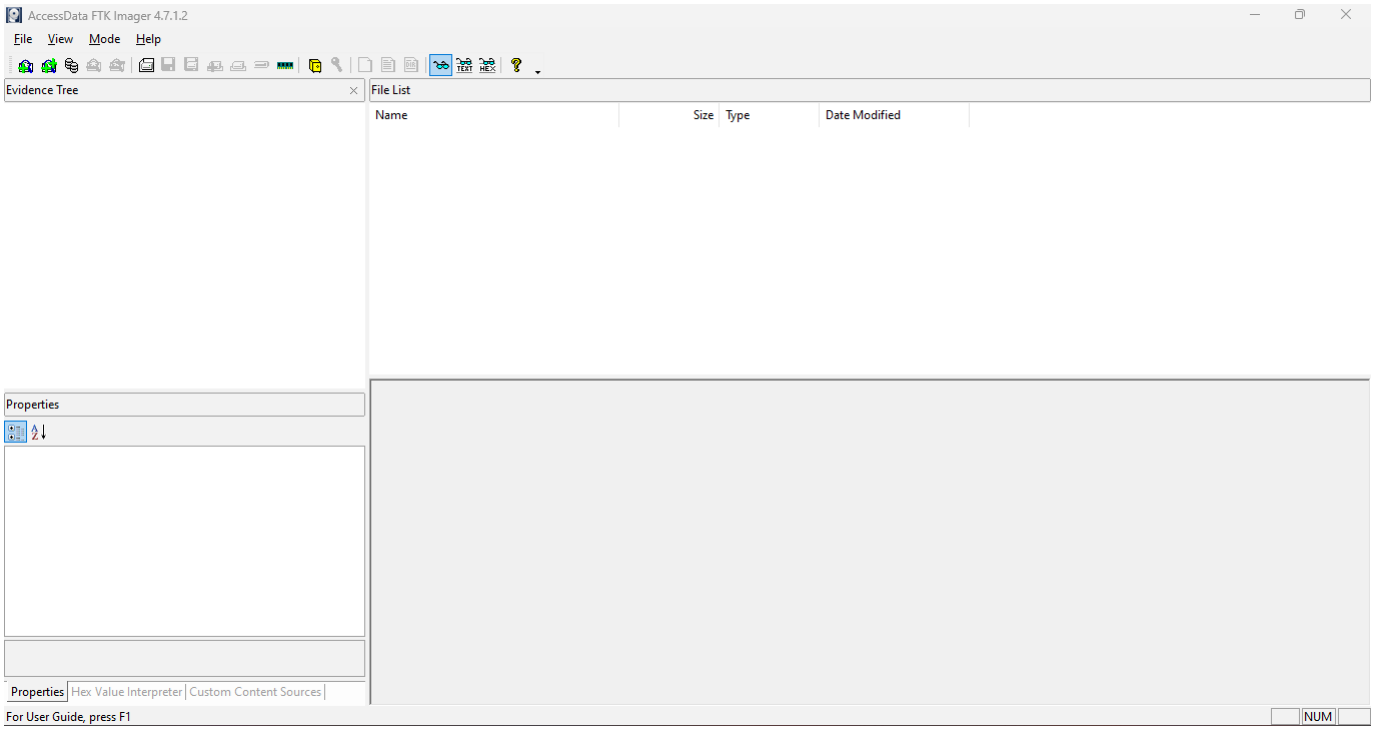
C. Preserving Evidence

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.

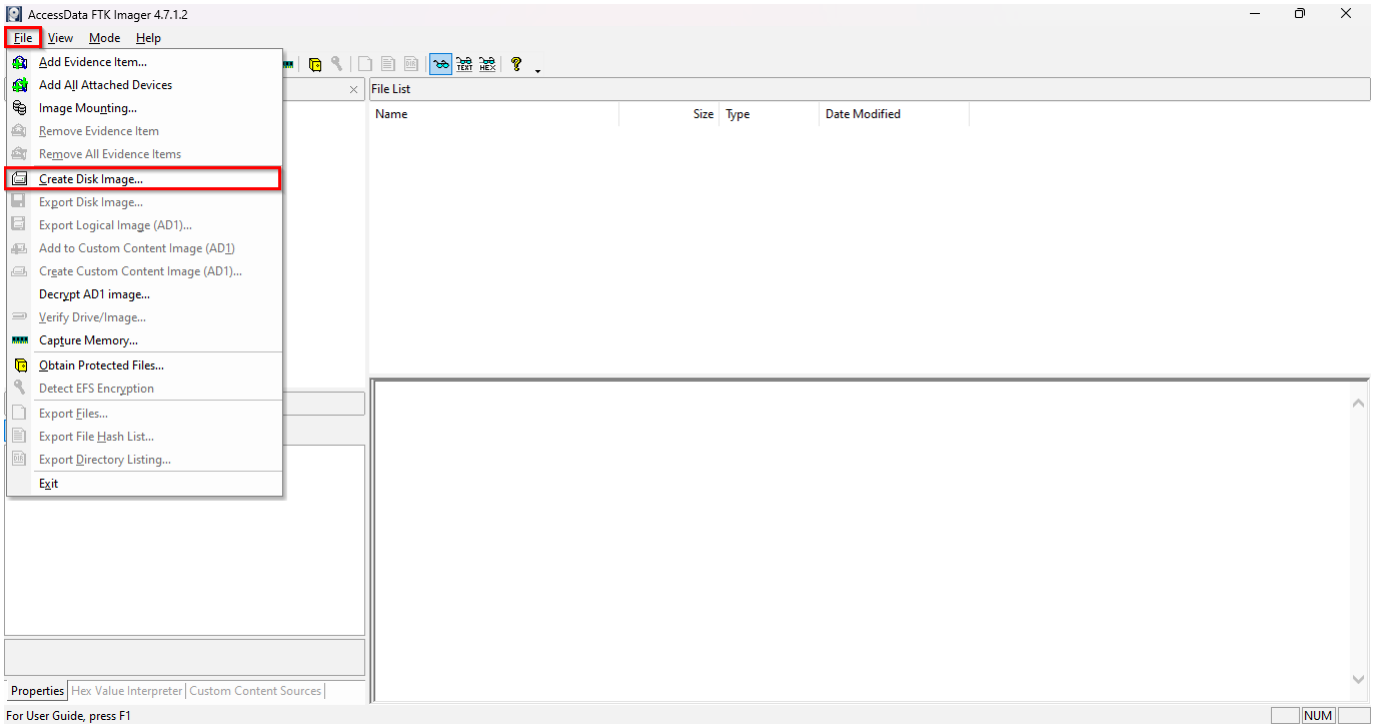
D. Method to Preserve Evidence

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

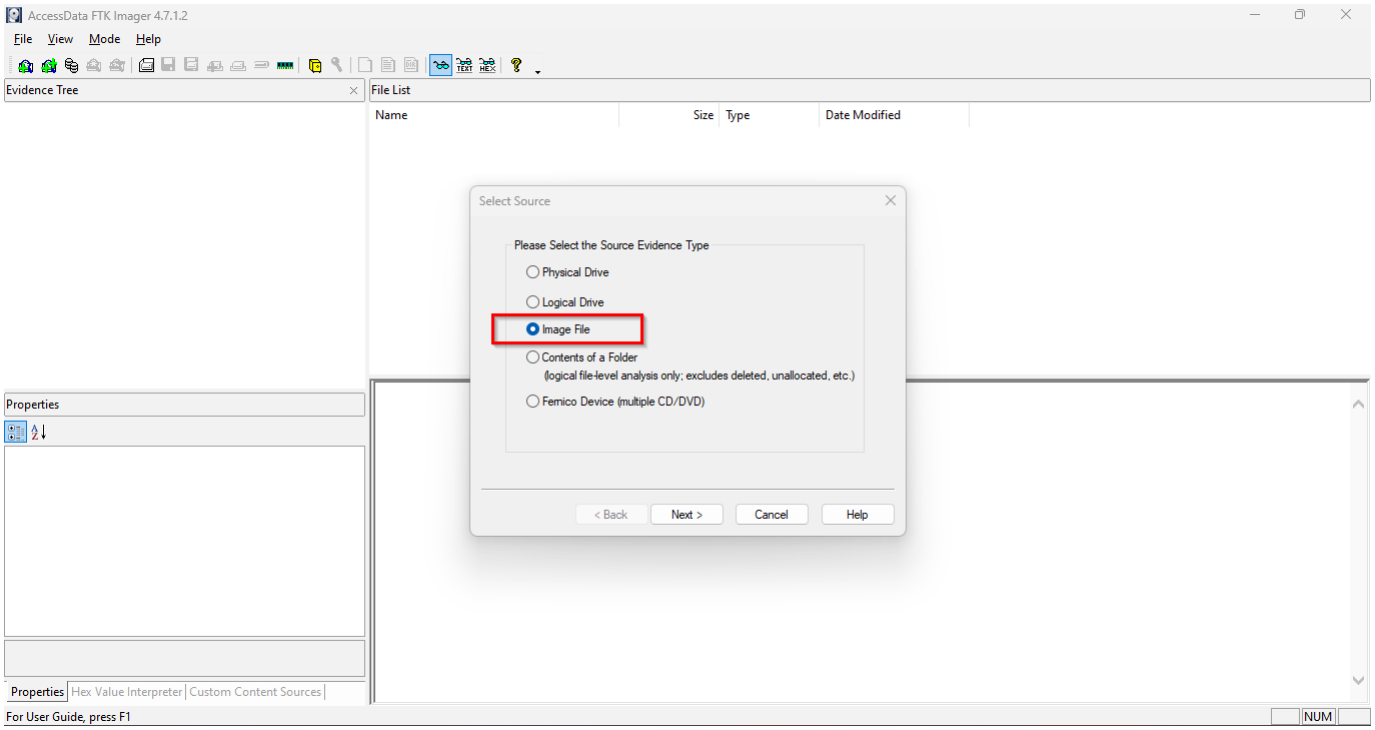
- Open FTK Imager tool.



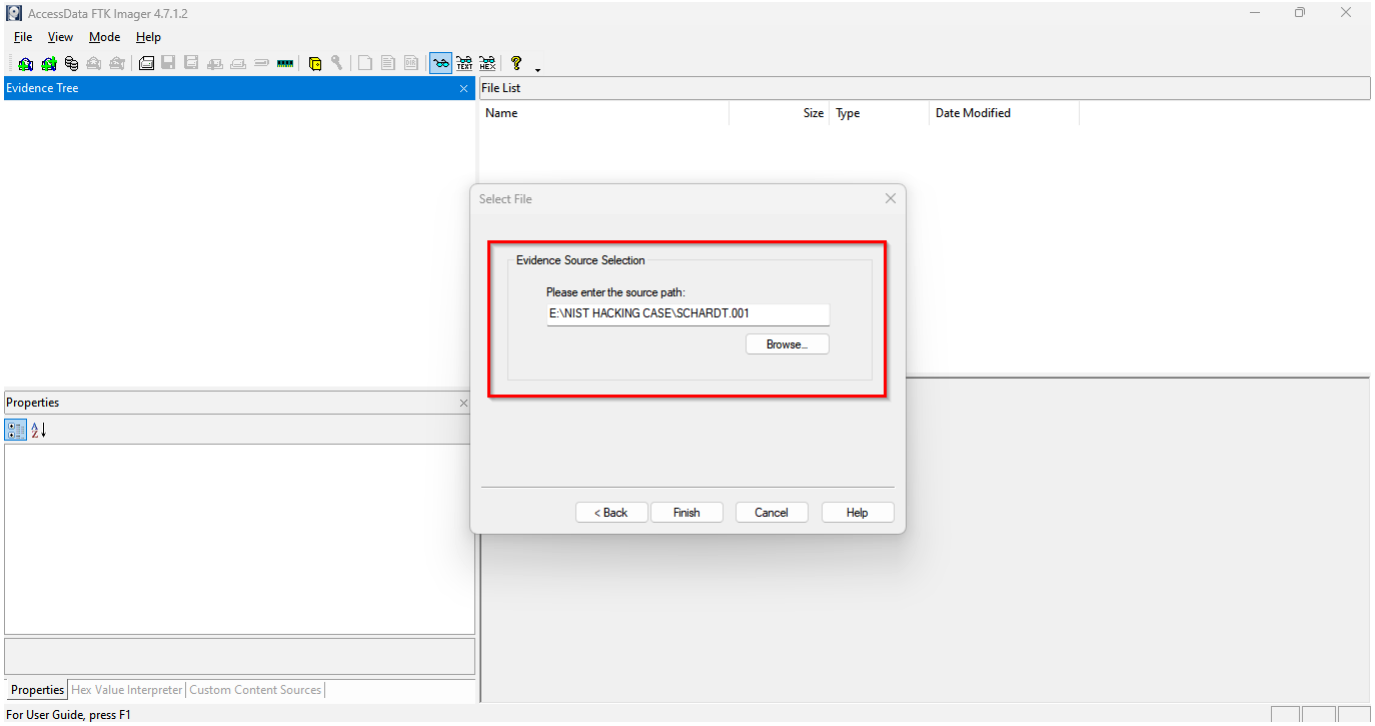
- Go to File — Create Disk Image:



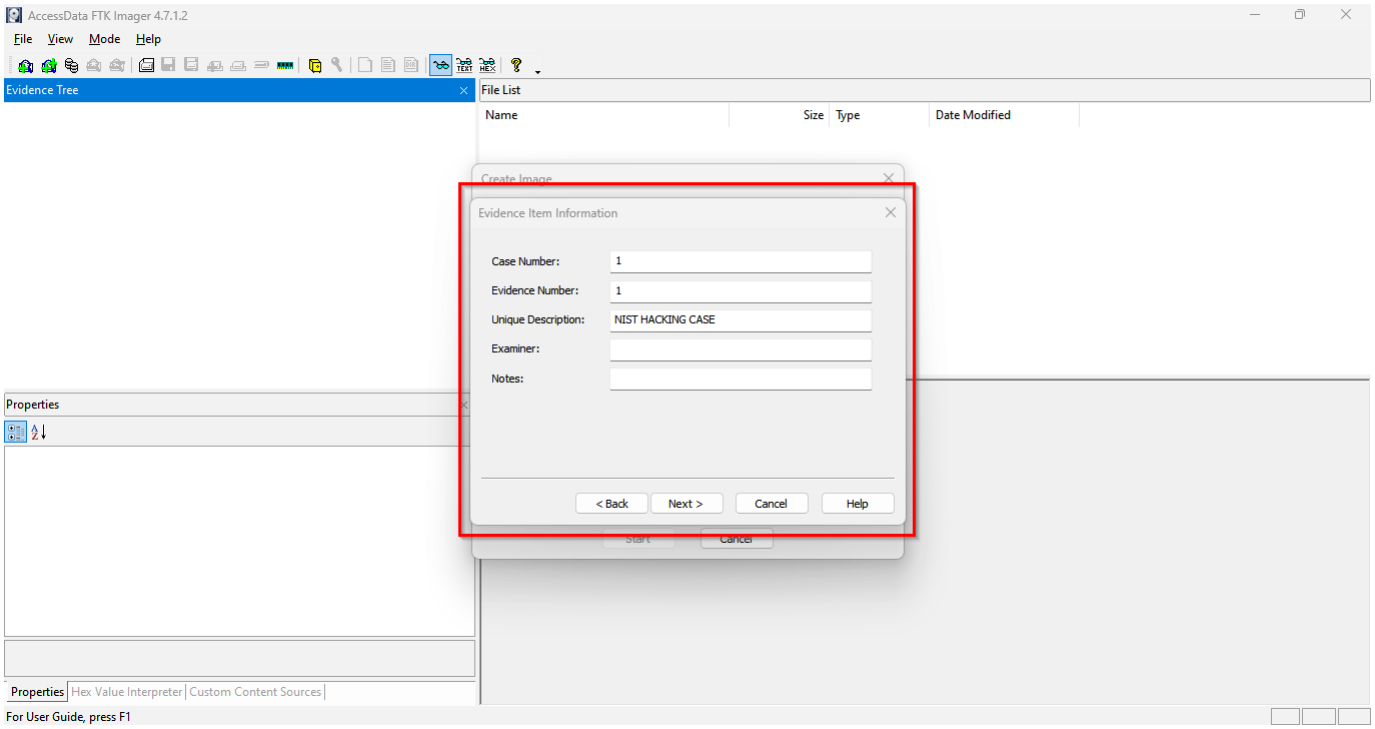
- Select Image File option.



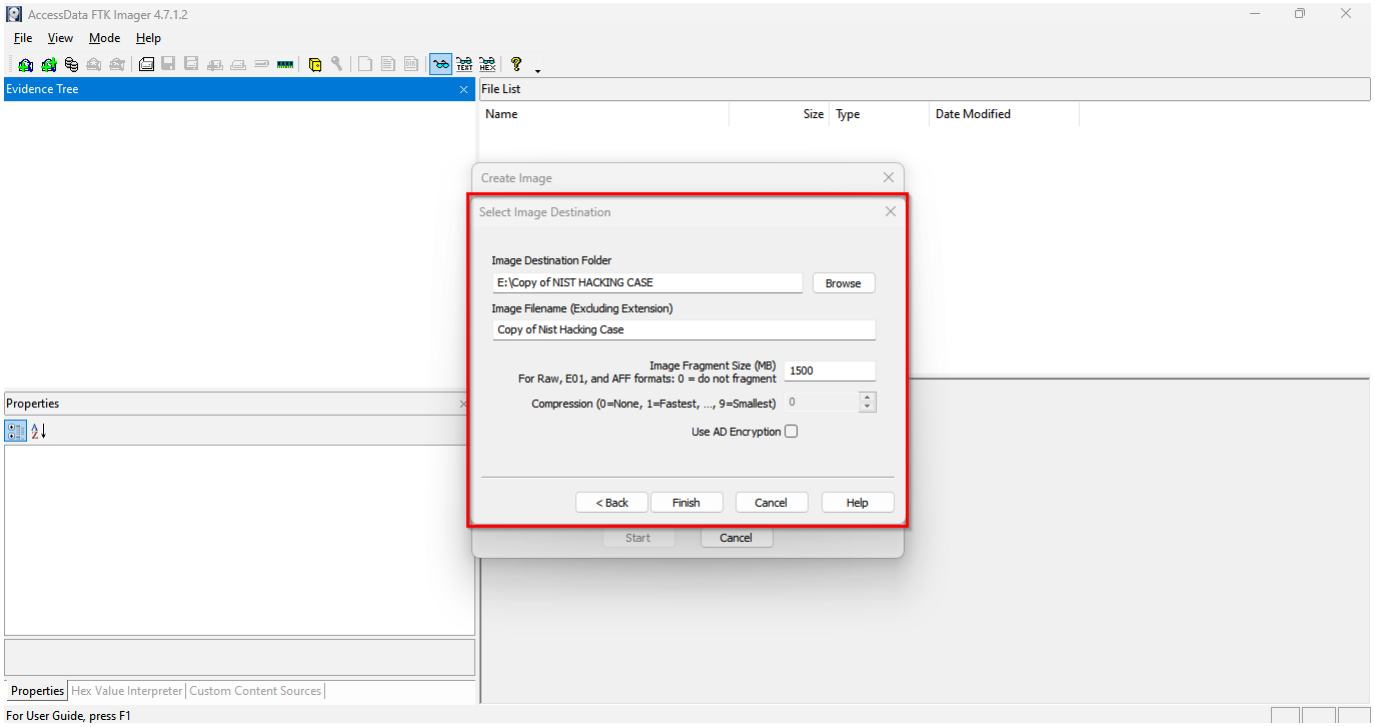
- Add the original image file.



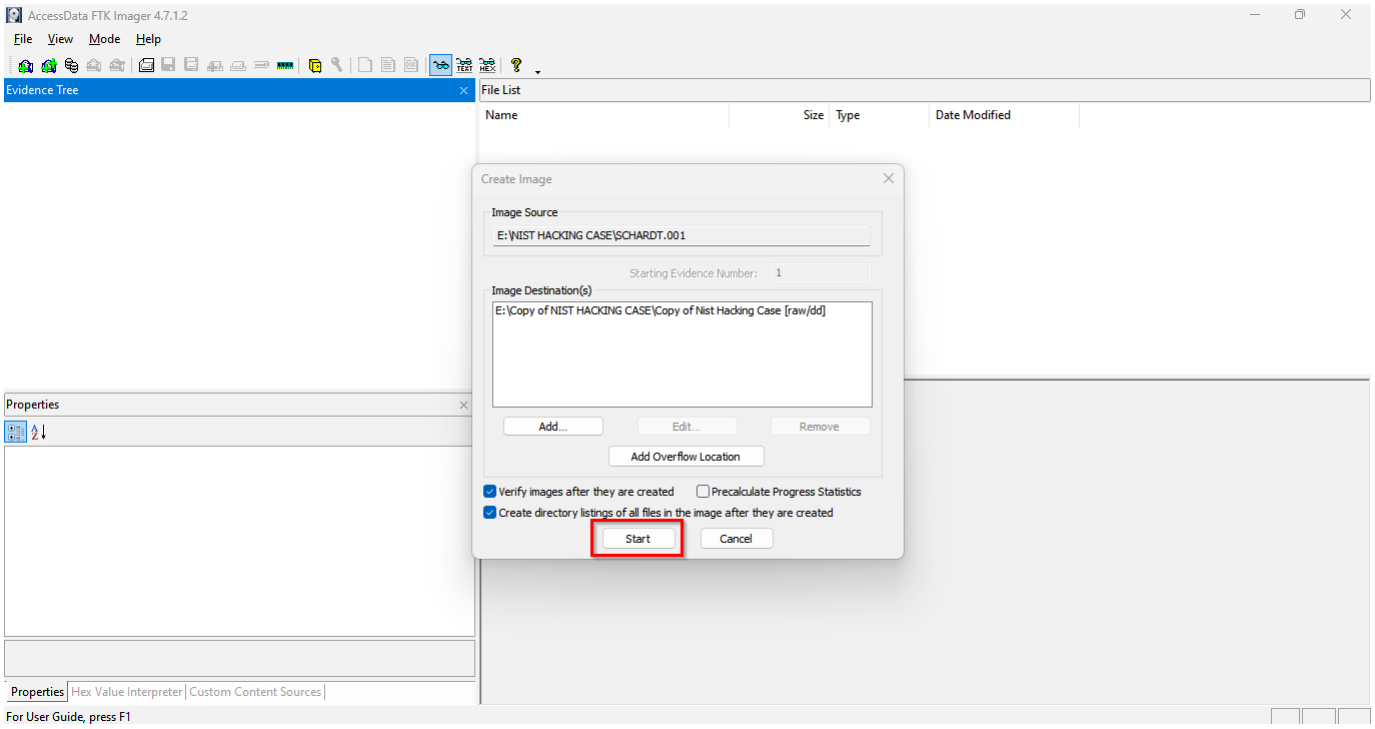
- Add the important necessary information.



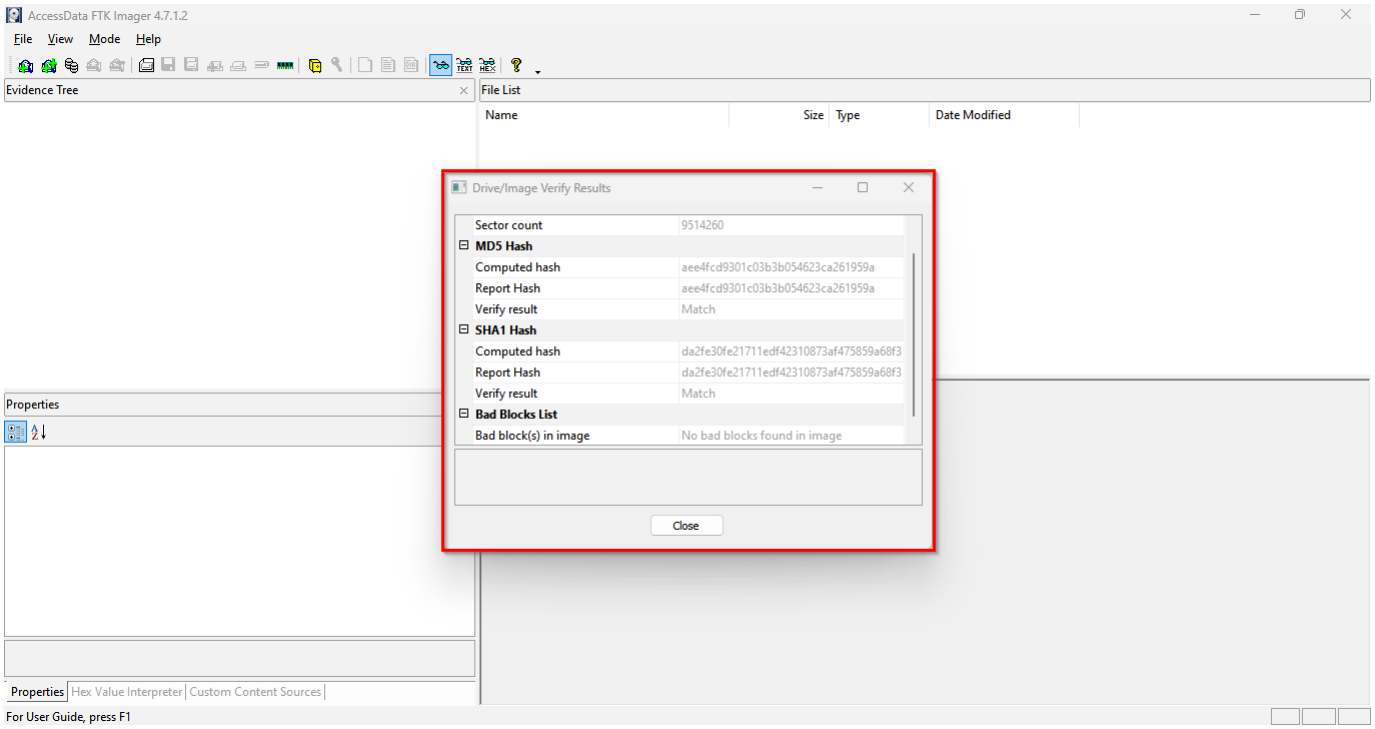
- Add image destination file.



- 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.

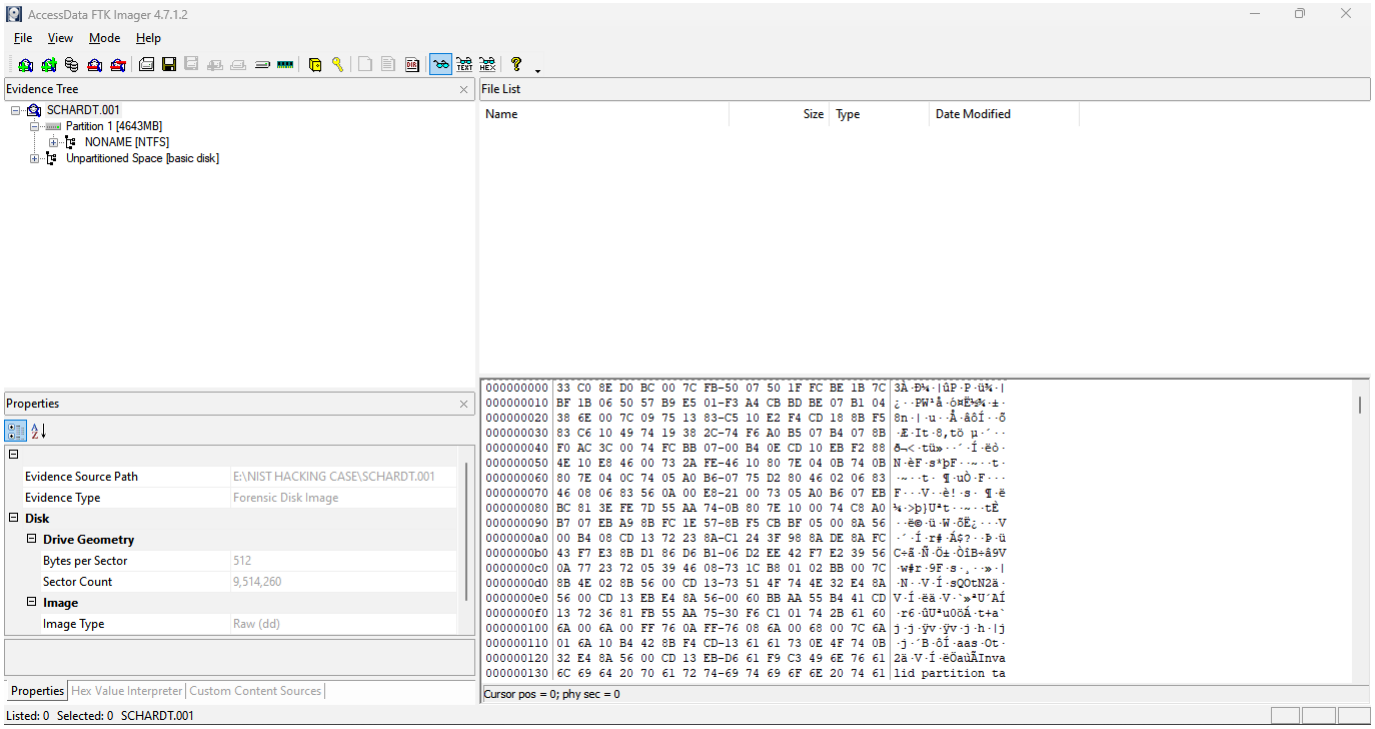
Original Image Hash: aee4fcd9301c03b3b054623ca261959a
Copying Image hash: aee4fcd9301c03b3b054623ca261959a

III. Tools Used

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

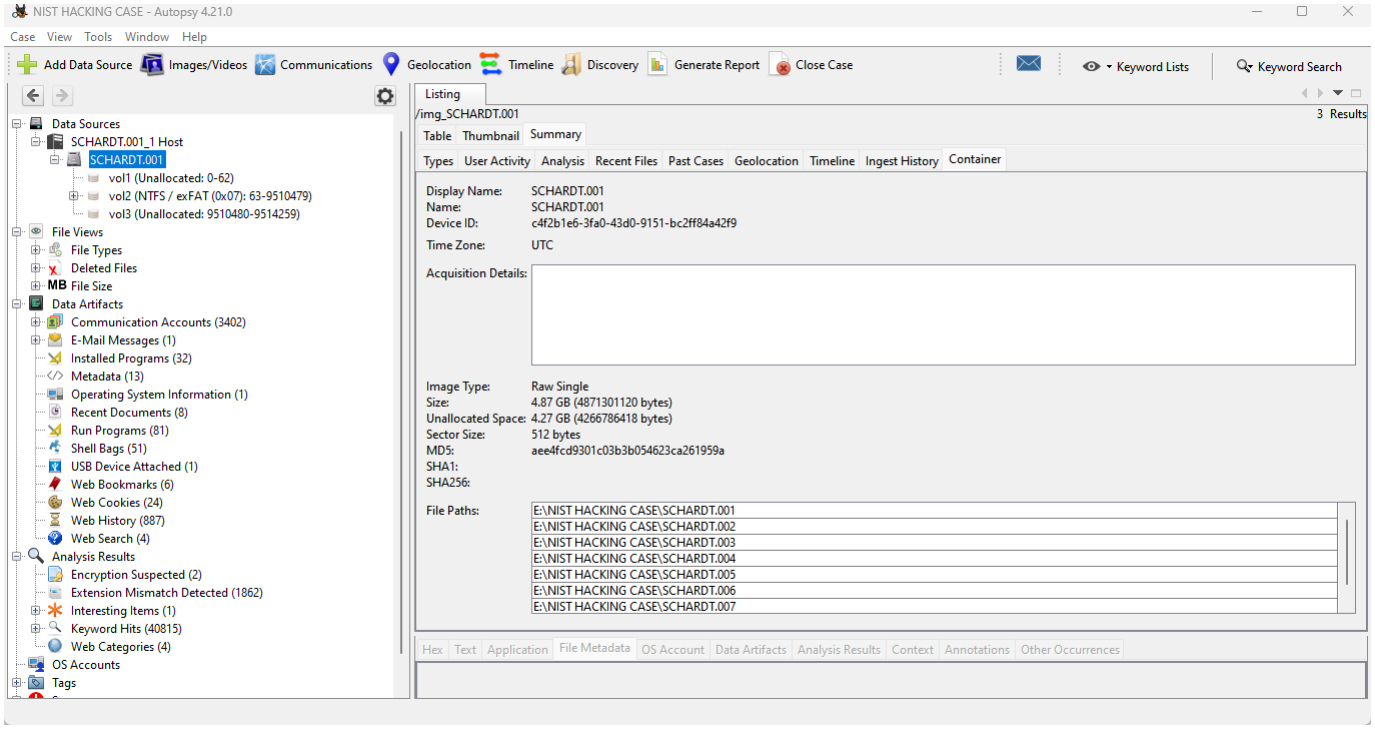
A. *FTK imager*

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).



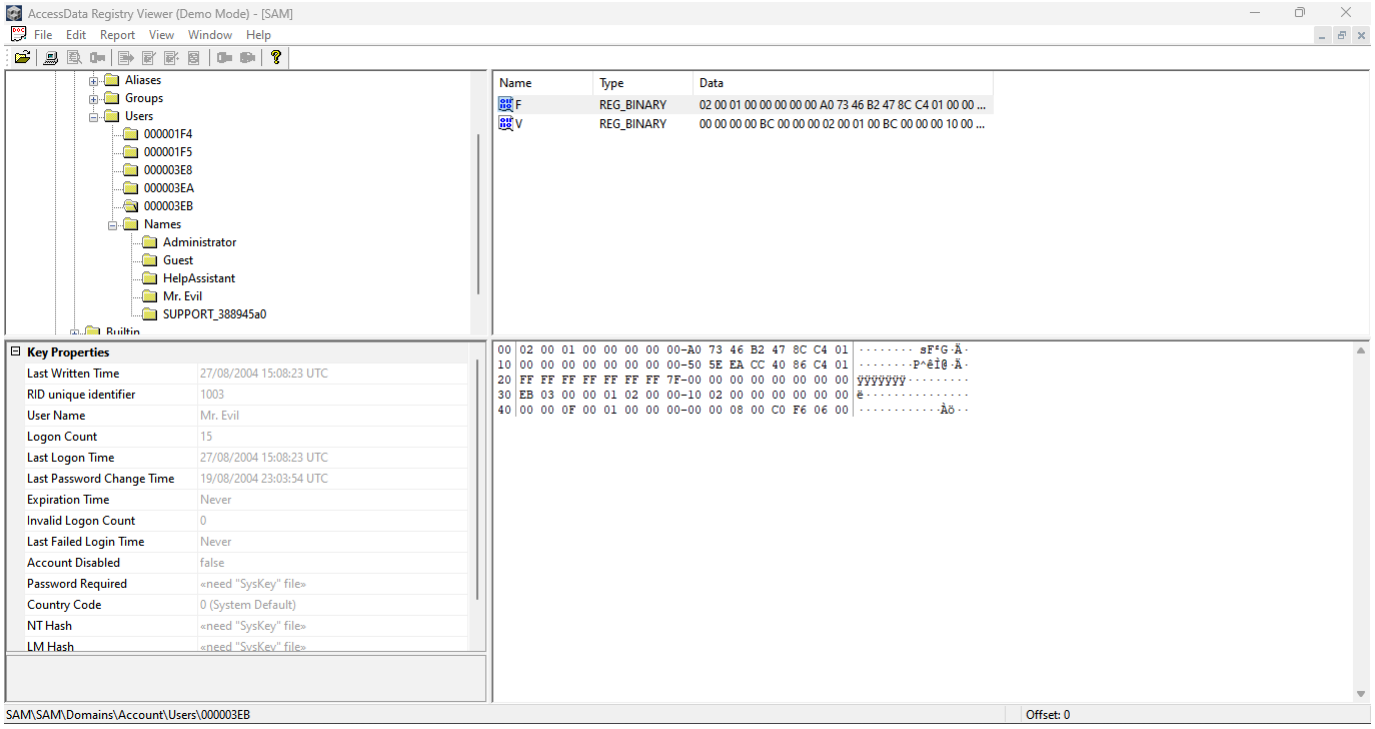
B. *Autopsy*

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).



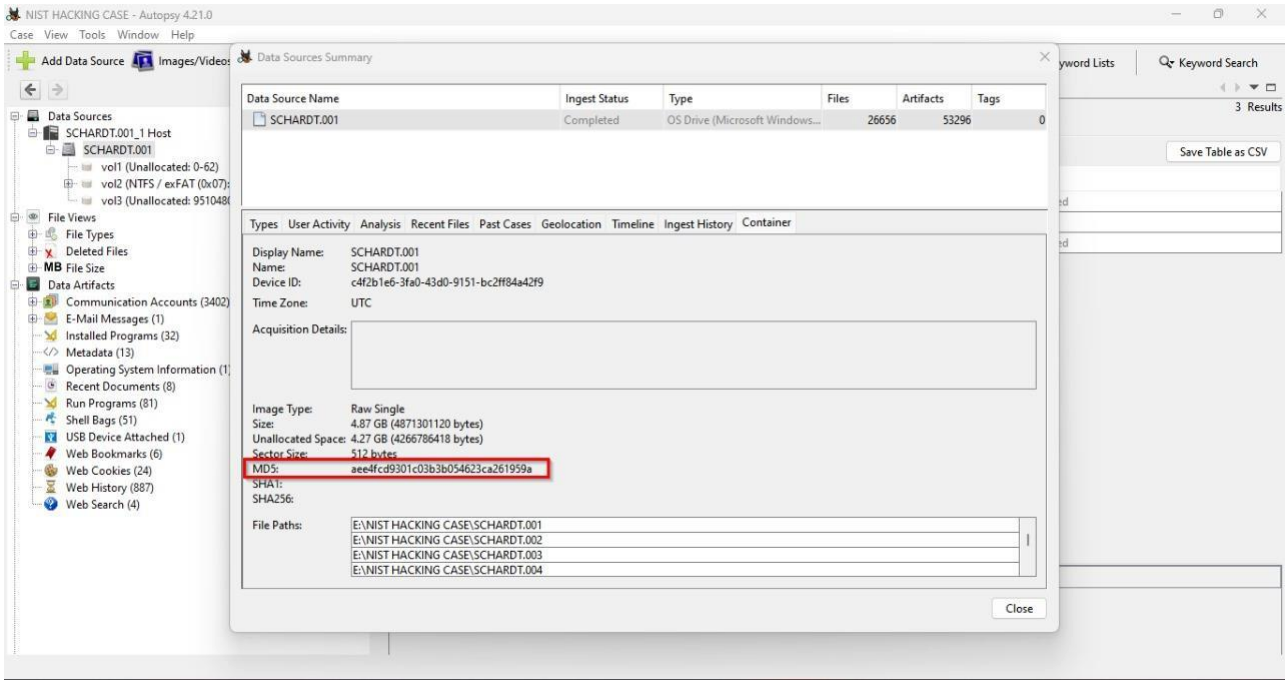
IV. Evidence Identification, Analysis, and Findings

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



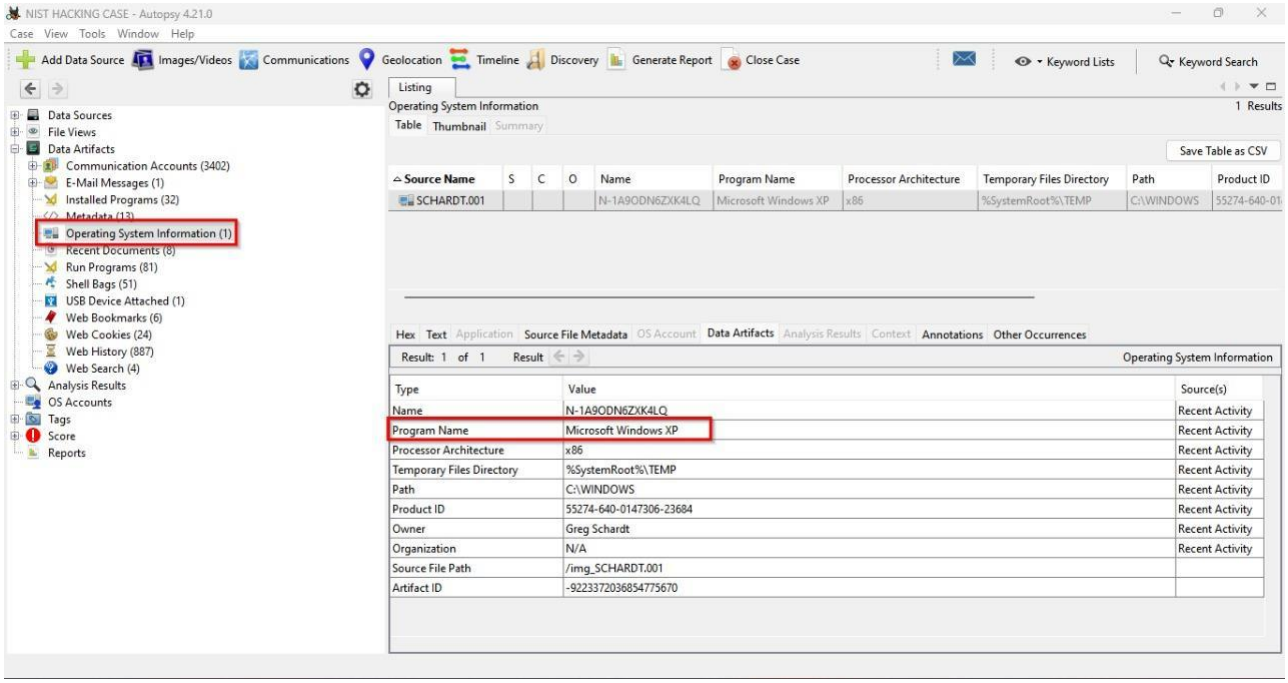
Q2. Operating System

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

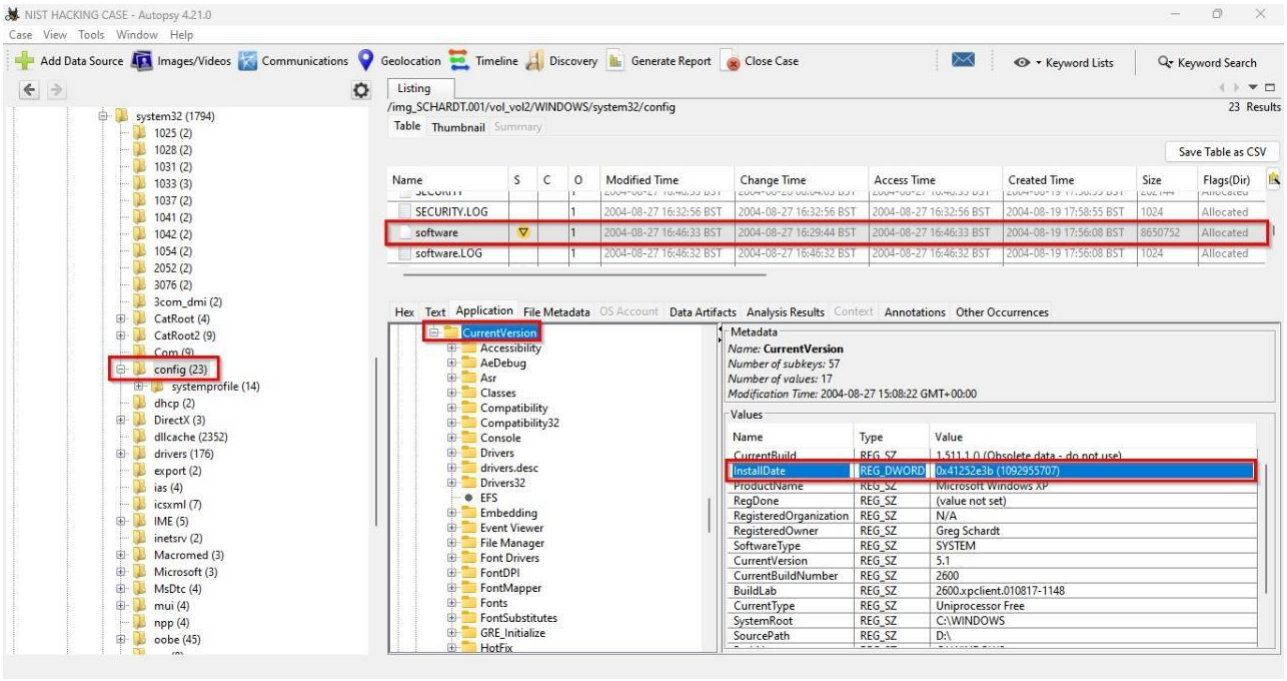


Q3. Operating System Install Date

Install Date in Registry: 0x41252e3b (1092955707)

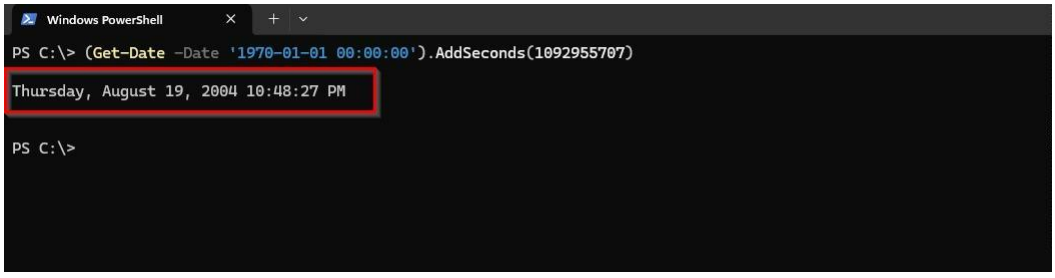
Knowing the installation date of the OS helps establish a timeline of events related to the system. It provides a starting point for investigating when the system was initially set up and potentially compromised.

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



After converting it into UTC Standard.

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



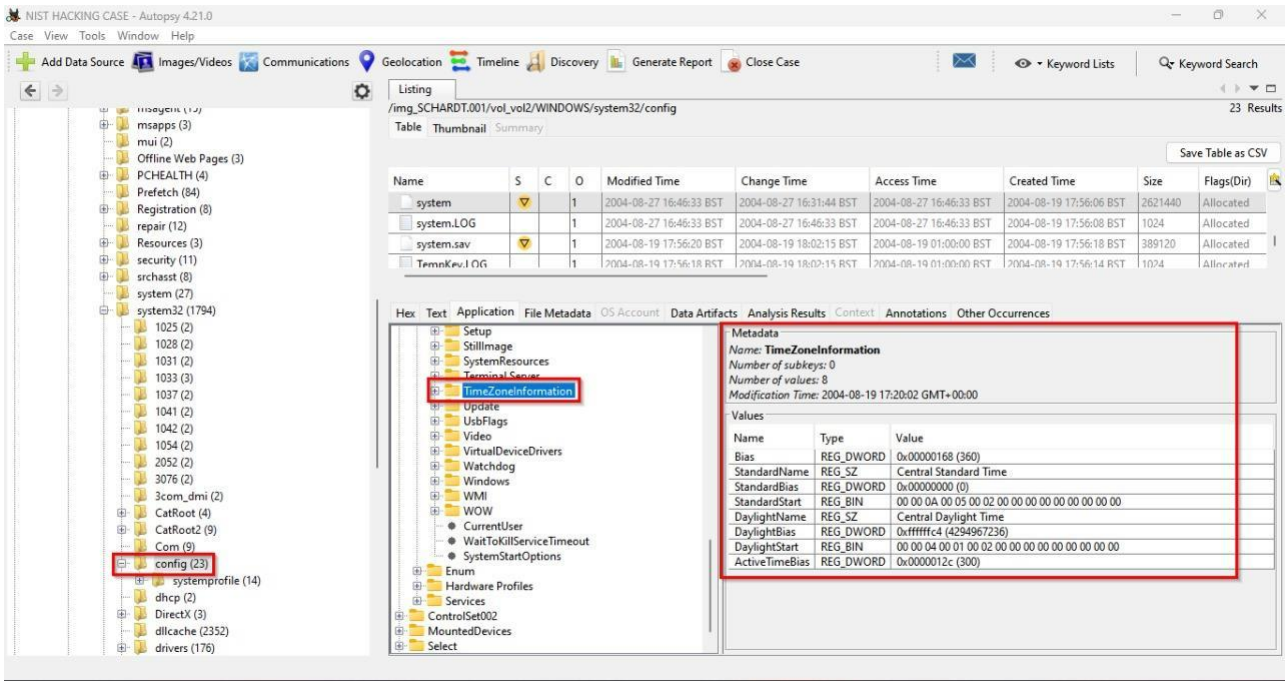
Q4. System Time Zone Settings

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

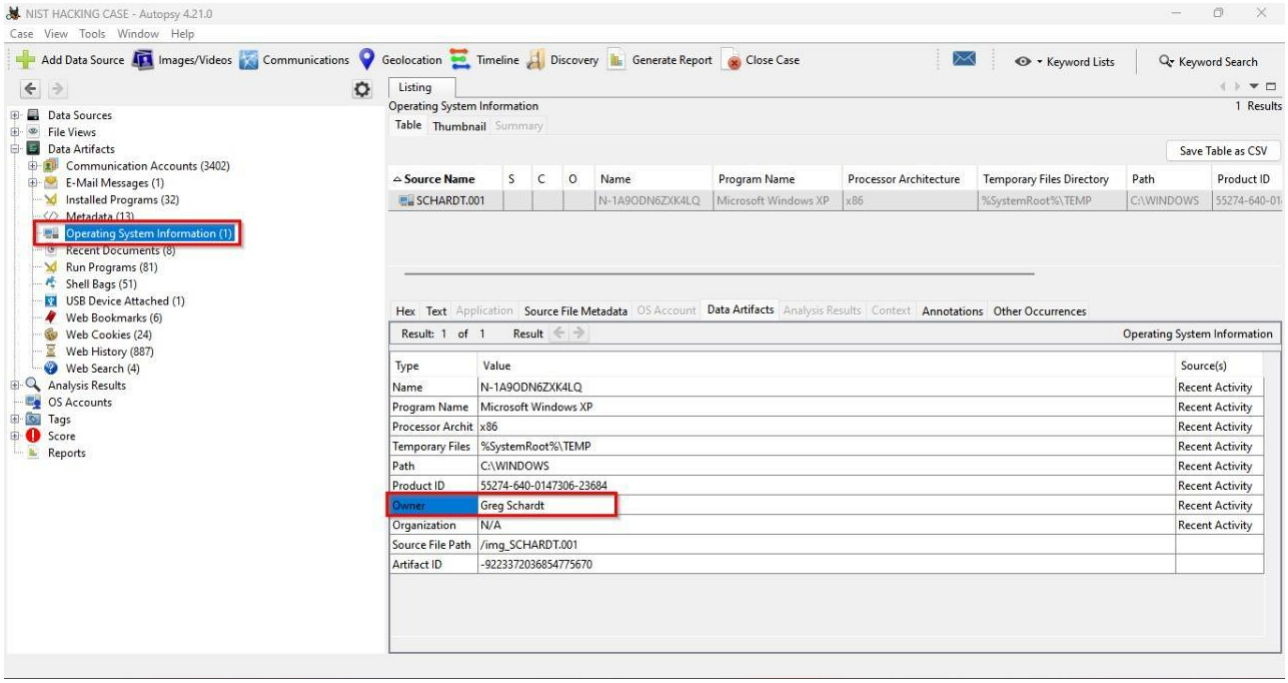


Q5. Operating System Registered Owner

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

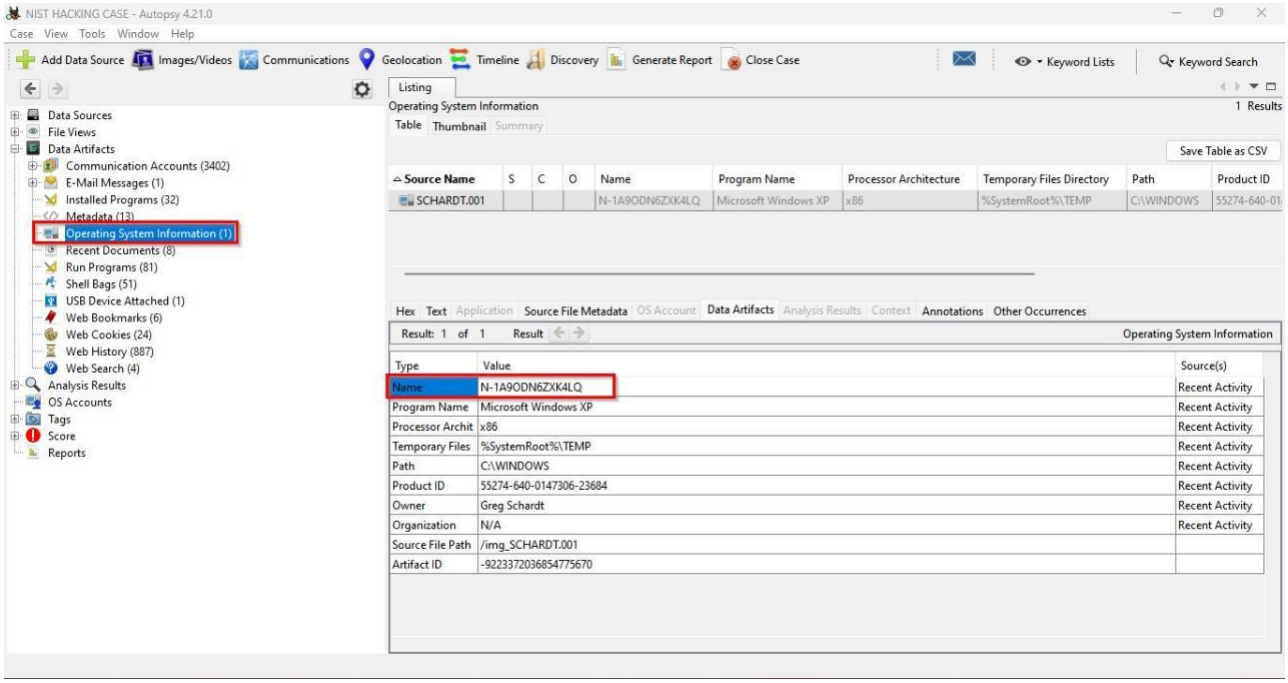


Q6. Computer Account Name

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



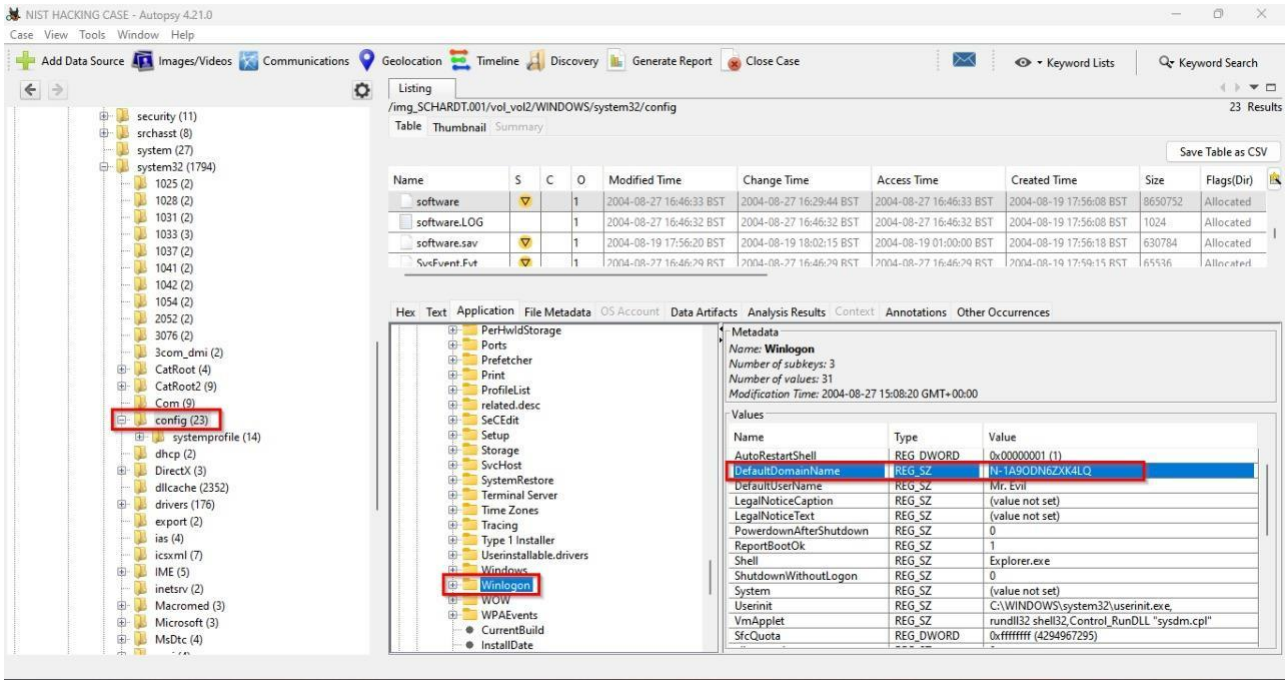
Q7. Primary Domain Name

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

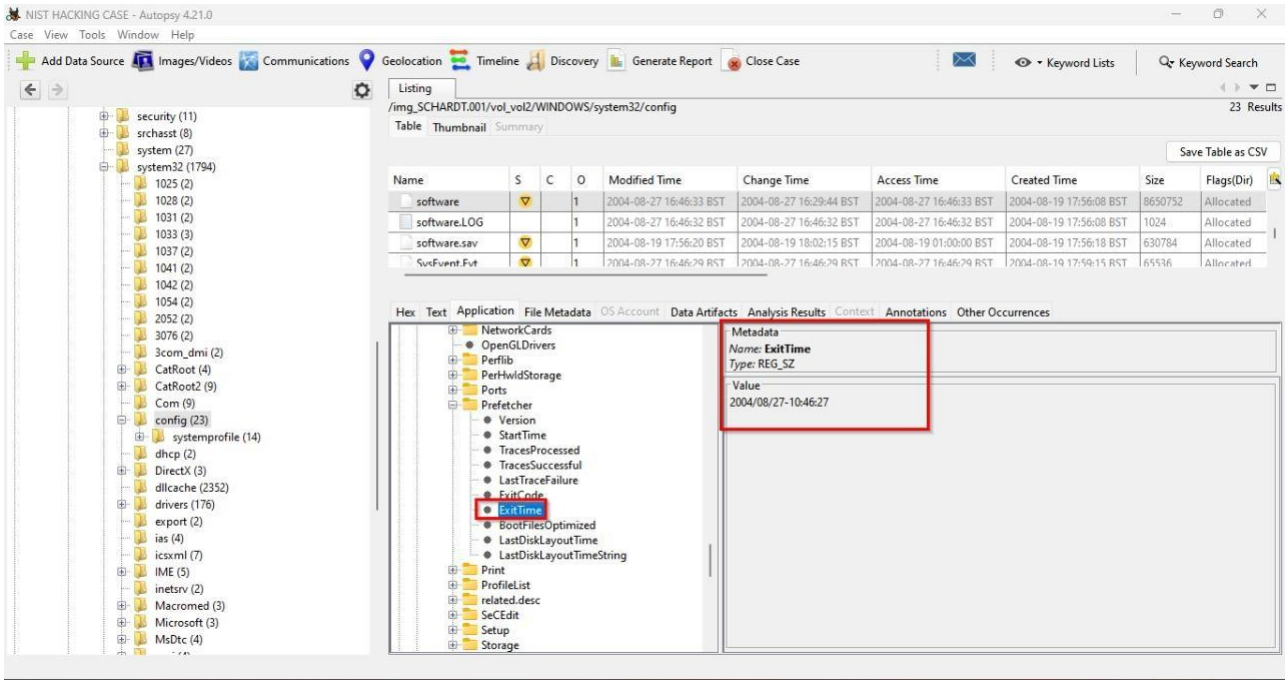


Q8. Last recorded shutdown date/time

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



Q9. Total OS Accounts

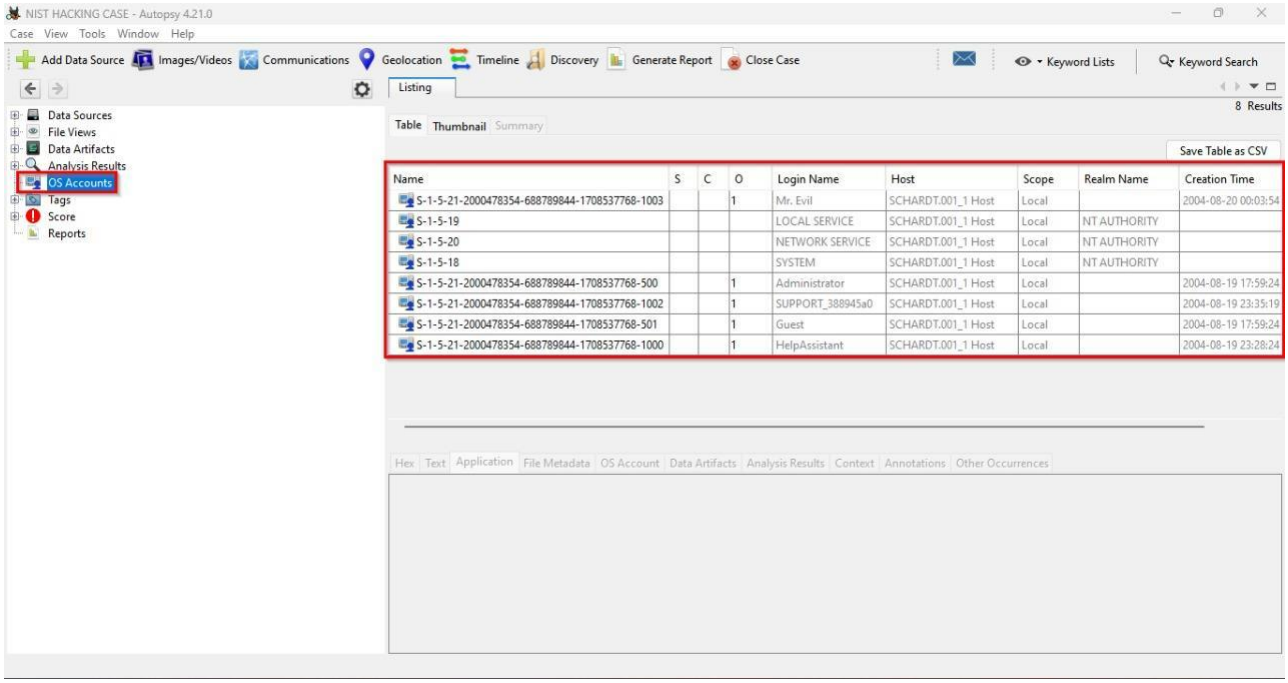
Accounts: 5

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



Q10. Computer Most Frequent User

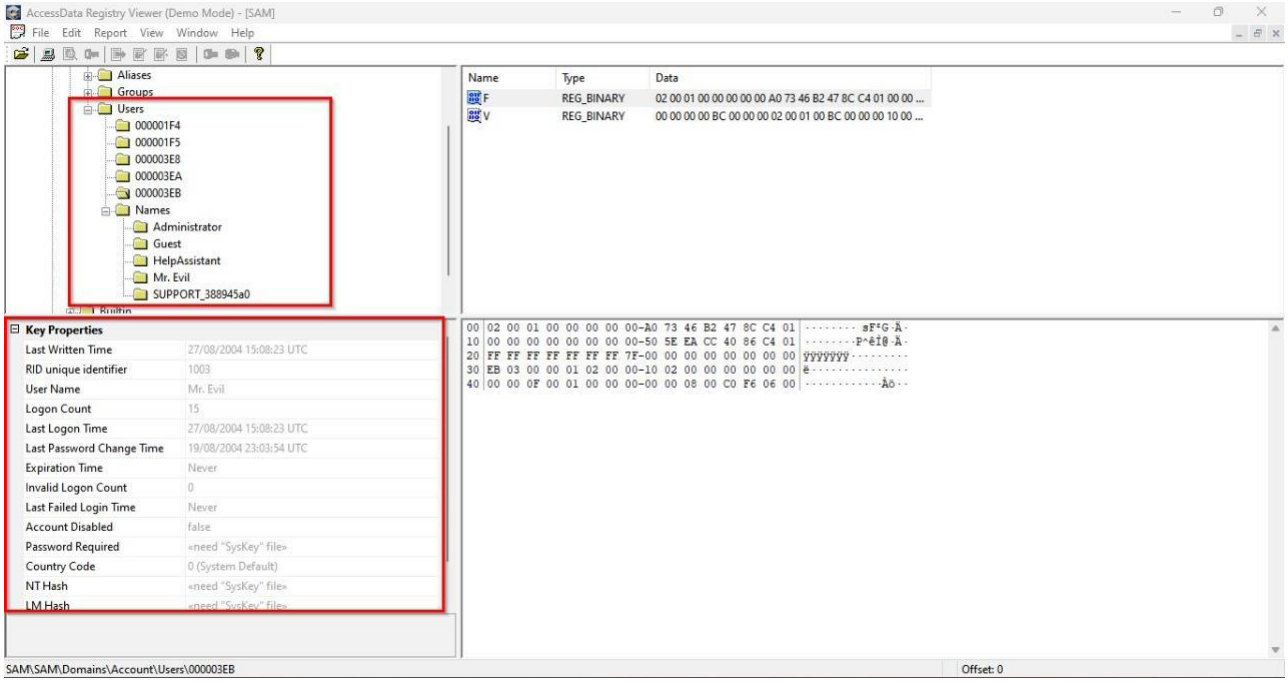
Account Name: Mr. Evil

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

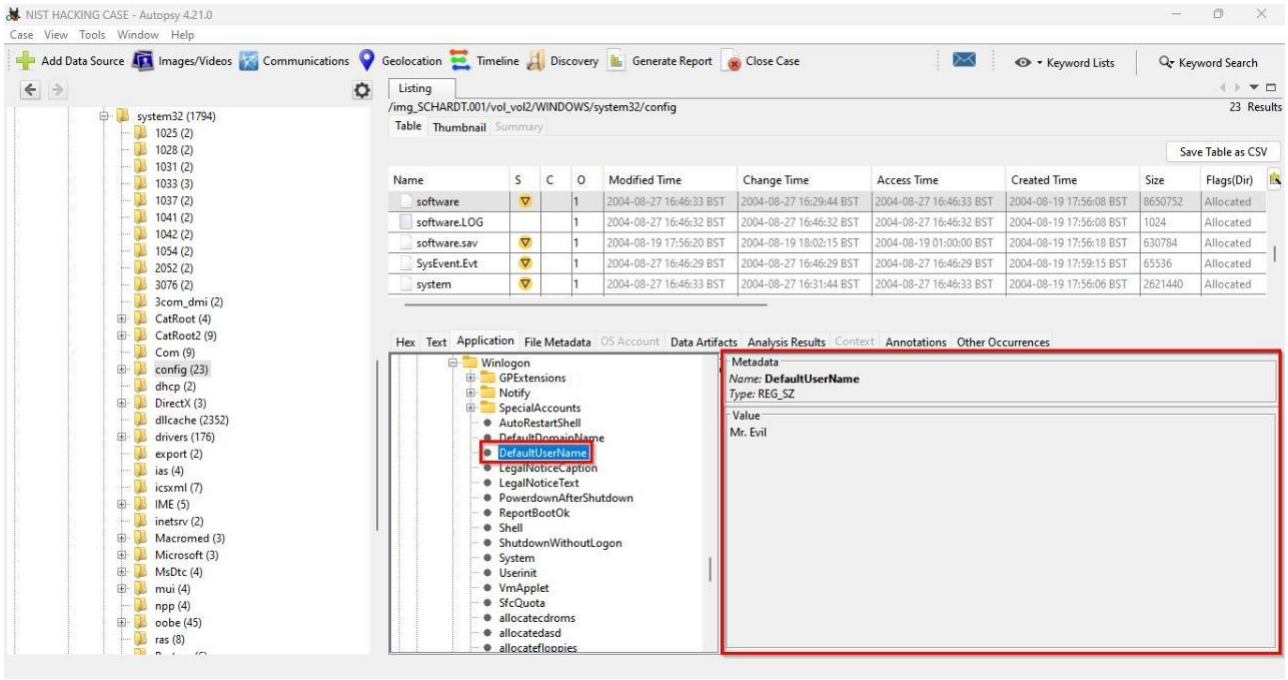


Q11. Last System Logon

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



Q12. Administrator Identification

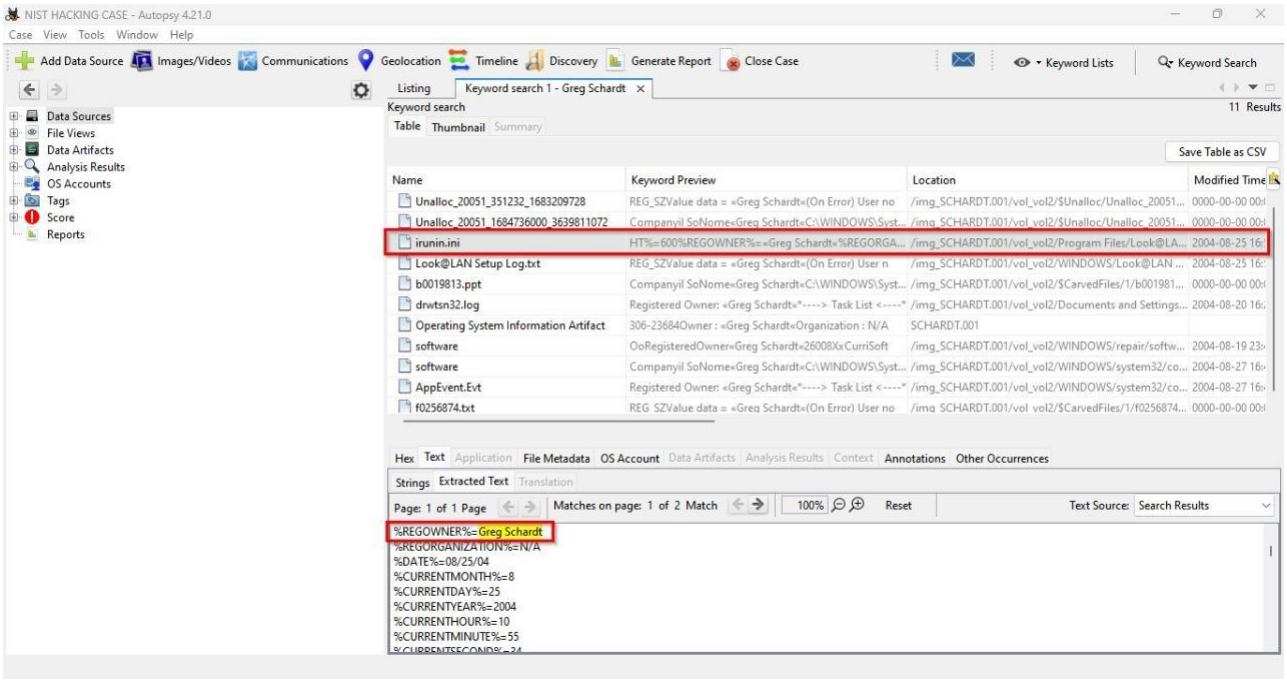
File: irunin.ini **Software:** Look@LAN

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”.

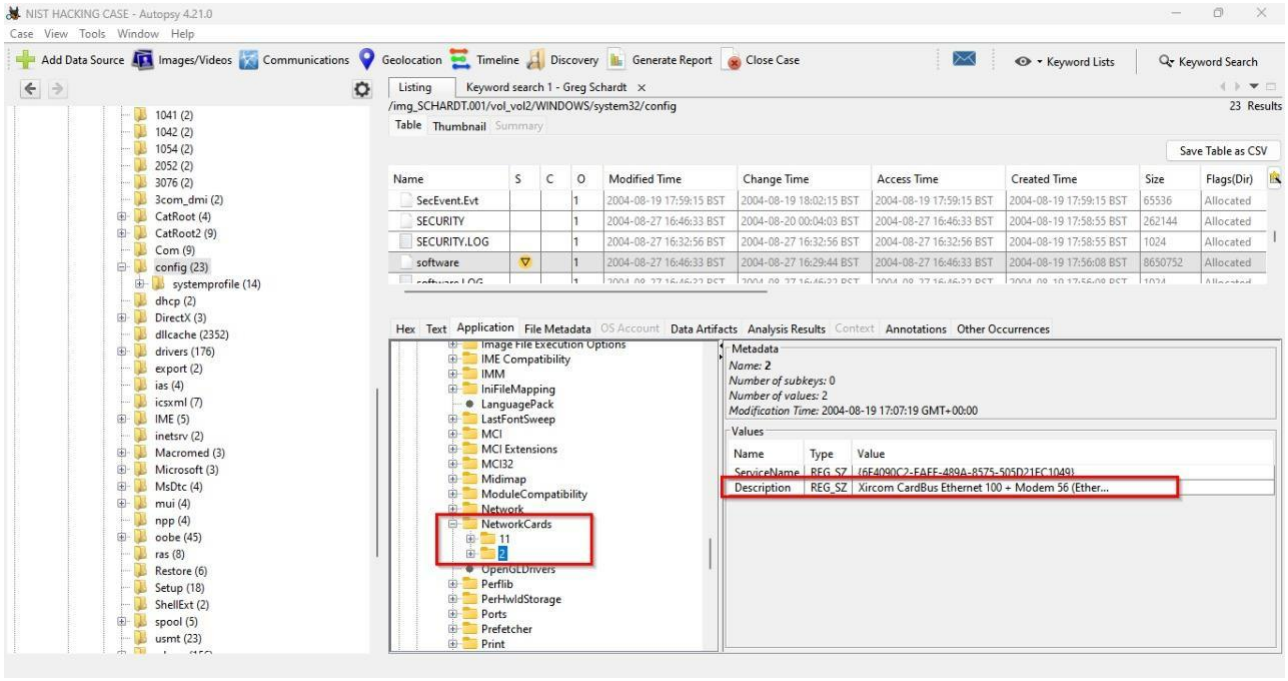


Q13. System Network Cards

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



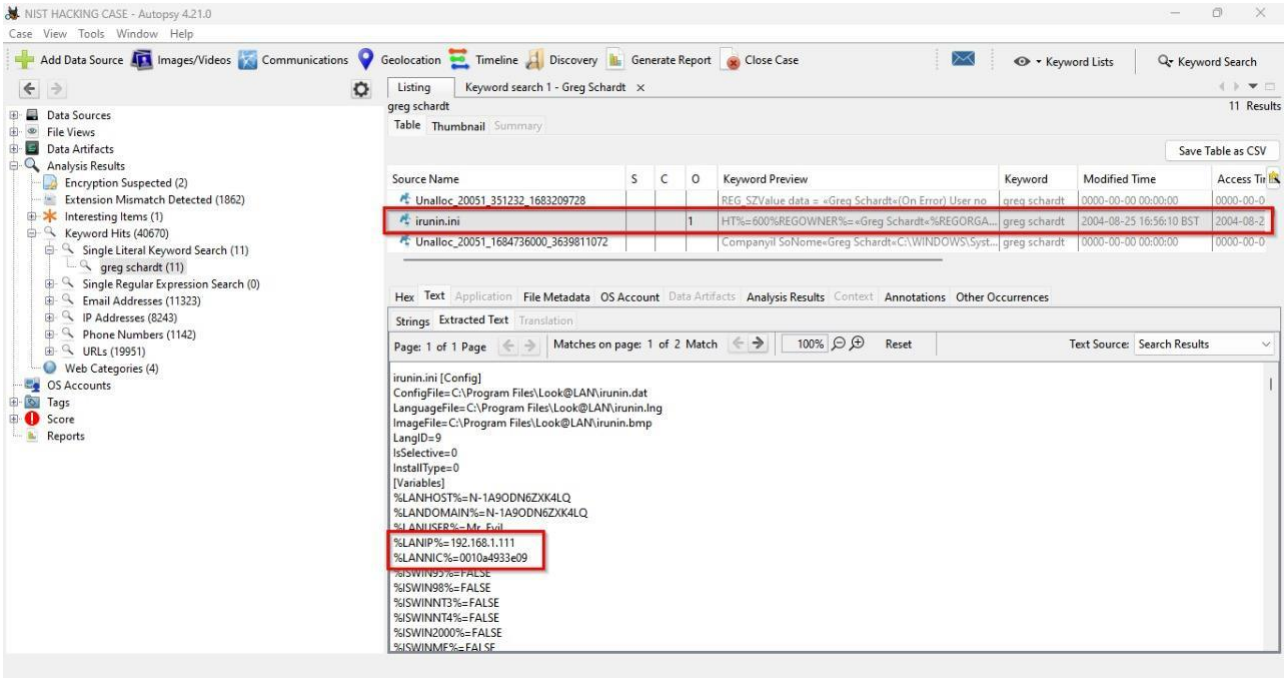
Q14. IP and Mac Address

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



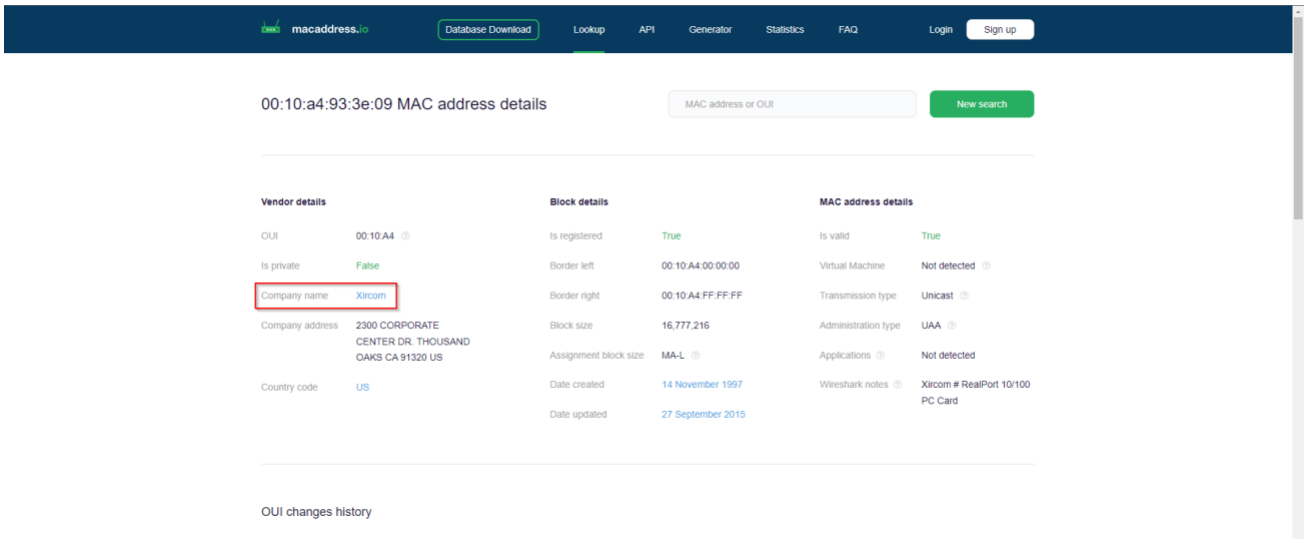
Q15. Mac Address Vendor

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.

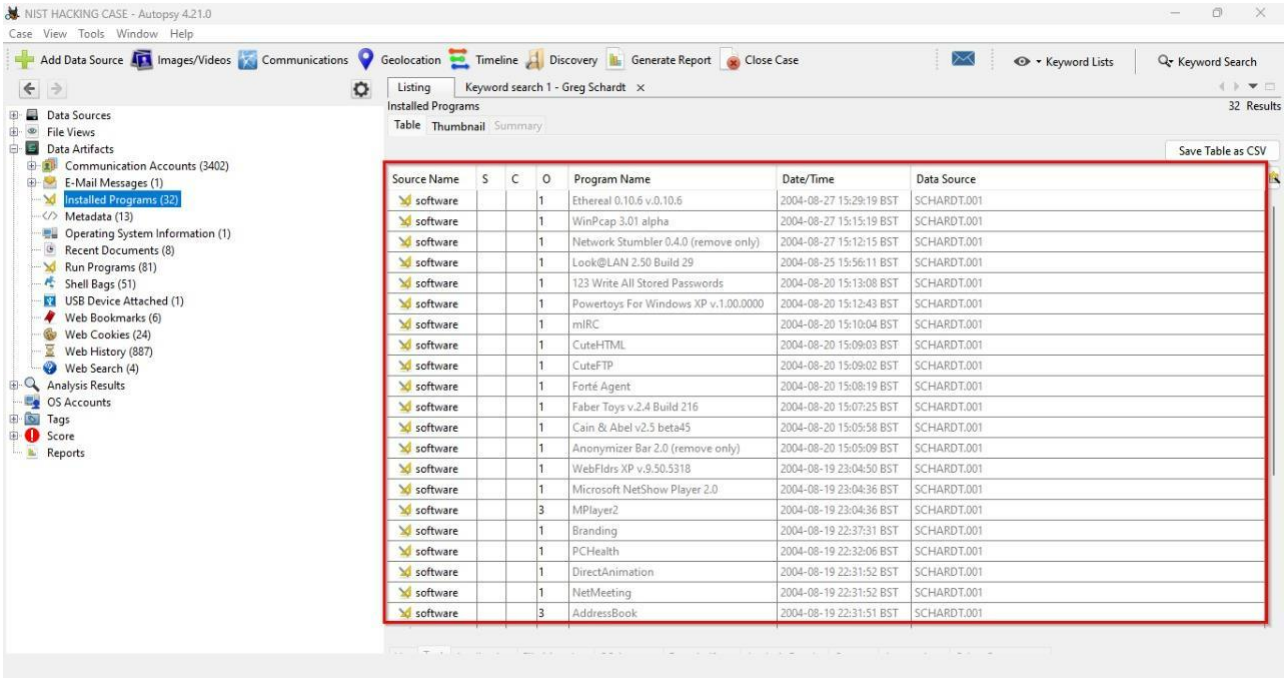


Q16. Installed Programs Used in Hacking

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

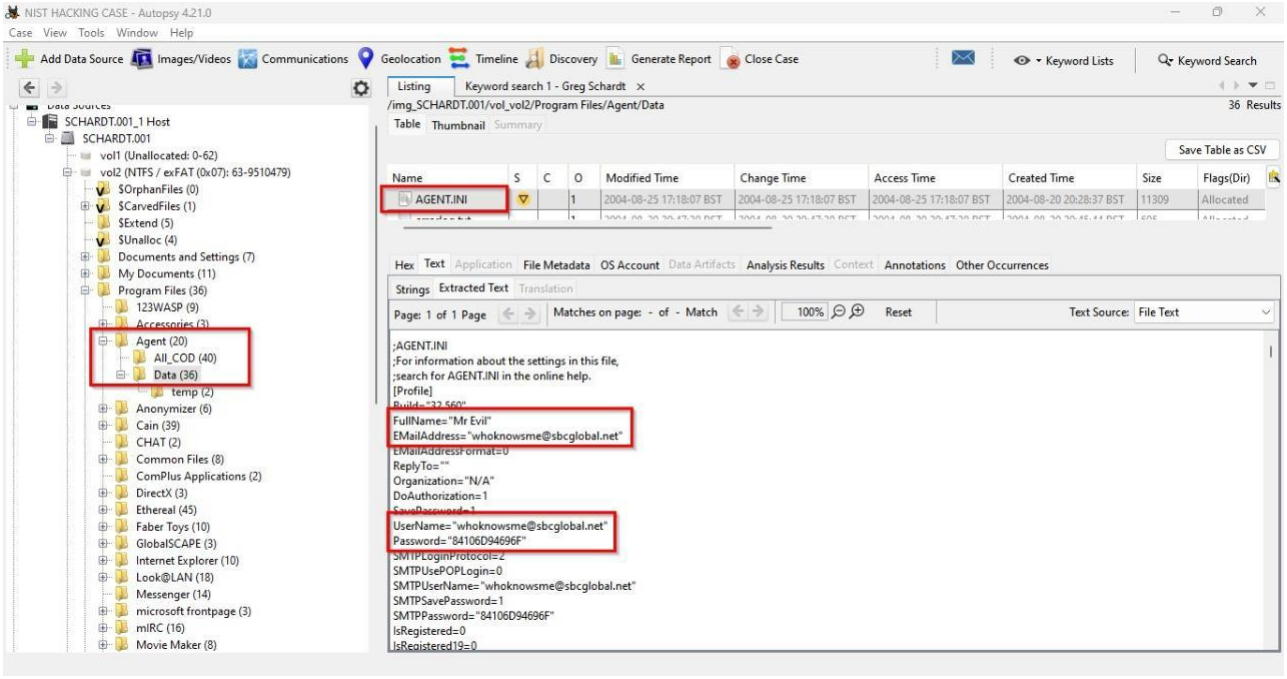


Q17. SMTP Email Address

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

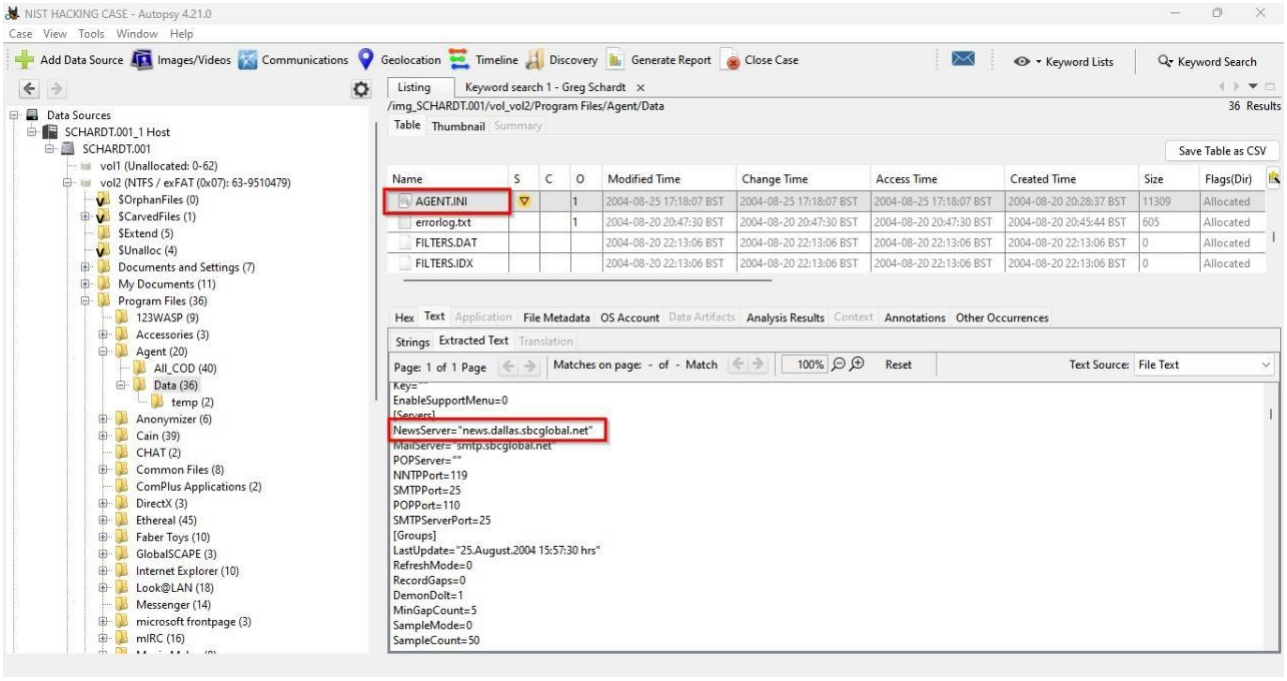


Q18. NNTP Server Settings

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



Q19. NNTP Server Settings Information

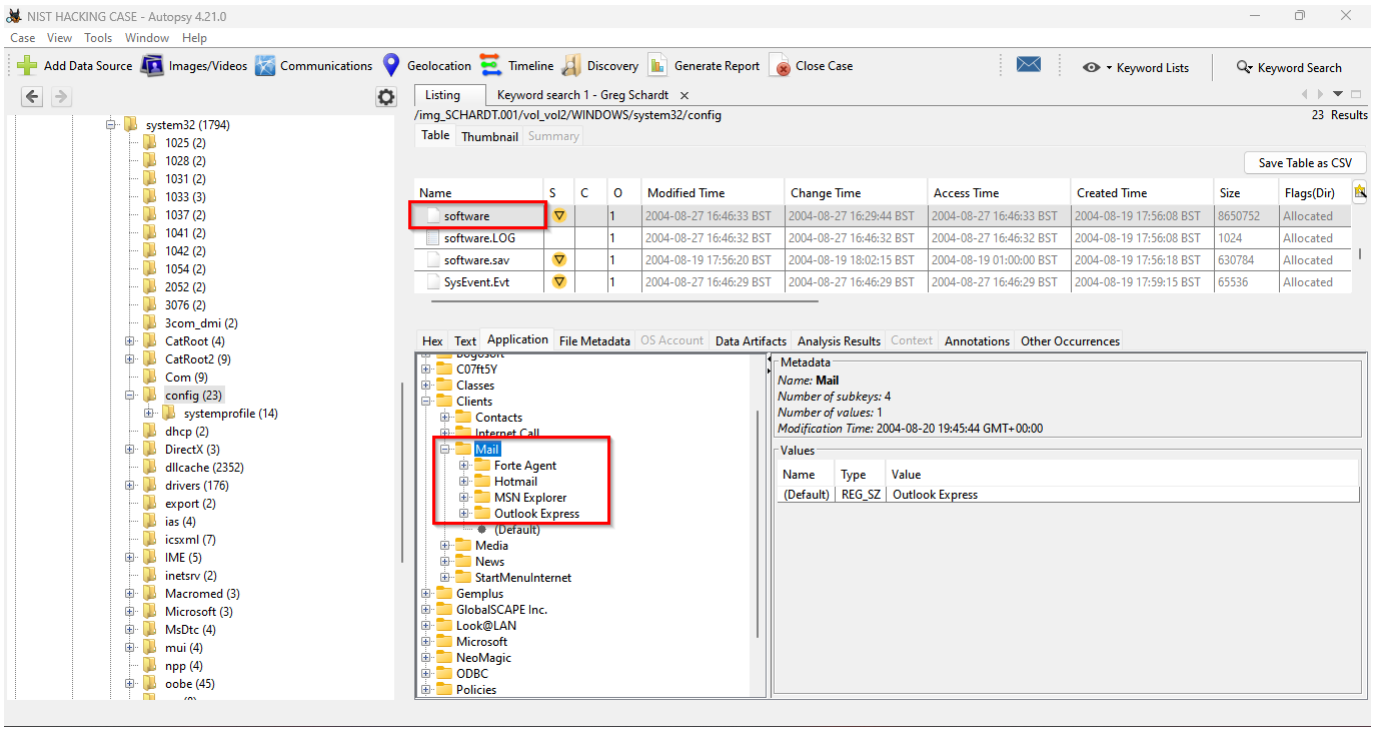
Programs:

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



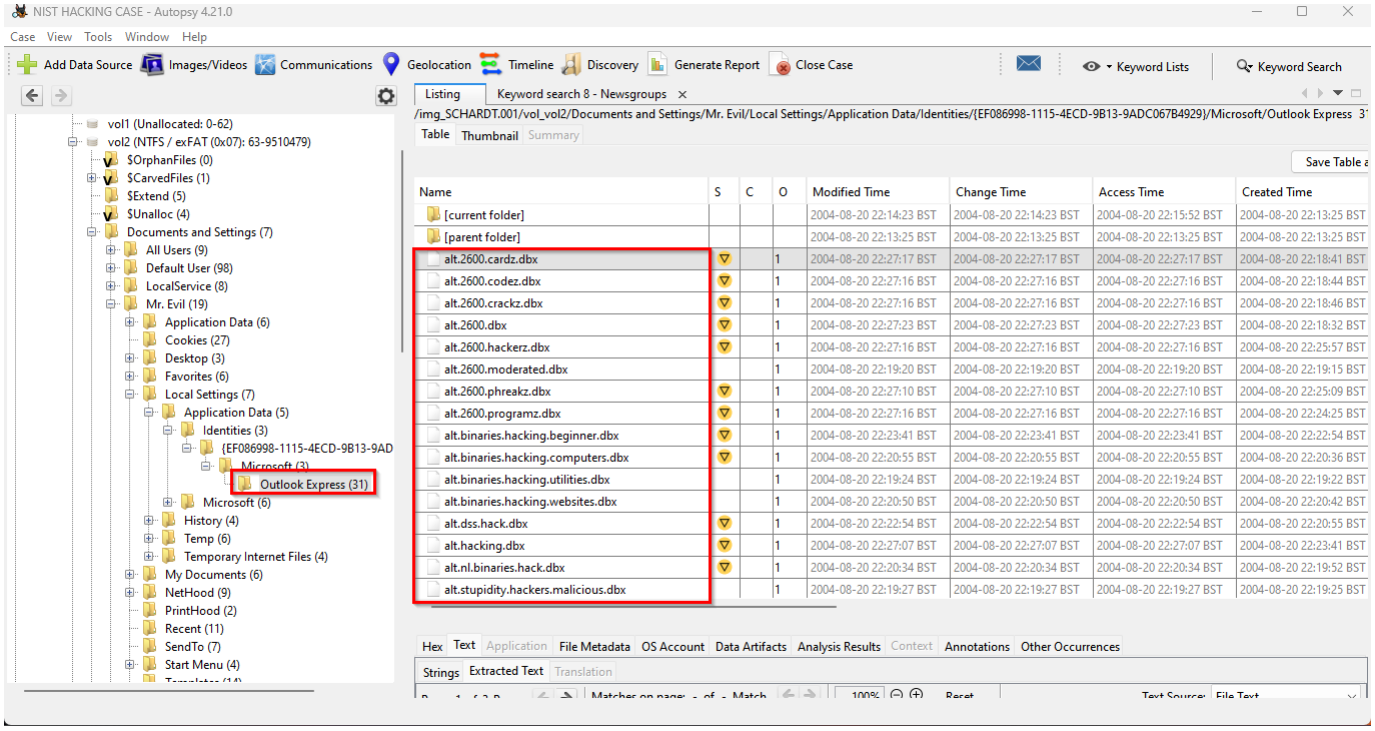
Q20. Subscribed Newsgroups

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

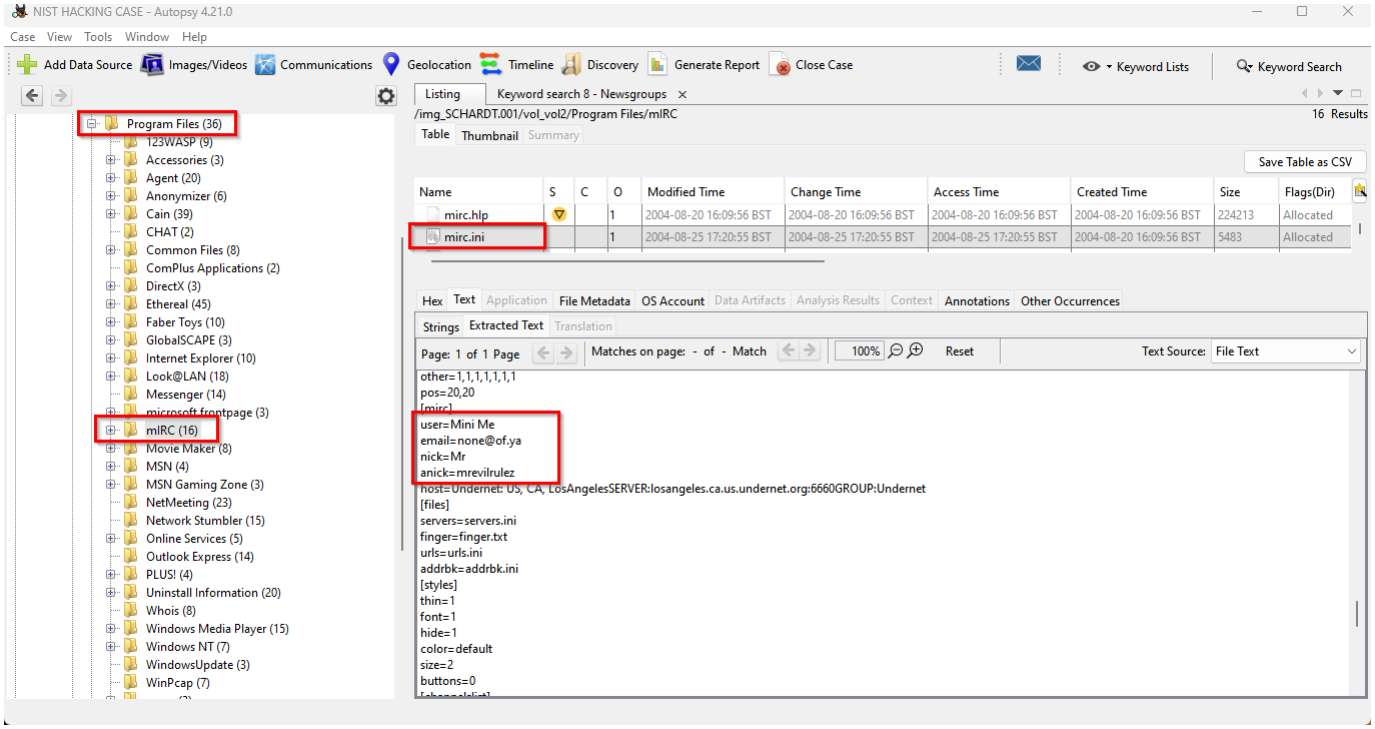


Q21. MIRC User Settings

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.



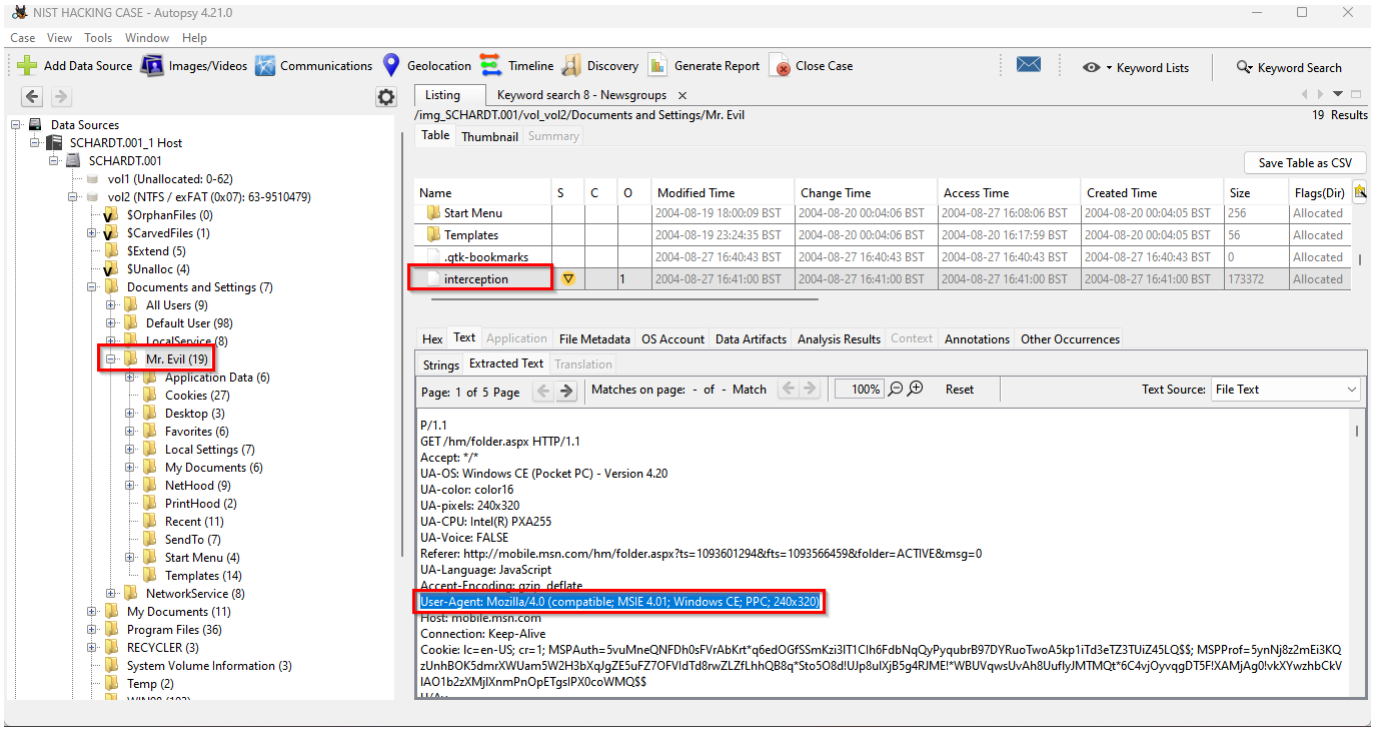
Q22. Information Reveal from Text File

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)



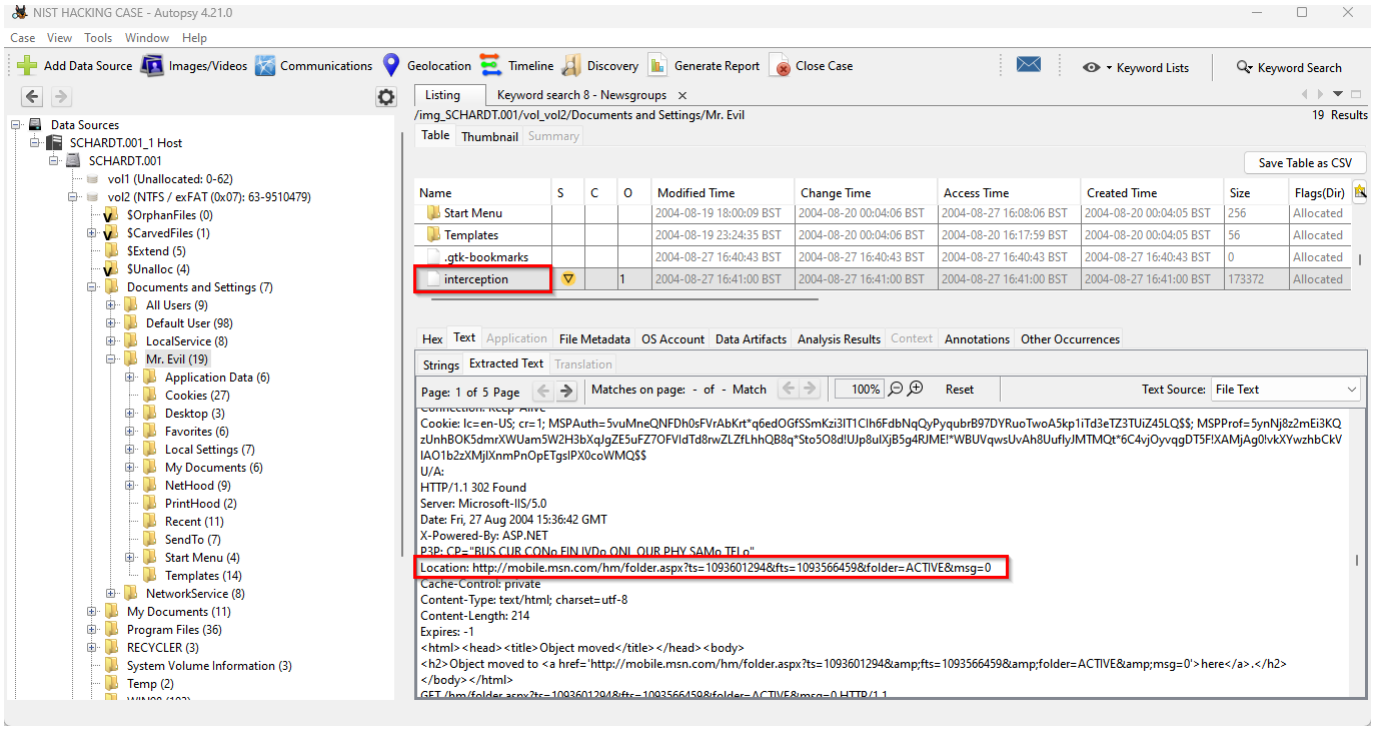
Q23. Victims Website Accessed

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.

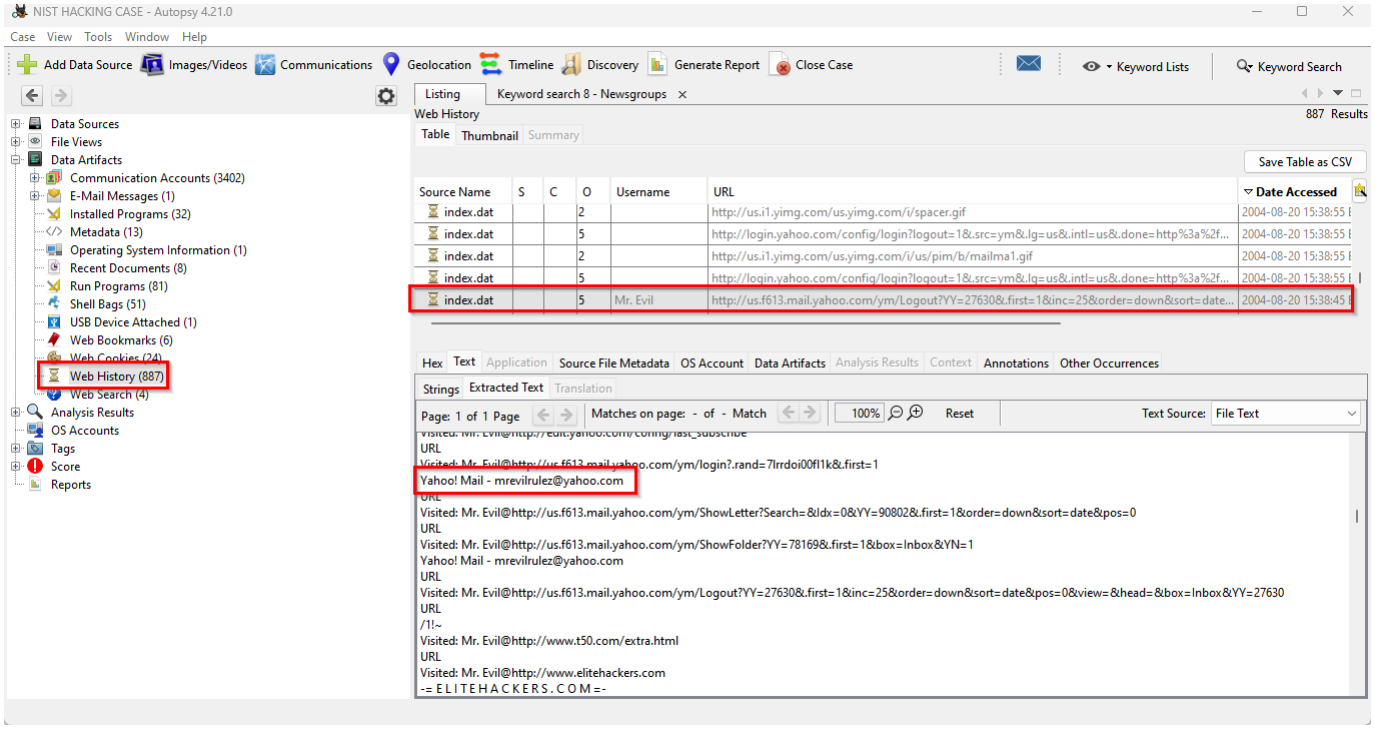


Q24. Users Web Based Email Address

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

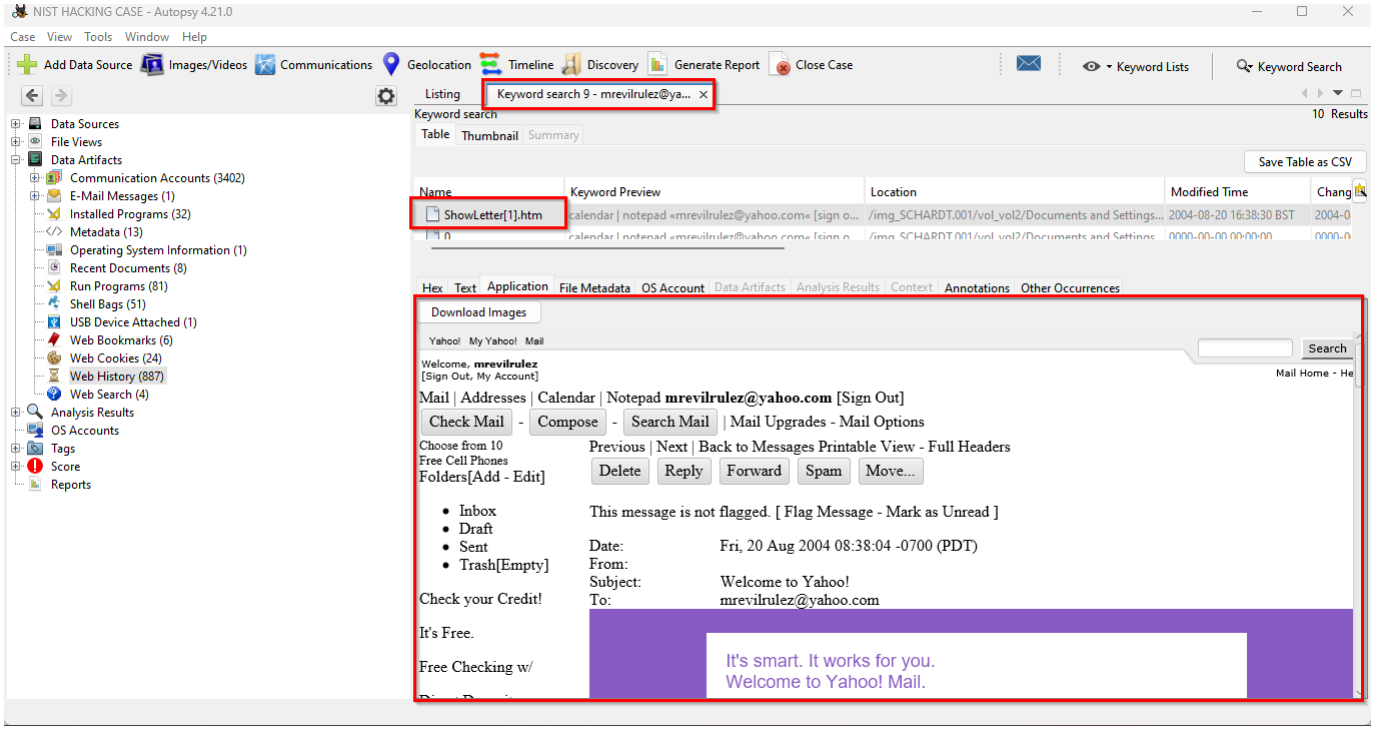


Q25. Yahoo File

File: ShowLetter[1].htm

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

Method: Keyword Search the Email.



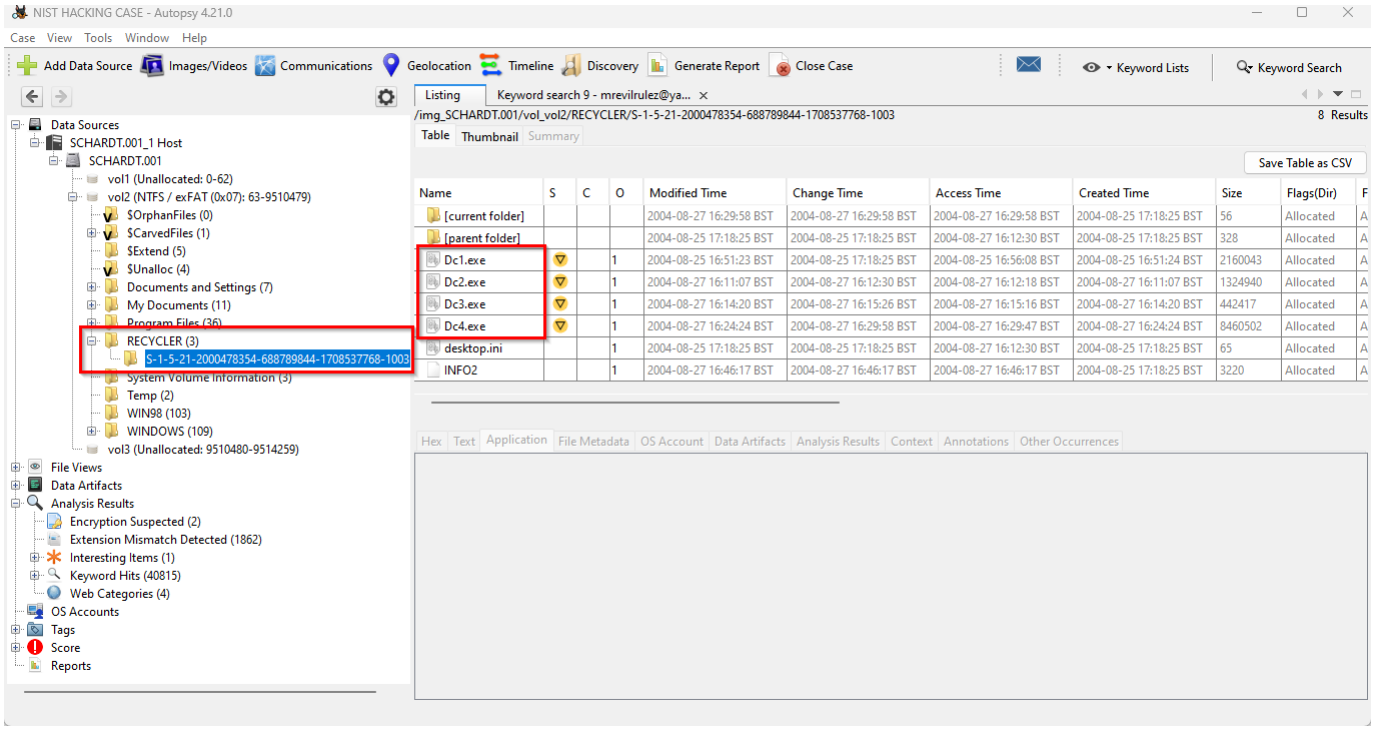
Q26. Executable files In RecycleBin

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



Q27 Really Deleted

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

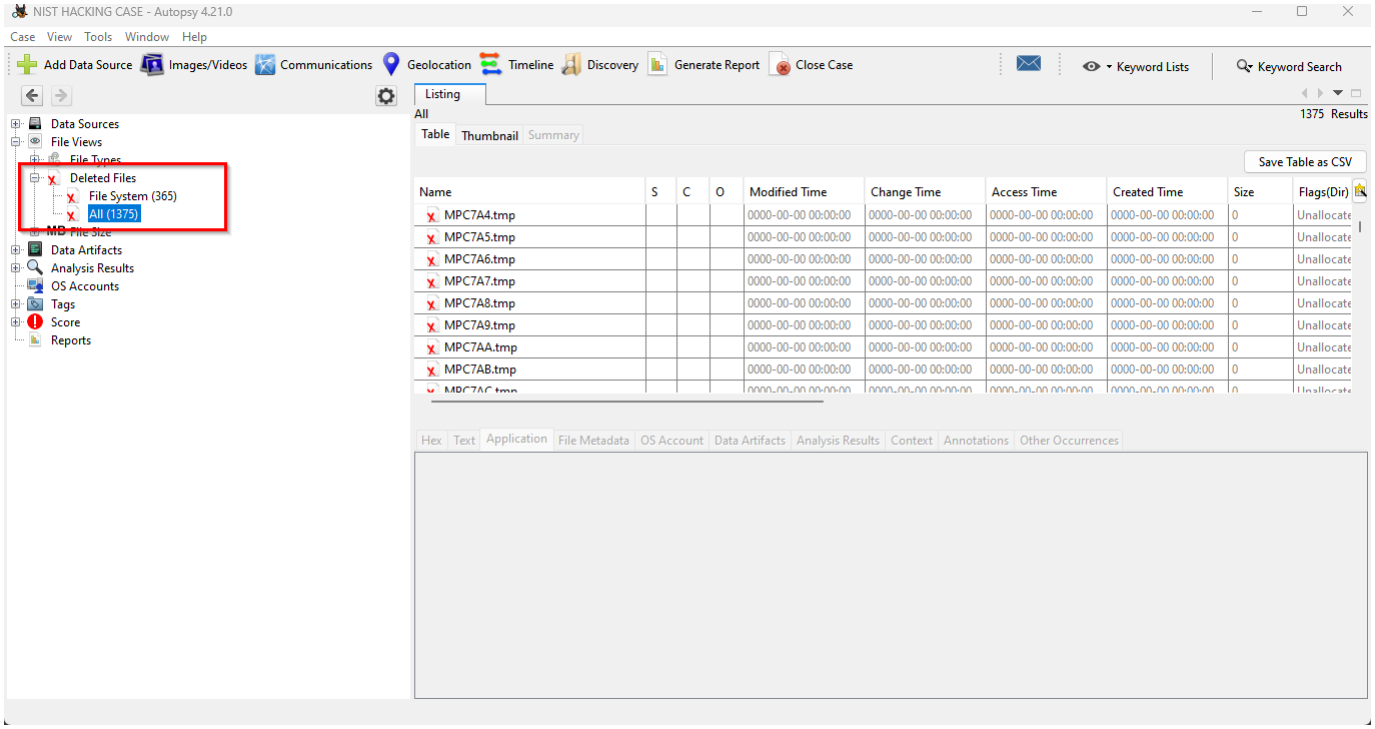
Q28. Reportedly Deleted

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.



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.