Digital Forensics Investigation of a Missing Laptop

Ashish Ahire, Ismail Bibers, Pradeep Mugithe

25th April 2023

Prof. Connie Justice

Purdue School of Engineering and Technology, IUPUI

Table of Contents

Executive Summary

The following executive summary is based on the digital forensics investigation of an abandoned Dell laptop, a wireless PCMCIA card, and an external homemade 802.11b antenna. The investigation aimed to find evidence of any hacking software or data generated by the attacker and determine the severity of the attack and potential data loss.

The investigation used industry-standard tools such as Autopsy and Kali Linux Forensic Mode to acquire digital evidence, and the analysis revealed the presence of several hacking tools and programs such as password-cracking tools, network sniffers, network scanners, and proxy tools. Additionally, frequent visits to online forums and websites related to hacking and illicit activity strongly suggested the involvement of the suspect "Mr. Evil," who was believed to be the same person as "Greg Schardt." However, the investigation was unable to definitively link the found laptop to the suspect.

Our investigation demonstrated the importance of digital forensics methods and processes in uncovering evidence related to cybercrime incidents. The findings highlighted the need for digital security measures to protect sensitive data and detect cyber threats. The evidence collected during the investigation can be used as legal evidence in a court of law.

Overall, the investigation provided valuable insights into the nature of the incident and the methods used by the hacker. The report emphasizes the importance of utilizing digital forensics techniques to detect and investigate cybercrime incidents, which can ultimately help prevent future incidents and safeguard critical data.

Overview/Case

Case

This digital forensics case involved an abandoned Dell notebook laptop that was suspected to have been used for hacking purposes. The notebook was found with a wireless PCMCIA card and an external homemade 802.11b antenna. It is believed that the suspect goes near the range of Wireless Access Points and intercepts internet traffic for hacking purposes such as obtaining credit card numbers, usernames, and passwords.

Overview

The case involves investigating Dell laptop, wireless PCMCIA cards, and homemade antennae that were found abandoned. The suspicion is that these devices were used for hacking purposes, specifically intercepting internet traffic to obtain sensitive information such as credit card numbers, username, password. The goal from this investigation is to find evidence of any hacking software or data that might have been generated.

As a digital forensic examiner/analyst in this scenario, the information regarding the issue at hand would include:

1. Details about the Dell laptop: This would include information such as the operating system, the type and capacity of the hard drive, installed software, and any user accounts or files stored on the laptop. An DD image can be created using dcfldd and dc3dd, which can be used to further analyze the data stored on the laptop hard drive.

2. The wireless PCMCIA card and external homemade 802.11b antenna: It's important to determine whether these devices were used for hacking. It is typically used for wireless

communication. Because the laptop has been set up to intercept wireless signals and gather information for malicious purposes such as unauthorized data collection. The attacker used these devices to increase the range and the strength of the wireless signal.

3. Any hacking software or tools found on the laptop: This would include any tools or software that were used for hacking, such as password cracking tools, network scanners, or other tools.

4. Network logs and traffic data: if possible, it would be very useful to obtain network logs and traffic data from the time period when the suspect was believed to have used the computer. This could provide valuable information about the types of all the activities the attacker engaged in and all the network connections that the attacker made.

5. Documentation of the forensic tools and techniques used.

The local police found the laptop along with a PCMCIA card and antennae, we were informed about the abandoned laptop and our team reached the site where it was found. Our team securely collected the devices without tampering them and documented the make, model, type, serial number, power state and condition of the devices. Each device was labeled and stored in the anti-static bags.

The collected devices were sent to the nearest Regional Computer Forensics Laboratory (RCFL), where the devices were processed and stored until the warrant was obtained to investigate the devices for evidence. After the warrant was issued, a DD image was created from the laptop using Kali Forensic mode, dcfldd and dc3dd. This DD image was further analyzed using Autopsy to find any hacking software was present on the laptop, any evidence which relates to the name of the suspected hacker and the data present on the laptop.

Objectives

The main objective of this case is to find and investigate if the suspected hacker used any hacking software, evidence of software being used, and any data that might have been generated by the hacker by intercepting the internet to get the credit card details, the customer's or the user's usernames and passwords. And investigating to check whether this found laptop has any ties to the suspect or not.

According to the information we've obtained from the suspect's associates, it is being said that the suspect parks his vehicle within the area of Wi-Fi hotspots like Starbucks and the T-Mobile store. They have also allegedly said that he uses this kind of Wi-Fi hotspots to go on the internet and then he tries to intercept the internet to get the customer's credit card numbers and then also their usernames and passwords too.

Based on the information we have collected till so far; it is assumed that an external attacker used advanced techniques and tools to exploit vulnerabilities in the system to carry out the hacking activity. The theft of private information, including financial or customer data, is thought to be the attacker's motivation.

A targeted investigation will be conducted as part of this investigation to find whether the hacker(s) specifically targeted any systems or data within the organization's infrastructure. Examining access logs, user account data, device storage bin, and other related information will be required for this.

In order to investigate the hacked systems and devices, this digital forensics investigation will specifically search for the following terms: "Evil and Greg Schardt or Greg". In this

investigation, the attacker or the suspect of the breach will be located, and the severity of the attack and any potential data loss will also be evaluated.

Evidence

Introduction

In computer forensics and as a digital forensic examiner, the evidence refers to digital information that is collected and analyzed for the purpose of investigating a crime. This evidence can include data from hard drives, mobile devices, network traffic, and other sources of digital information. Our goal as forensic examiners is to extract information from this evidence that can be used to identify the perpetrator or the cause of the breach.

The evidence is crucial in computer forensics because it is used to establish the facts of a case. It can help investigators identify the source of a breach, track the activities of a suspect, and provide evidence to support criminal charges. However, it is essential to handle the evidence carefully and follow the rules of evidence to ensure that it is admissible in court. This means that the original data should be touched as little as possible, and copies should be made for examination to avoid altering it. Additionally, compliance with the relevant rules of evidence, such as the chain of custody and the Daubert standard, is critical to ensure the admissibility of the evidence in court.

Chain of custody

The chain of custody is particularly important in criminal investigations and legal proceedings because it ensures that evidence is handled properly and remains intact and uncontaminated. It is a critical component of the justice system and is necessary for the prosecution to prove its case beyond a reasonable doubt. Without a clear and unbroken chain of custody, the integrity of the evidence may be compromised, and the evidence may be inadmissible in court.

The chain of custody also helps to protect the rights of the accused by providing transparency and accountability in the handling of evidence. It ensures that the evidence presented in court is reliable and that it has not been tampered with or altered in any way. The chain of custody is an essential part of due process, and failure to maintain it can lead to legal challenges and appeals. Overall, the chain of custody is a crucial aspect of any legal investigation or proceeding, and it plays a vital role in upholding the principles of justice and fairness.

The evidence for this hacking case includes a laptop Dell CPi notebook, a wireless PCMCIA card, an external homemade 802.11b antennae, and A DD image and EnCase image of the computer that have been created as part of the investigation.

Sr. No.	**Items**	**Description**
1.	Dell CPi notebook computer	**Make:** Dell **Model:** CPi **Serial#:** VLQLW The laptop was used for hacking purposes and contains all the data which was intercepted by the hacker.
2.	Laptop Hard Drive	**Model:** “IBM-DBCA-204860”

		Serial#: "HQ0RQQF7429" **Drive Size:** 4.5 GB All the intercepted data is present in the hard drive and creating a DD image of the hard drive would help the examiner investigate the data.
3.	Wireless card PCMCIA	The hacker might have used this device as an adapter to connect the homemade antenna.
4.	Homemade 802.11b antennae	The antenna was used to increase the strength and range of the signals.
5.	DD Image	The DD image was created from the laptop hard drive and divided into 8 parts.
5.1.	SCHARDT.001	**MD5 Hash value:** 28A9B613 D6EEFE8A 0515EF0A 675BDEBD **Sectors:** 1301248

5.2.	SCHARDT.002	**MD5 Hash value:** C7227E7E EA82D218 66325739 7679A7C4 **Sectors:** 1301248
5.3.	SCHARDT.003	**MD5 Hash value:** EBBA35AC D7B8AA85 A5A7C13F 3DD733D2 **Sectors:** 1301248
5.4.	SCHARDT.004	**MD5 Hash value:** 669B6636 DCB4783F D5509C47 10856C59 **Sectors:** 1301248
5.5.	SCHARDT.005	**MD5 Hash value:** C46E5760 E3821522 EE81E675 422025BB **Sectors:** 1301248
5.6.	SCHARDT.006	**MD5 Hash value:** 99511901 DA2DEA77 2005B5D0 D764E750 **Sectors:** 1301248

5.7.	SCHARDT.007	**MD5 Hash value:** 99511901 DA2DEA77 2005B5D0 D764E750 **Sectors:** 1301248
5.8.	SCHARDT.008	**MD5 Hash value:** 8194A79A 5356DF79 883AE2DC 7415929F **Sectors:** 405524

Table 1. Evidence Details

Analysis

Digital forensic analysis is the process of examining digital devices and data in order to uncover evidence related to a computer crime or other digital incident. This can include analyzing hard drives, USB drives, mobile devices, and network traffic to recover deleted files, track user activity, and identify malicious software or hacking attempts. The digital forensic analysis uses specialized tools and techniques to preserve the integrity of the data and ensure that it can be used as evidence in a court of law.

The first and most critical step in the analysis was to preserve and acquire the digital evidence. As we said in the previous section, we made sure to gather the original evidence to prevent any changes to the original data. We used industry-standard tools such as Autopsy and Kali Linux Forensic Mode for the acquisition and analysis of the evidence. The forensic images were then verified using hash values to ensure their integrity.

Acquisition of Evidence

As an examiner/analyst, we first made a copy of the evidence so that the original evidence remains secure and untouched if anything goes wrong while investigating. We used the open source operating system, Kali Linux 2022.4 in Forensic mode for acquisition of evidence. As the evidence was divided into 8 parts, we reconstructed the drive image using Kali Linux. In Kali Linux, using the cat command, the evidence image was reconstructed. The reconstructed drive image was created in .IMG format which is acceptable format in Autopsy for analysis. The image was then securely transferred to the Windows system so that the image can be further investigated and analyzed using Autopsy. The figure 1 below shows the reconstructed image in Kali Linux.

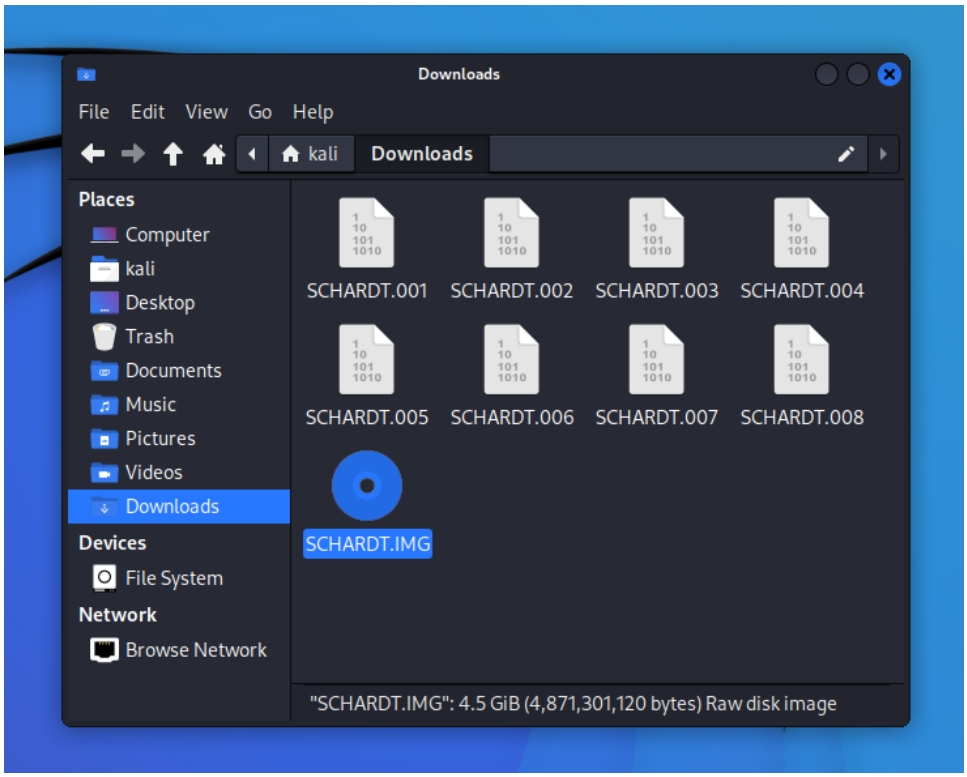


Figure 1. Reconstructed Image in Kali Linux

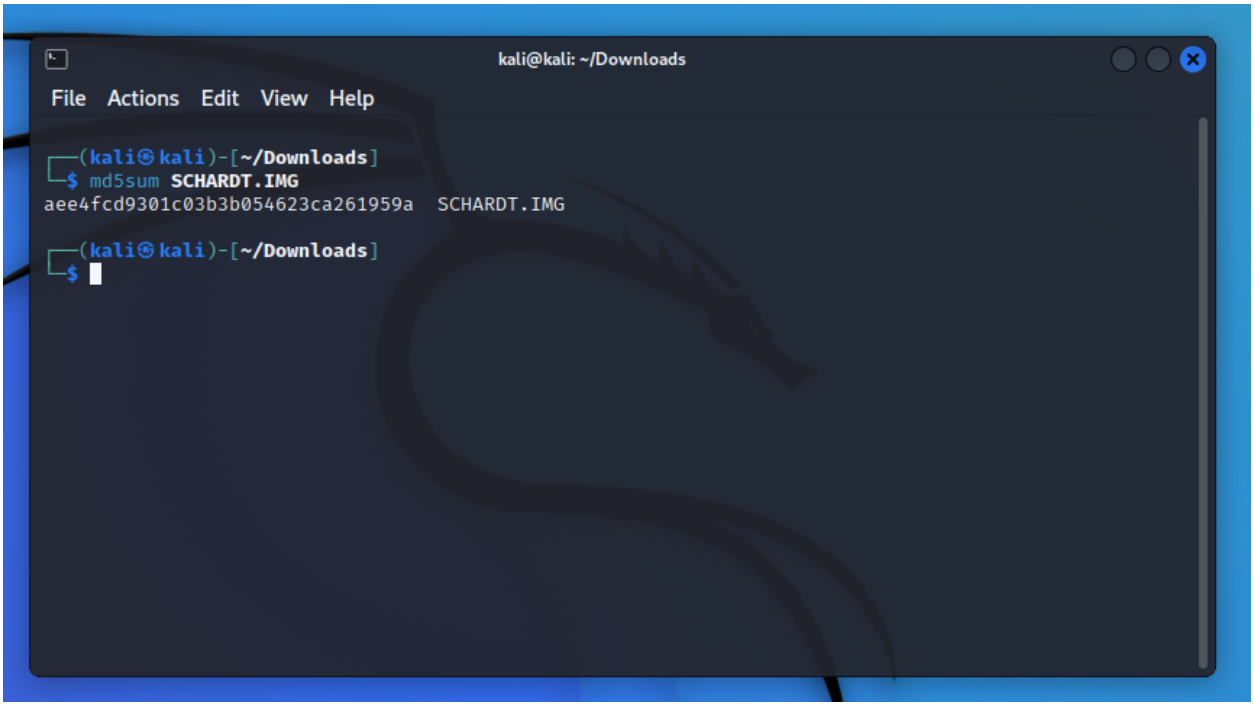


Figure 2: MD5 hash of the reconstructed image

The figure 2 shows the MD5 hash value of the reconstructed image in Kali Linux. This hash value is important because it can be used by the examiner to verify the integrity of the evidence image after transferring it to Windows system for analysis using Autopsy

Analysis of Acquired Evidence:

On the windows system, Autopsy 4.20.0 was used to investigate and analyze the hard drive image. A new case was created on Autopsy using the case name “Hacking” and case number “1” was provided and the details of the examiner like name, phone number, and email were included. Figure 3 below shows the case details in Autopsy. After the case was created, the hard drive image was added as a data source and all ingest modules were run on the hard drive image to discover relevant findings. Figure 4 shows the evidence image being added as data source in Autopsy.

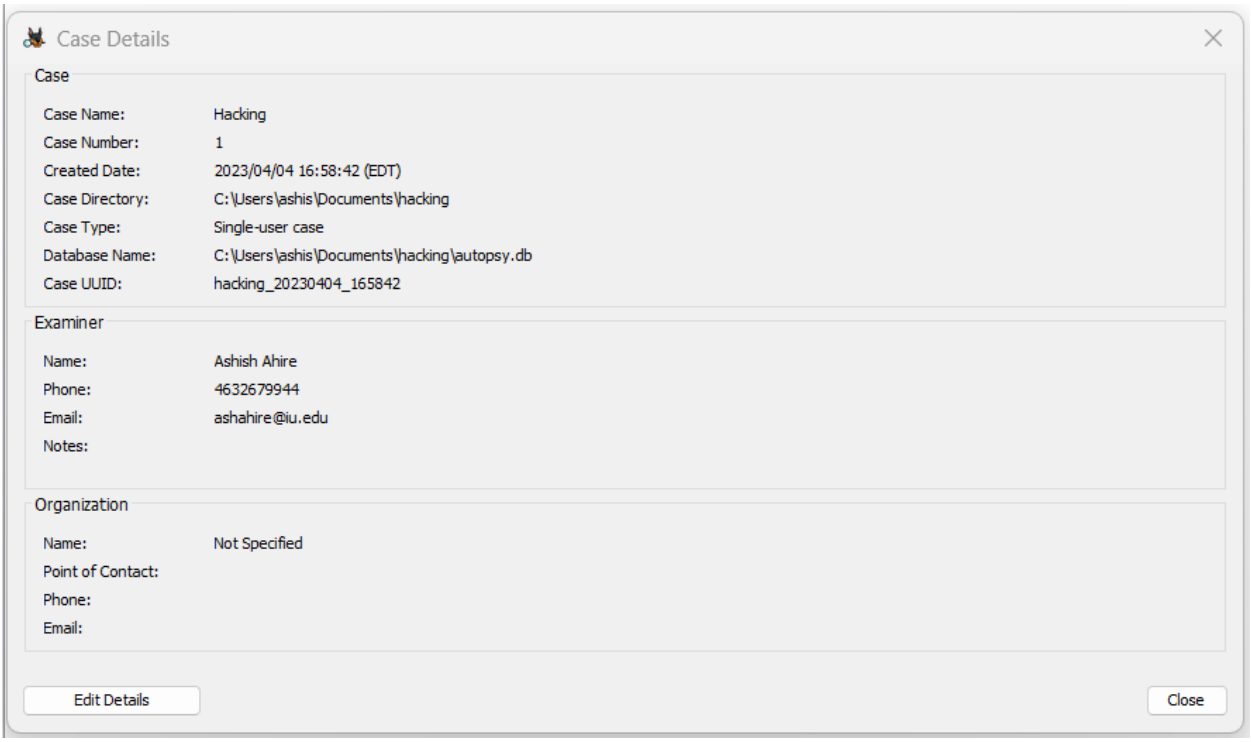


Figure 3: Case Details

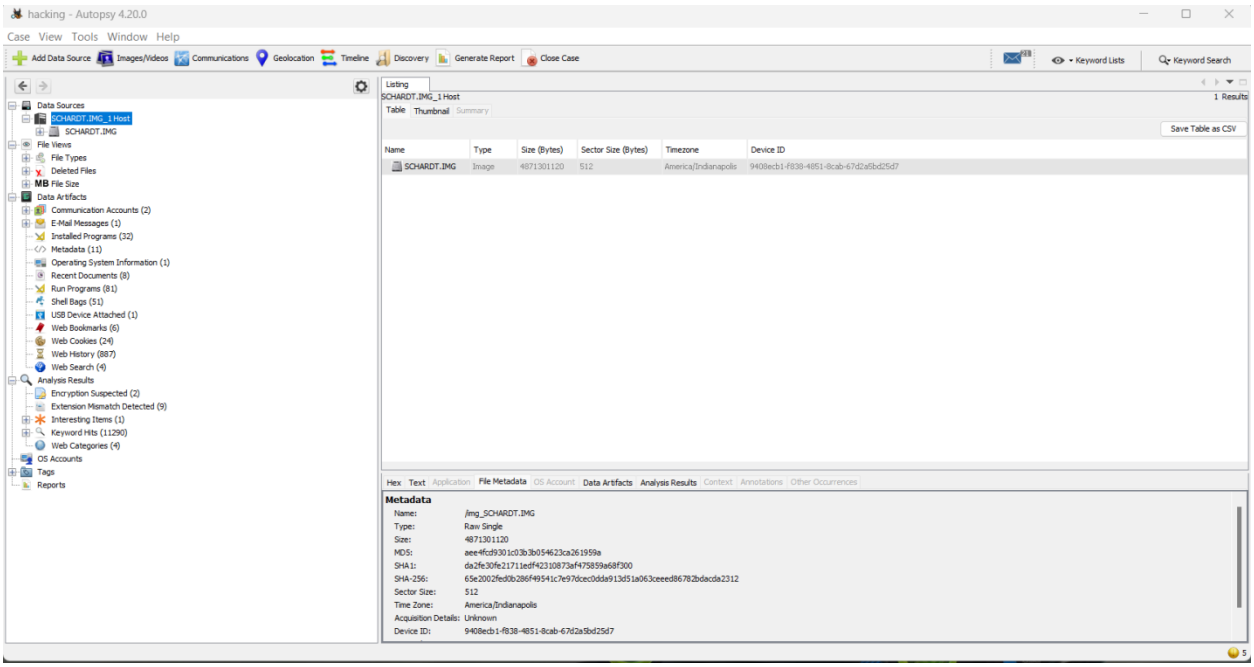


Figure 4. Drive image added to Autopsy

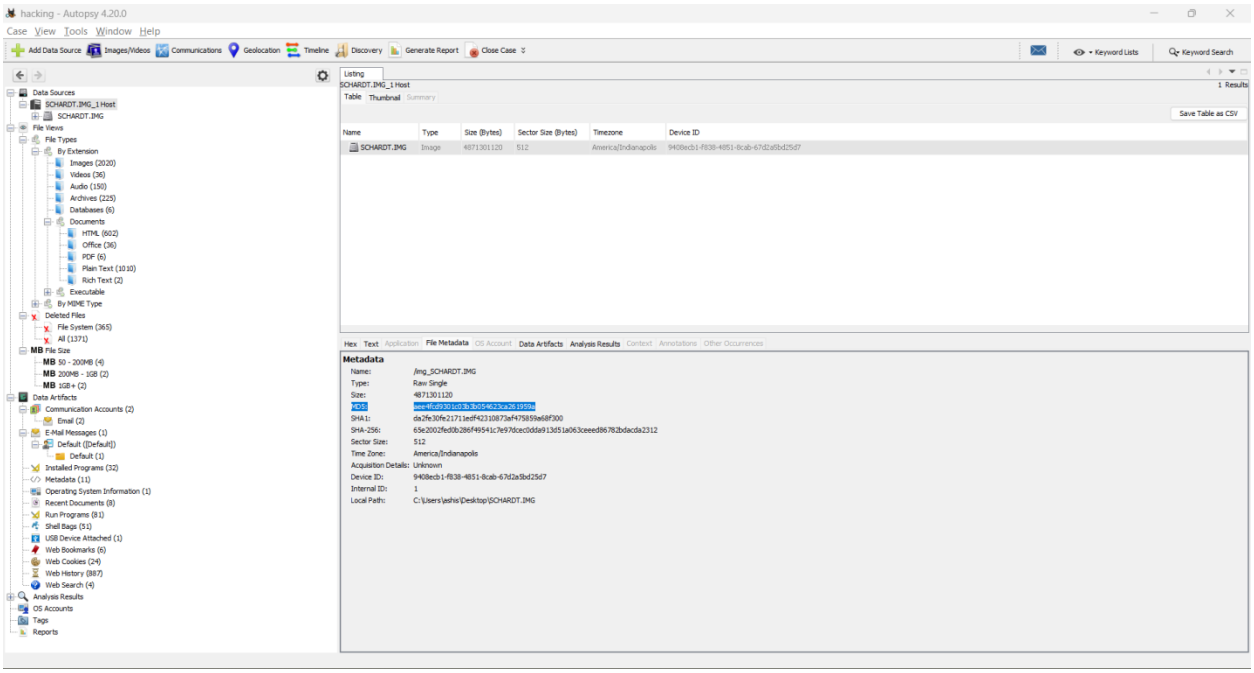


Figure 5. Hash values of image in Autopsy

Figure 5 shows the three different verification hash values which are MD5, SHA1 and SHA256, these hash values can be used to compare with acquisition hash value and image drive can be checked for integrity.

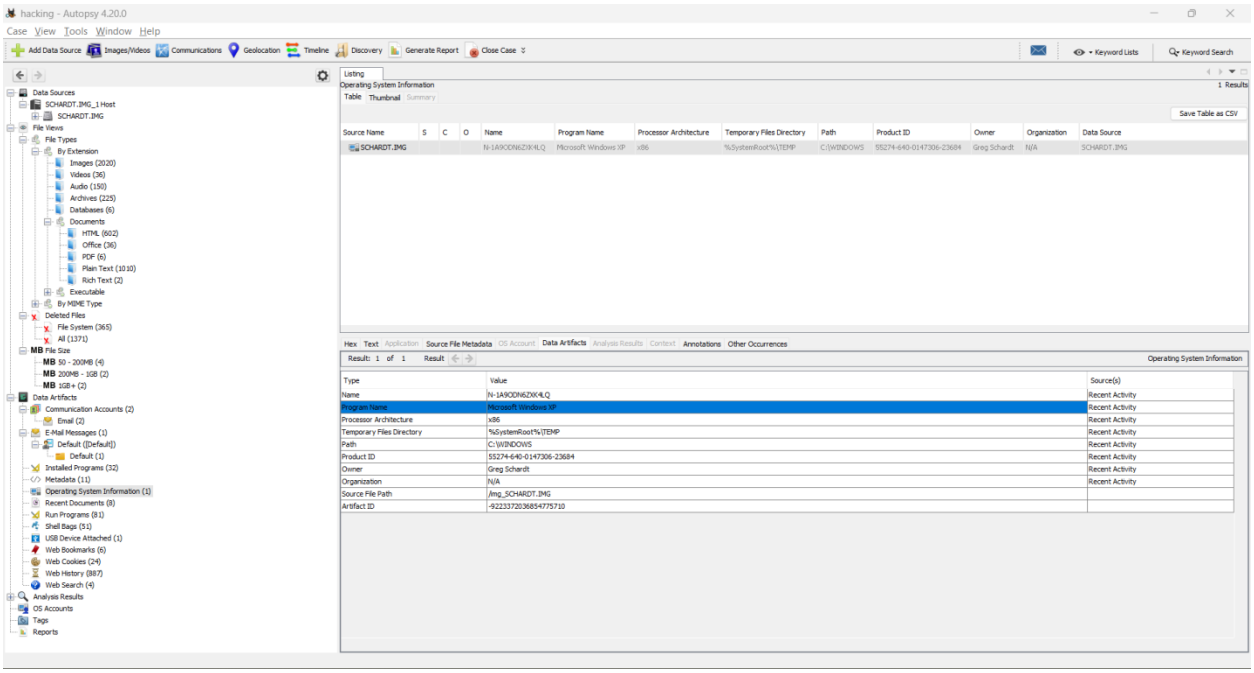


Figure 6. Details of OS and Owner

Details of the Operating system and the owner name of the system can be seen in figure 6 and also the processor architecture can be known from figure 6. The name of the owner of the laptop can help us link him to the suspected hacker.

In figure 7, all the OS accounts that were created can be observed. These accounts can link us to the user of the system and hence, help us find the hacker.

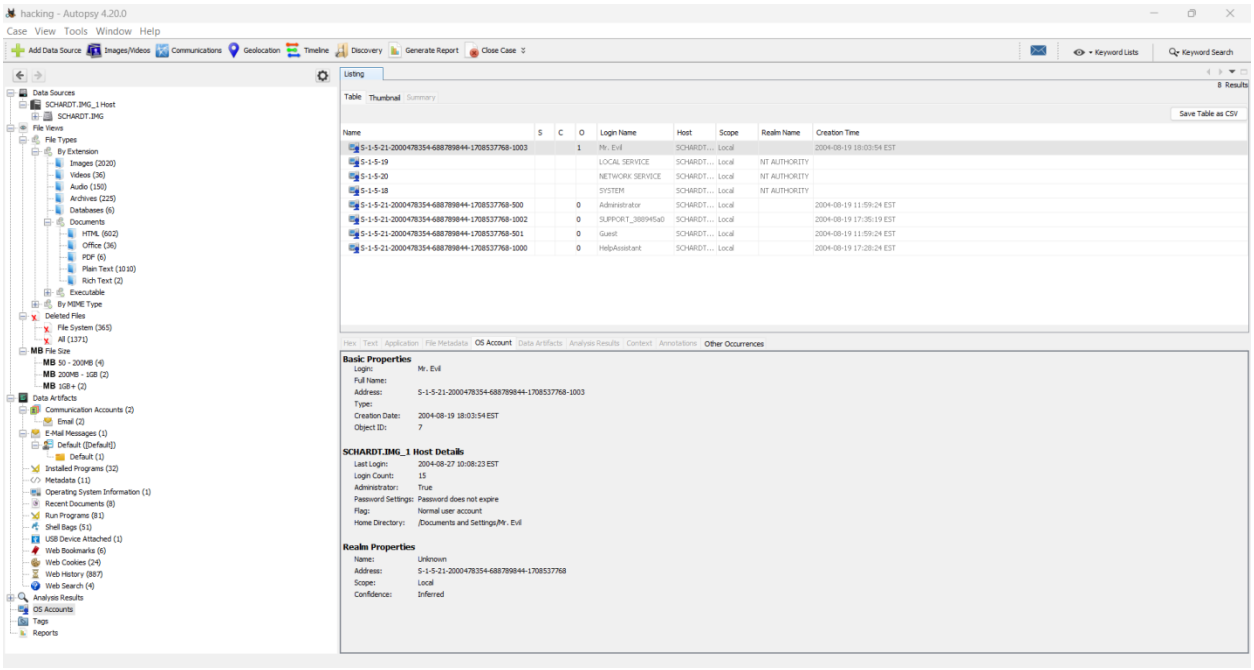


Figure 7. OS Accounts

Figure 8 shows all the programs that were installed on the system. In this list, there are few hacking tools that the hacker might have used to gain information of connected users to the nearby network devices.

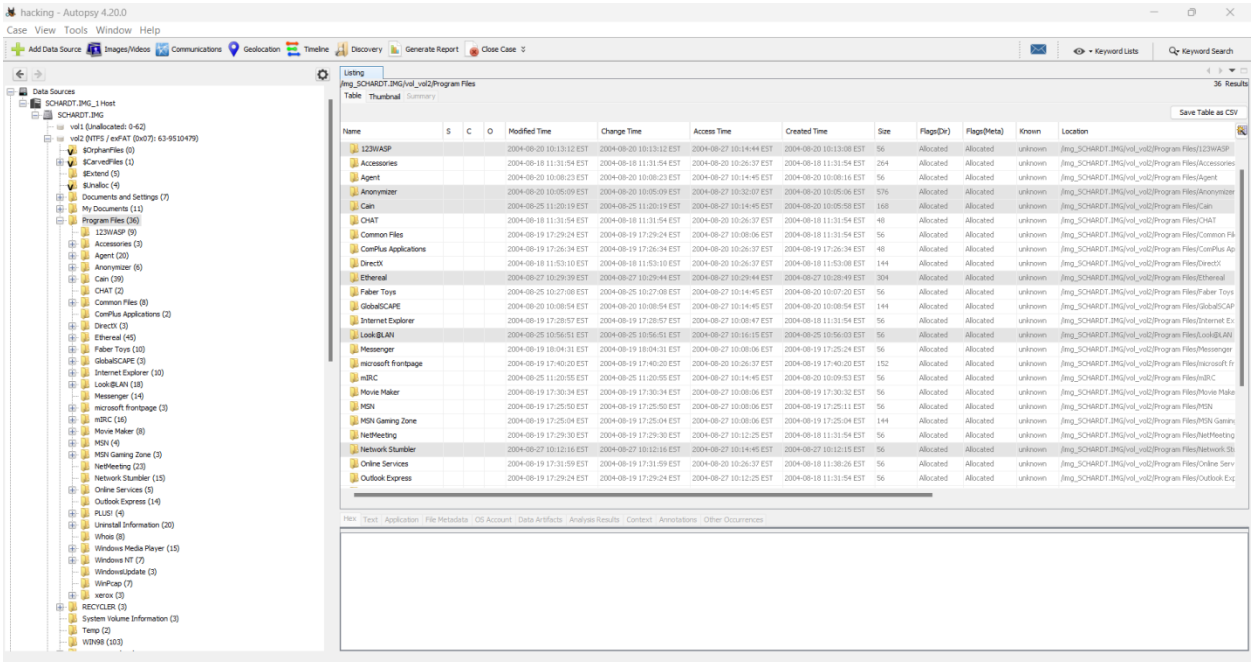


Figure 8. Some Hacking tools found

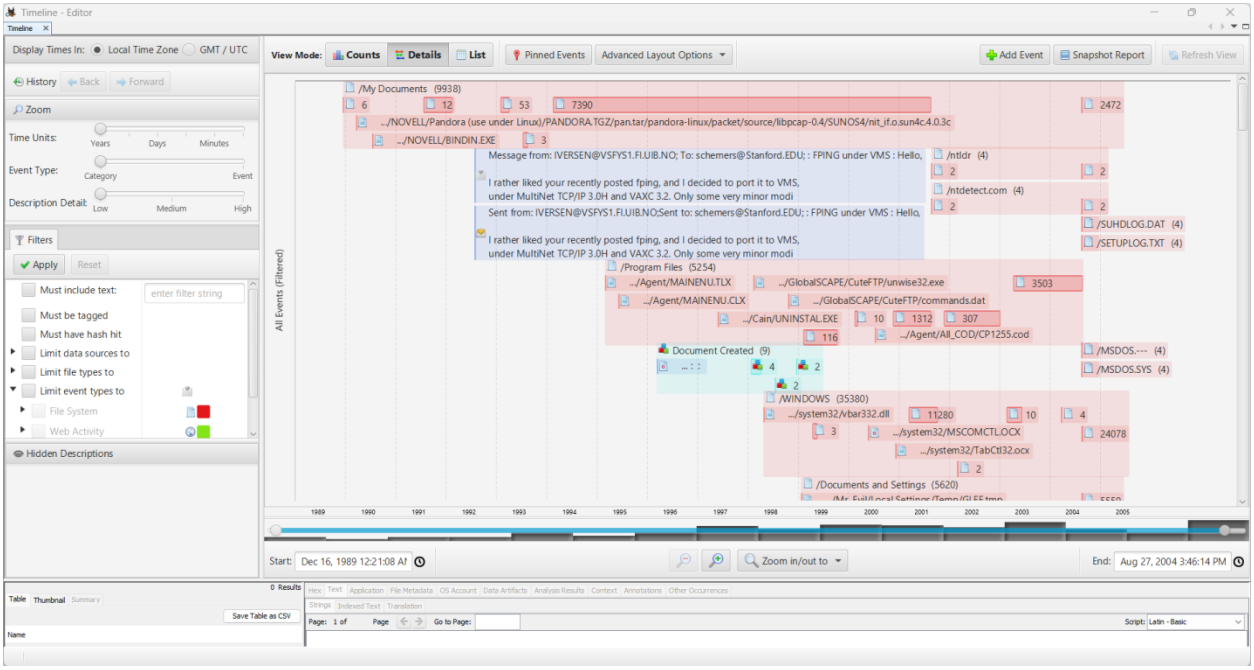


Figure 9. Timeline

Using the timeline shown in figure 9, files can be checked based on the date and time they were created on the system. Some important files that were created in the year 2004 can help us find the suspected hacker.

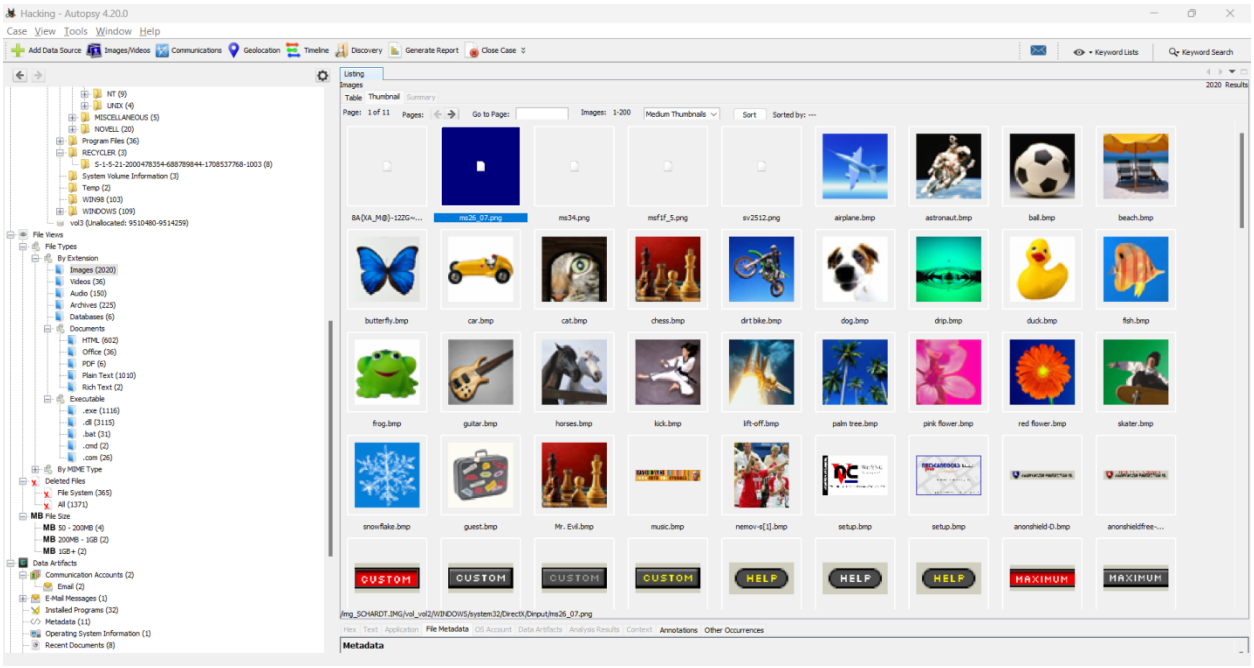


Figure 10. Images in system

Large number of images were found on the system. Some images aren't viewable and are in PNG format. Figure 10 shows a few images found on the system. These images might contain hidden information, which is hidden in images using steganography techniques.

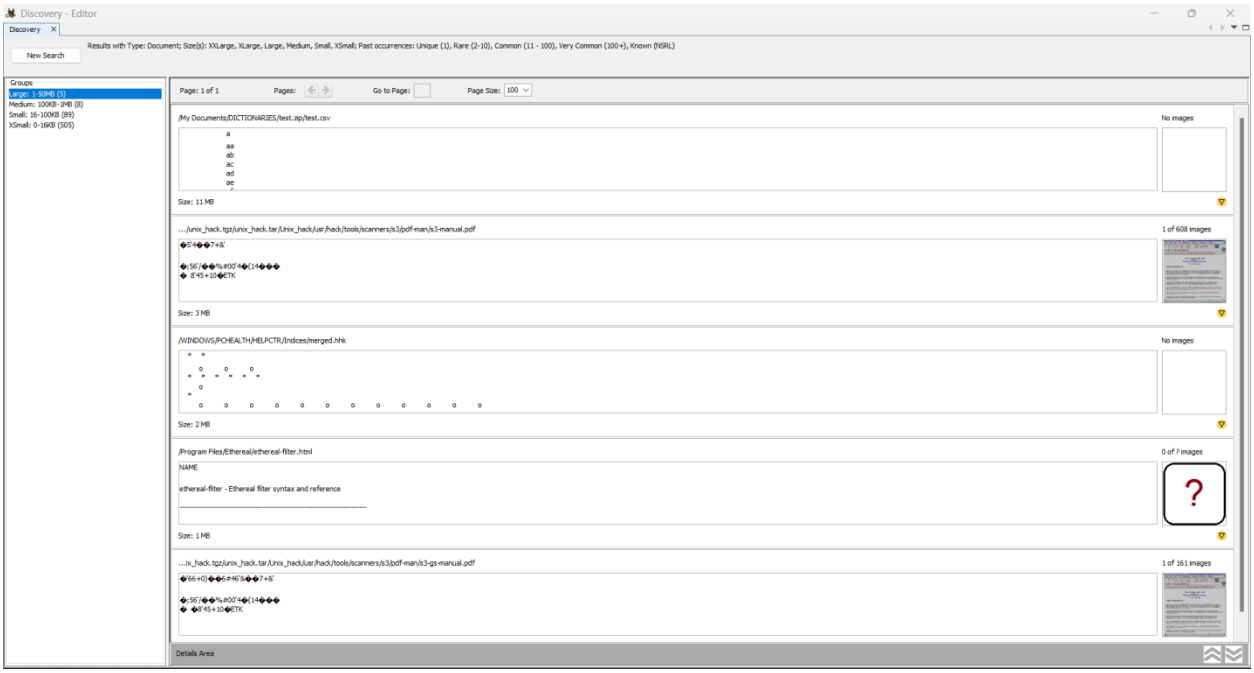


Figure 11. Documents found on system

Many documents are found on the system. These documents include manuals, dictionary files, etc which might have been used for hacking purposes. Figure 11 shows the found documents in the system.

Relevant Findings

Introduction

During the analysis of the laptop drive image, we found several relevant findings that can help determine what activities were performed using the device and who may have been responsible for performing those hacking activities. These findings include evidence of unauthorized access to the laptop, indications of data theft or deletion, network activity logs, and user activity logs.

In this part of the investigation, we will focus on the relevant findings that can shed light on the suspected hacker's activities performed using the laptop. By analyzing these findings, we can gain

valuable insight into hacking tools used by the hacker, network traffic intercepted and hence identify the potential suspect “Greg Schardt”.

The Image Hash

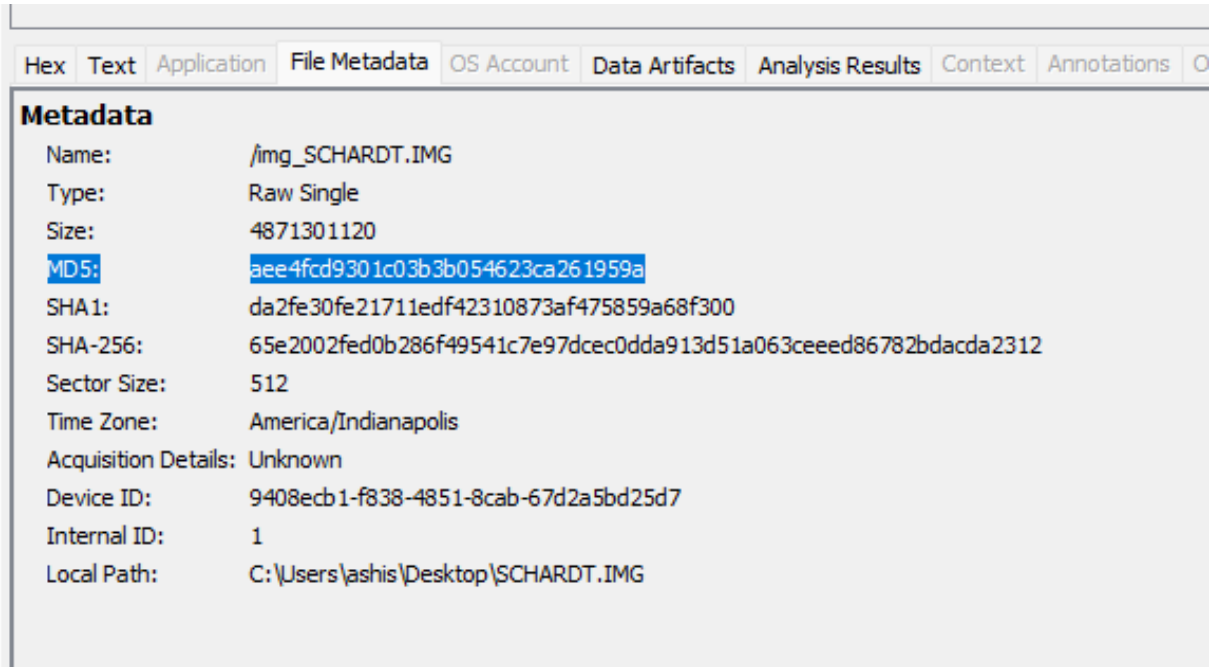
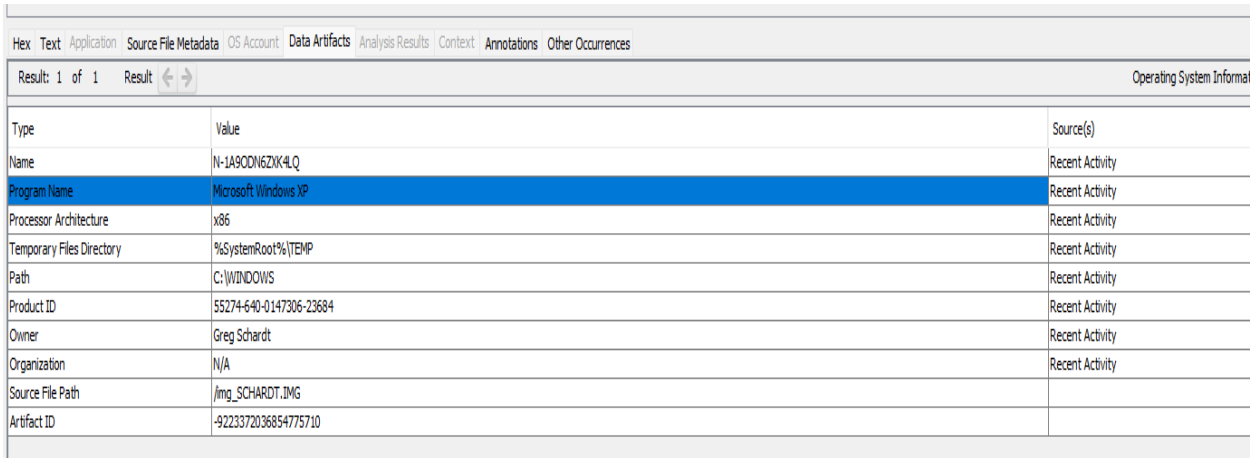


Figure 12. MD5 hash image

In the context of this investigation, the concept of image hash pertains to the utilization of the MD5 hashing algorithm to generate a unique digital fingerprint or signature for a given image file. The main purpose is to determine if the acquisition hash and the verification hash match with each other, which would indicate that the original image file has not been changed.

In light of the evidence collected during this investigation, the verification hash for the image in Figure 12 has been identified as “aee4fcd9301c03b3b054623ca261959a”. When the hash in figure 2 was compared with the hash in figure 12, it was found that the acquisition hash and verification hash match.

The Operating System used



Type	Value	Source(s)
Name	N-1A9ODN6ZXK4LQ	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.IMG	
Artifact ID	-9223372036854775710	

Figure 13. The Operating System used on the laptop

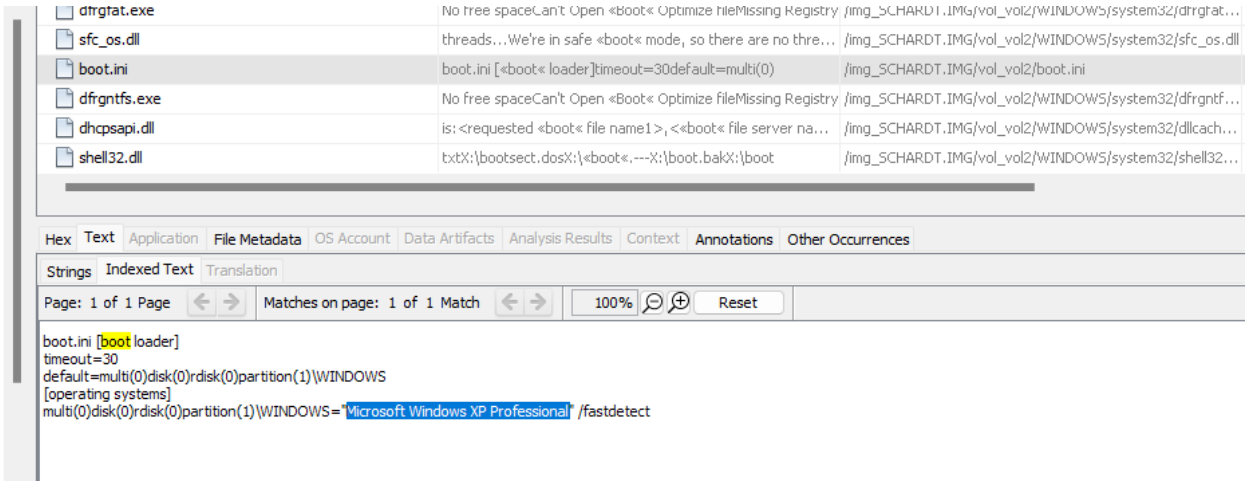


Figure 14. Operating System on Laptop

There were two methods employed in order to determine the operating system used on the computer. According to Figure 13, The first method involved collecting acquisition details related to the computer's hardware and software configuration, which provided relevant information pertaining to the operating system. According to Figure 14, The second method involved locating a file named "boot.ini", located at the path "C:\boot.ini", which explicitly indicated the operating system being utilized as Microsoft Windows XP Professional.

Through a meticulous analysis of these sources of information, it has been concluded that the operating system used on the computer was indeed **"Microsoft Windows XP Professional"**. The integrity and accuracy of the findings were thoroughly verified, ensuring that the final determination of the operating system is reliable and credible.

OS installation date

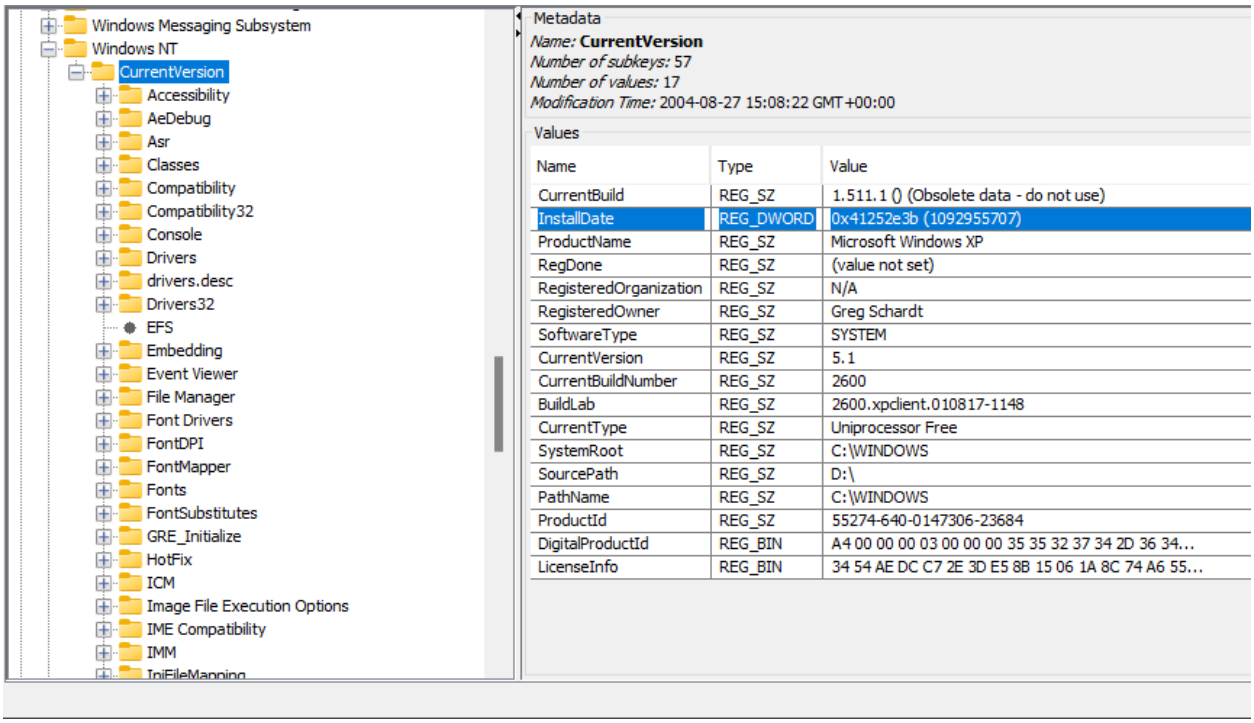


Figure 15. OS installation date.

Figure 16. Timestamp to date converter.

It was deemed necessary to determine the installation date of the operating system on the computer. After a thorough analysis of the available evidence, it has been determined that the installation date of the operating system was on **Thursday, August 19, 2004, at 5:48:27 PM GMT -05:00 (EST).** This information was derived from the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Install Date,** which is stored in the file path: **C:\Windows\system32\config\Software\Microsoft\Windows NT\CurrentVersion\InstallDate**

It should be noted that the time value stored in the registry key is in the UNIX time format, which requires conversion to accurately determine the installation date. This was done with precision and care using a timestamp converter, [4] to ensure that the findings are valid and reliable. Figure 16 shows the conversion of UNIX timestamp to human readable date. The installation date of the operating system is a crucial piece of information that sheds light on the history and usage of the computer, and its determination is an important step towards understanding the nature of the investigation.

Timezone settings

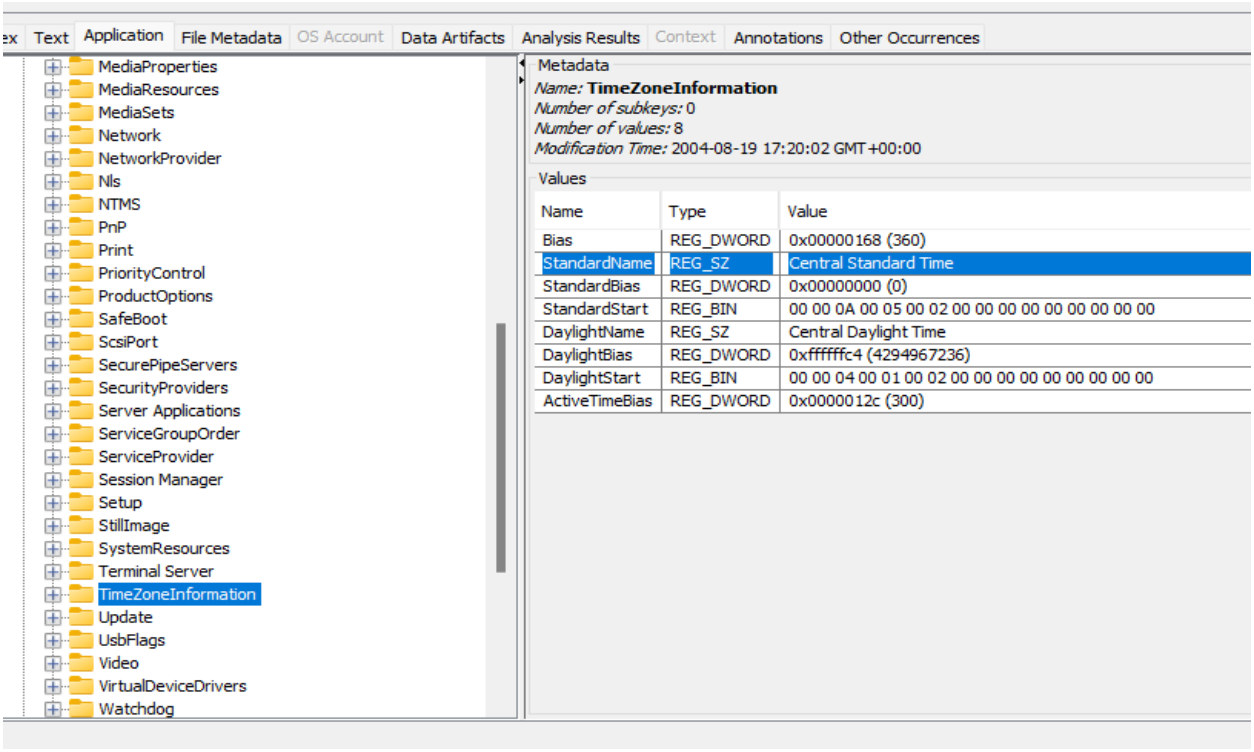


Figure 17. Timezone settings

From figure 17, it has been ascertained that the timezone settings were configured to Central Standard Time. This information was retrieved from the registry key **HKEY_LOCAL_MACHINE\system\ControlSet001\Control\TimeZoneInformation,** which is stored in the file path: **C:\windows\system32\config\system\ControlSet001\Control\TimeZoneInformation.**

The identification of the timezone settings is a crucial aspect of the investigation, as it helps to establish the temporal context of the activities and events that took place on the computer. The accuracy and reliability of the findings have been thoroughly verified, ensuring that the conclusion is trustworthy and credible. By ascertaining the timezone settings of the computer, investigators can gain valuable insights into the potential correlation between the actions taken on the computer and the corresponding time frames in which they occurred.

Registered Owner

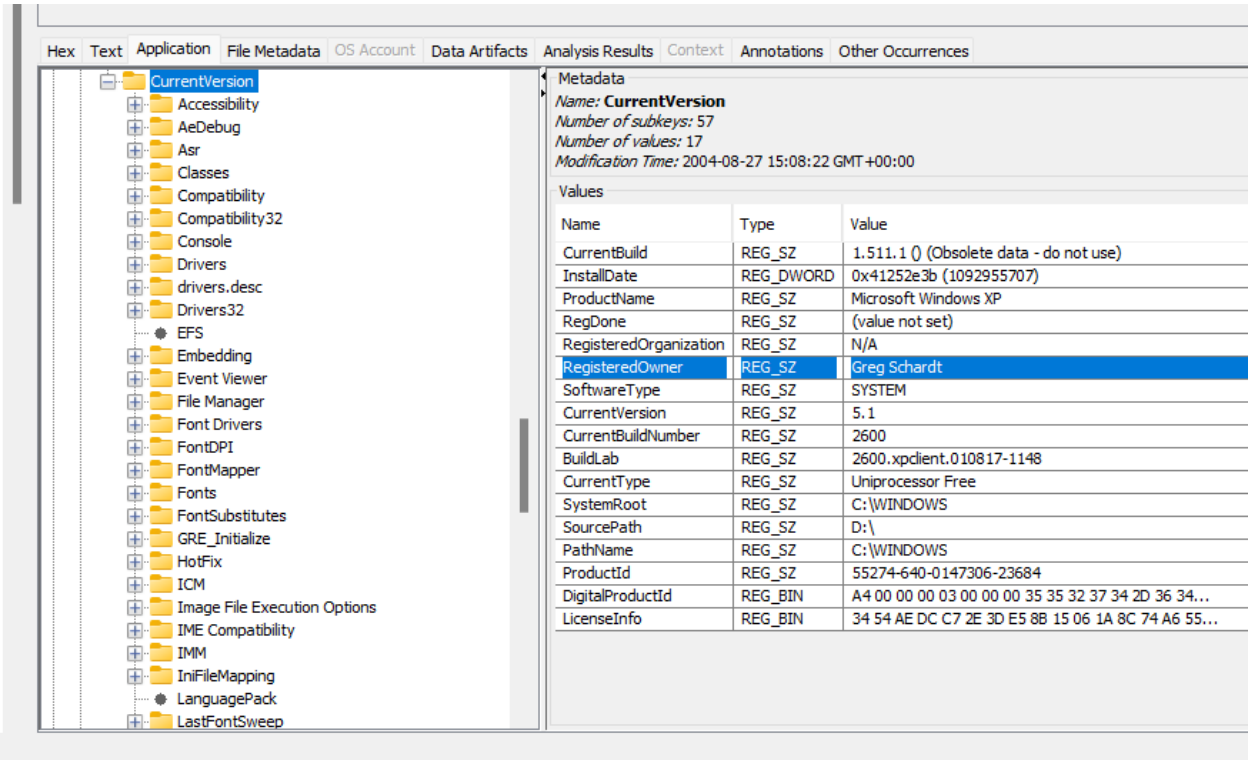


Figure 18. Registered Owner

According to figure 18, the name of the registered owner of the laptop is “Greg Schardt”. He is believed to be the suspected hacker. This finding is an important proof that it was Greg who owns the laptop and used to go near wireless access points and use it to intercept network traffic to obtain user information.

The information about registered owner was retrieved from registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\RegisteredOwner,** which is stored in the file path: **C:\Windows\system32\config\Software\Microsoft\WindowsNT\CurrentVersion\RegisteredOwner**

The name of the suspected hacker being known is a breakthrough for investigators, further findings against Greg would make the case more stronger.

Computer User

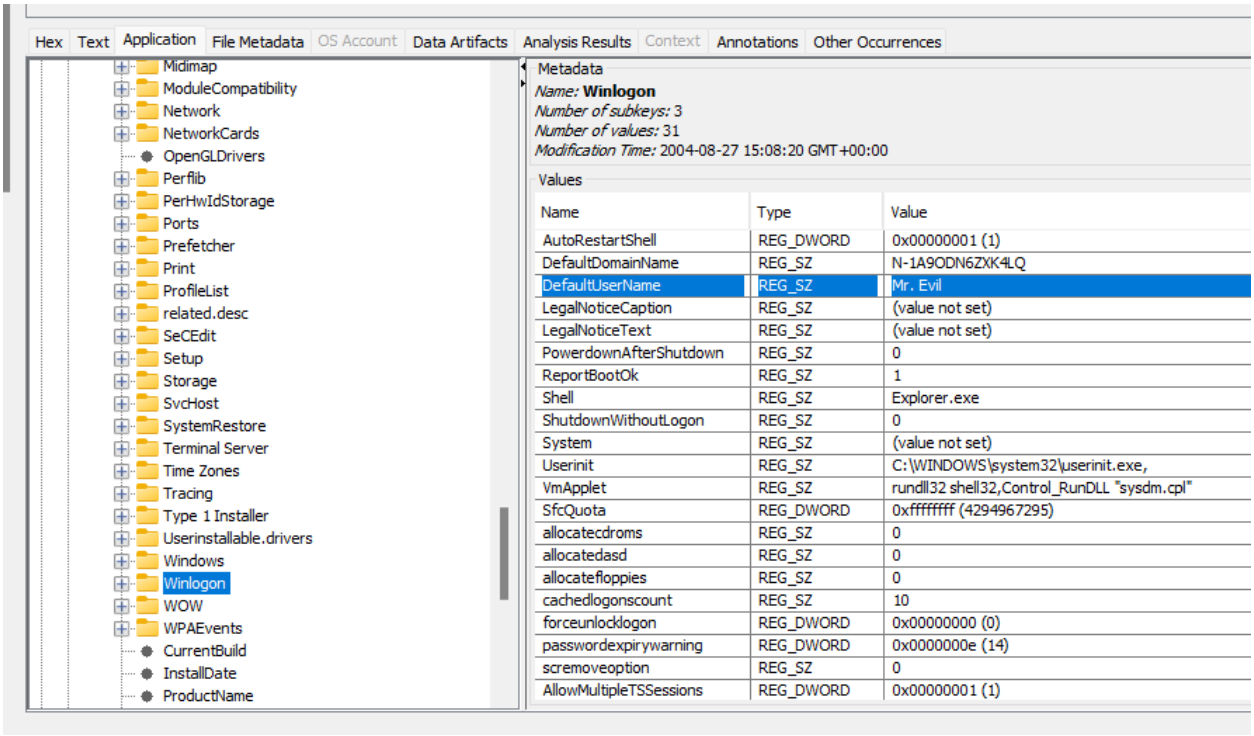


Figure 19. Computer account name

The name of the user using the laptop is very important because in many cases, most of the hackers use stolen laptops/computers for hacking and hence name of the user and registered owner might be different.

The information about the computer user name was retrieved from registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon,** which is stored in the file path: **C:\Windows\system32\config\Software\Microsoft\Windows NT\CurrentVersion\Winlogon**

The name of the computer user found on the system and as shown in the figure 19 is “Mr. Evil”. Now, it is important to determine whether Greg Schardt and Mr. Evil are the same person or not. We will find it out in further findings.

Primary Domain Name

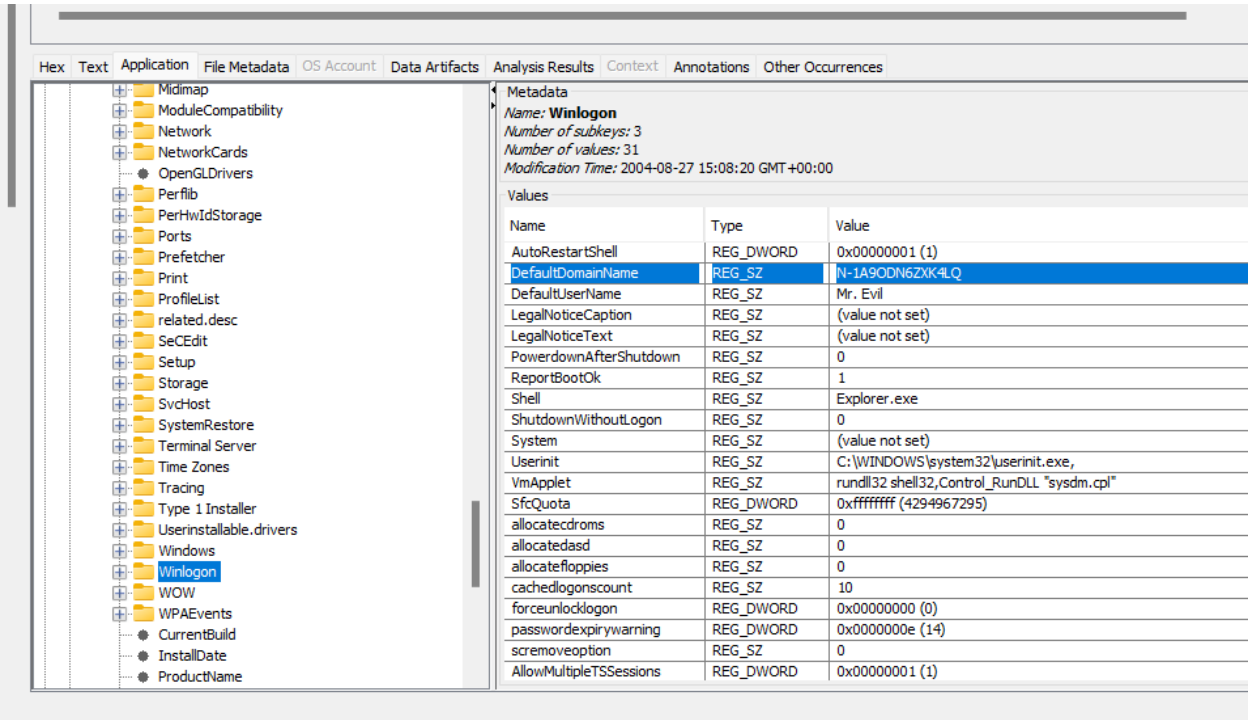


Figure 20. Primary domain name

The domain name is a unique identifier for a system in the network. No two systems can have the same domain name. The domain name information was retrieved from registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon,** which is stored in the file path: **C:\Windows\system32\config\Software\Microsoft\Windows NT\CurrentVersion\Winlogon**

The primary domain name found according to figure 20 using Autopsy is “N-1A9ODN6ZXK4LQ”.

Computer Shutdown Time

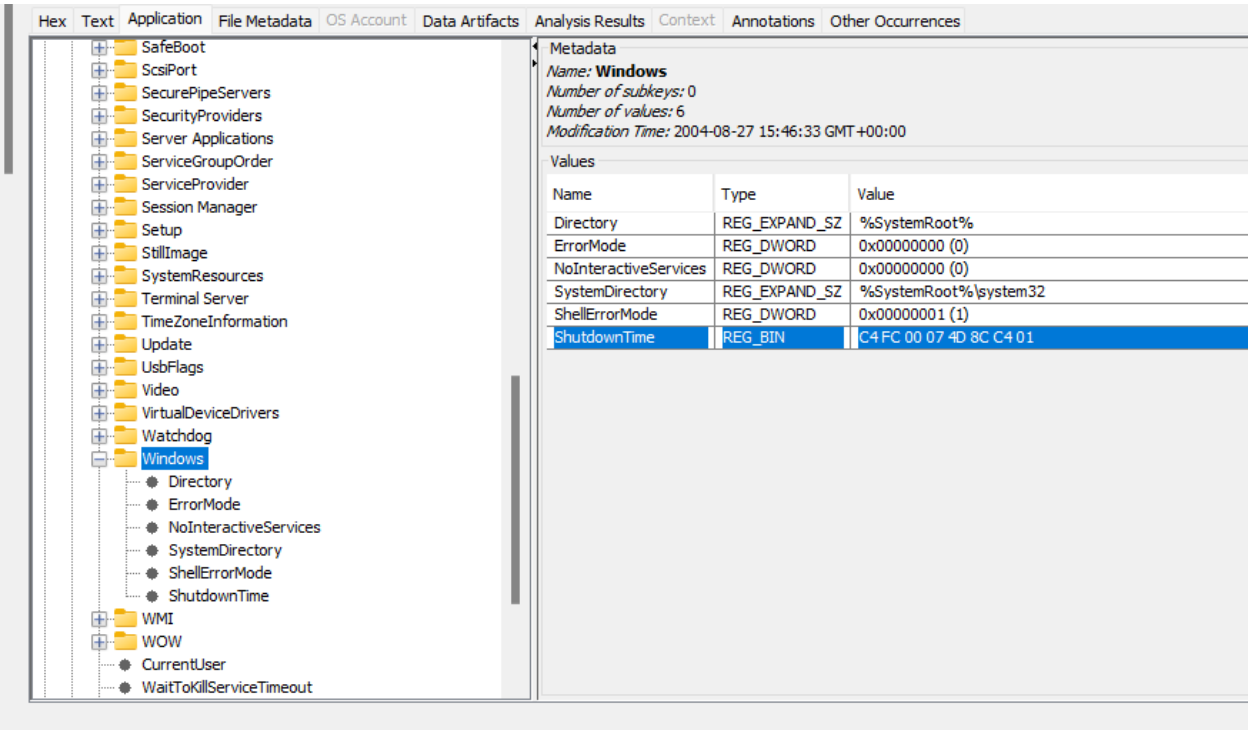


Figure 21. Computer shutdown date/time

The date and time when the laptop was shutdown is very important for the examiner as it determines when the laptop was last used before shutdown. This helps the examiner determine what tasks were done on the laptop a day or week before the shutdown. The computer shutdown date and time was retrieved in Windows 64bit Hex format from registry key **HKEY_LOCAL_MACHINE\system\ControlSet001\Control\Windows/ShutdownTime,** which is stored in the file path: **C:\windows\system32\config\system\ControlSet001\Control\Windows/ShutdownTime**

According to figure 21, the computer shutdown date/time found was “C4 FC 00 07 4D 8C C4 01”. This Windows 64bit Hex timestamp was converted into date and time using Windows

64bit Hex (Little Endian) converter, [5] so the shutdown date and time is "27 August 2004, 15:46:33 UTC". The converted date and time can be observed in figure 22.

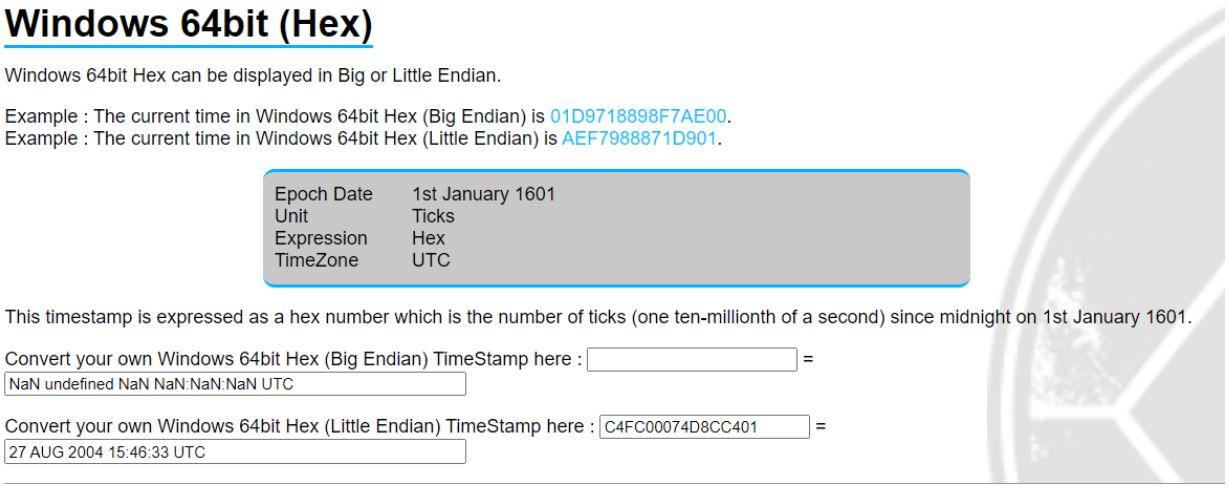
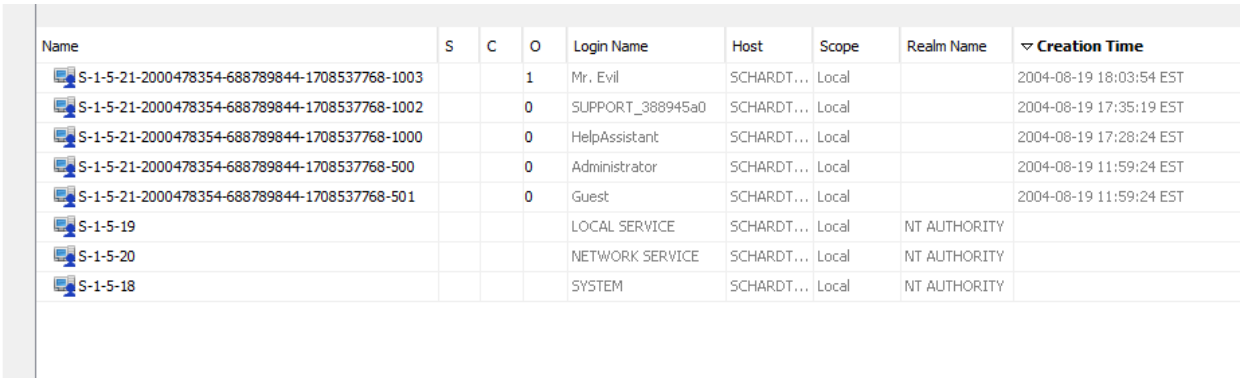


Figure 22. Shutdown date/time converted from hex

OS Accounts

According to figure 23, five OS user accounts were found which are Administrator, Mr. Evil, Guest, HelpAssistant, Support_388945a0. These user accounts were used to logon the Windows XP Professional system. The user account information was retrieved from the OS Accounts in the left tree structure in Autopsy.



Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-2000478354-688789844-1708537768-1003			1	Mr. Evil	SCHARDT...	Local		2004-08-19 18:03:54 EST
S-1-5-21-2000478354-688789844-1708537768-1002			0	SUPPORT_388945a0	SCHARDT...	Local		2004-08-19 17:35:19 EST
S-1-5-21-2000478354-688789844-1708537768-1000			0	HelpAssistant	SCHARDT...	Local		2004-08-19 17:28:24 EST
S-1-5-21-2000478354-688789844-1708537768-500			0	Administrator	SCHARDT...	Local		2004-08-19 11:59:24 EST
S-1-5-21-2000478354-688789844-1708537768-501			0	Guest	SCHARDT...	Local		2004-08-19 11:59:24 EST
S-1-5-19				LOCAL SERVICE	SCHARDT...	Local	NT AUTHORITY	
S-1-5-20				NETWORK SERVICE	SCHARDT...	Local	NT AUTHORITY	
S-1-5-18				SYSTEM	SCHARDT...	Local	NT AUTHORITY	

Figure 23. OS accounts

The user who mostly uses the computer can be found from figure 23 by counting the occurrences of the account and “Mr. Evil” account has the most occurrences in the list.

Last User to Logon

It is very important to know who was the last person to logon because the last person can be the hacker who intercepted the network traffic. The information about the last user who logged on the system was retrieved from the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon,** which is stored in the file path: **C:\Windows\system32\config\Software\Microsoft\Windows NT\CurrentVersion\Winlogon**

The last user to log on the system was “Mr. Evil” who can be the suspected hacker according to figure 24.

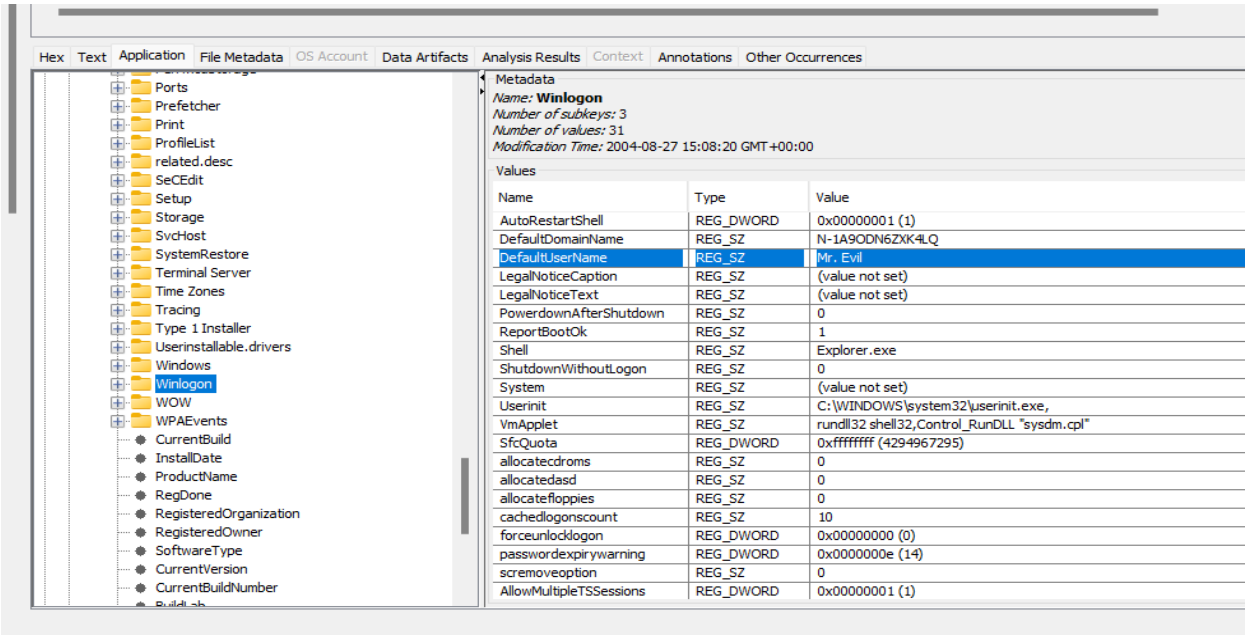


Figure 24. Last user to logon

Keyword Search for 'Greg Schardt'

As Greg Schardt is the registered owner of the laptop, he is suspected to be the hacker who intercepts network traffic. So, a keyword search was run to find the results of appearance in files. The search resulted in 11 files which contained the name "Greg Schardt". After looking at all the files, one file was found "irunin.ini" which revealed that Greg Schardt is Mr. Evil because the file contains Greg Schardt as the registered owner and Mr. Evil is the LAN User. This proves that Mr. Evil and Greg Schardt are the same person. Figure 25 shows the file irunin.ini which contains the suspect information. The file path of irunin.ini is: **C:\Program Files\Look@LAN\irunin.ini**

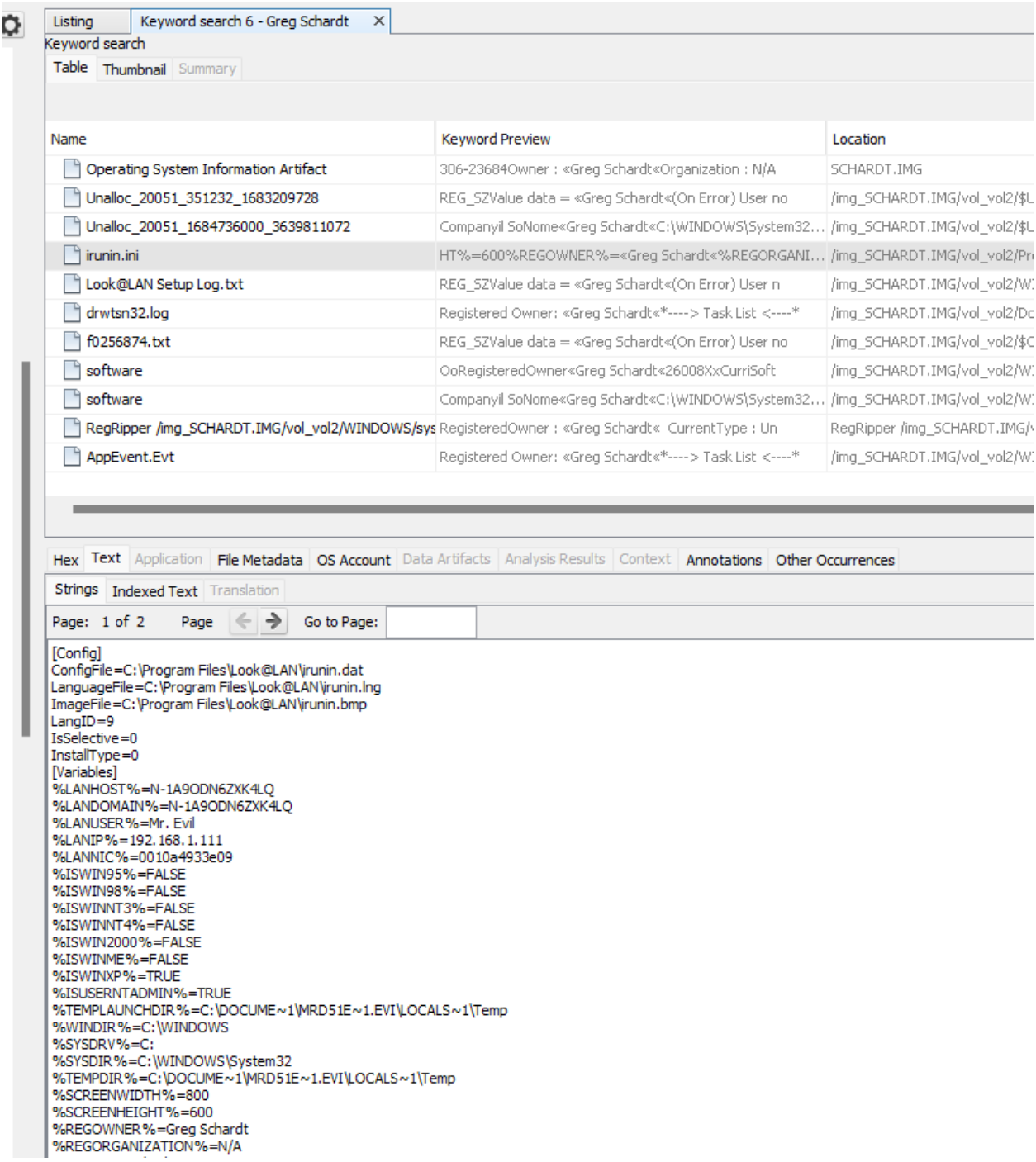


Figure 25. Keyword Search

Network Cards

The hacker used network cards to intercept the network traffic. The information about the network cards was retrieved from the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkCards,** which is stored in the file path: **C:\Windows\system32\config\Software\Microsoft\WindowsNT\CurrentVersion\NetworkCards**

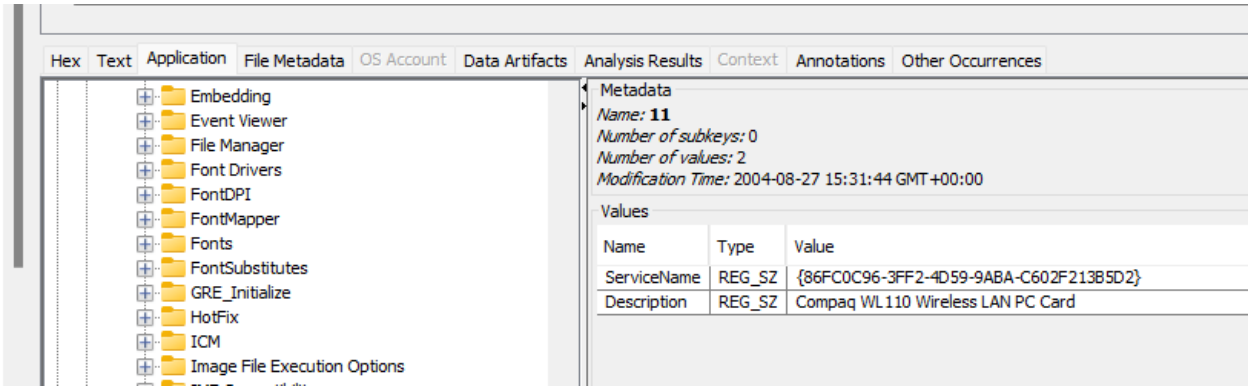


Figure 26. Network card 1

From figure 26, the Network card 1 is Compaq WL110 Wireless LAN PC Card.

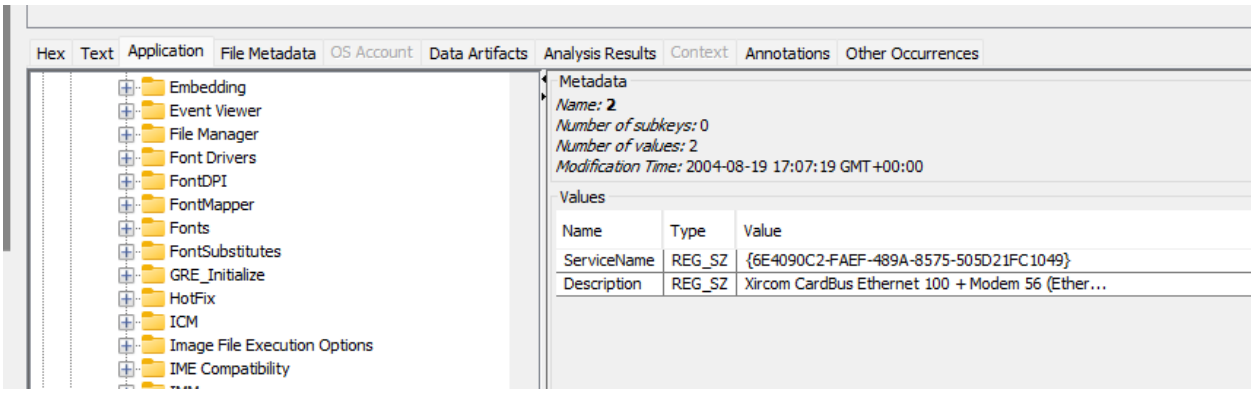


Figure 27. Network card 2

According to figure 27, the Network card 2 is Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface).

IP address and MAC address of computer

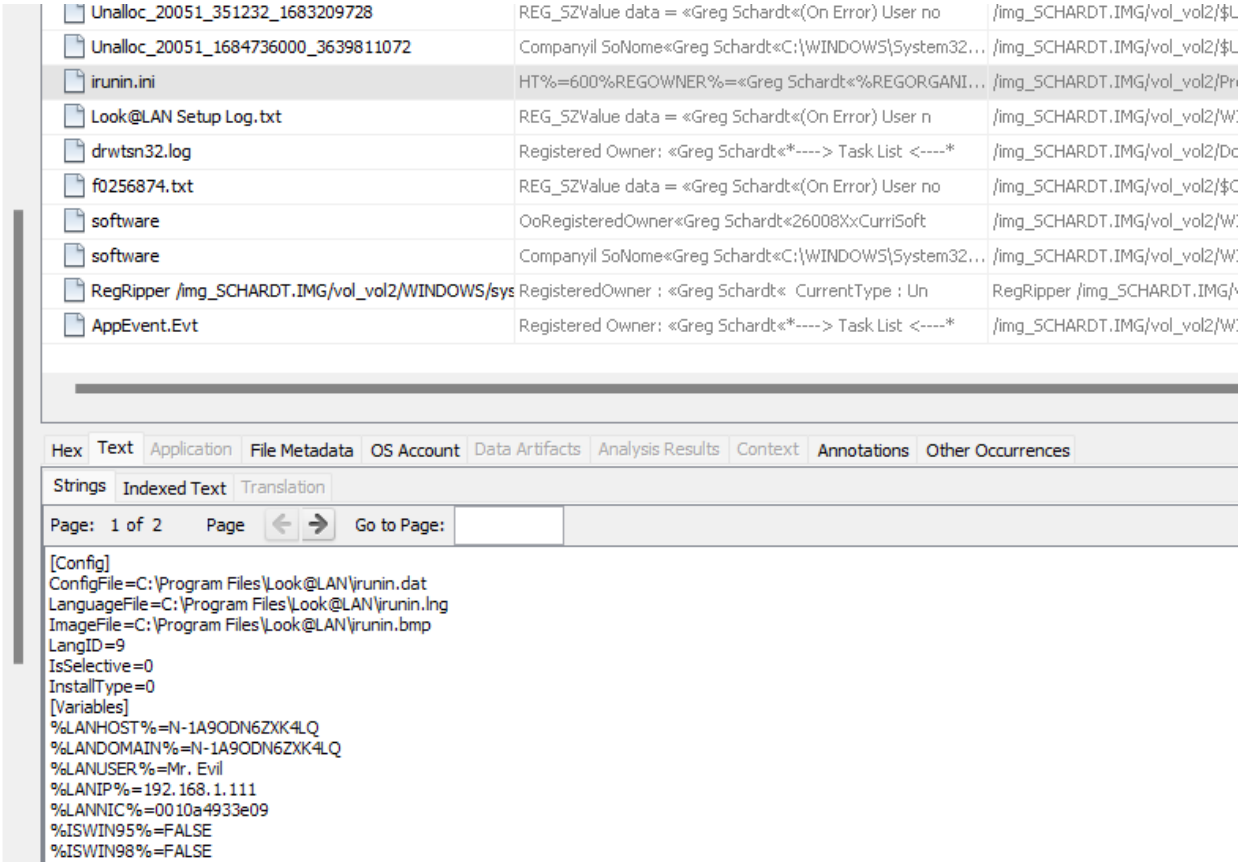


Figure 28. IP address and MAC address

According to figure 28, the IP address of the computer is “192.168.1.111” and the MAC address of the computer is “00:10:A4:93:3E:09”. This information is useful to the examiner as he/she can find the hacker in the network if the IP address was not changed using proxy. The information about the IP address and MAC address was retrieved from the file ‘irunin.ini’ which is located at the path: **C:\Program Files\Look@LAN\irunin.ini Network card Vendor**

The MAC address of the network card obtained from irunin,ini file in figure 28 was searched for vendor information using MAC address lookup tool [6]. The search result returned the Network card information like Company name - Xircom. So, the network card which was used while setting up Look@LAN is “Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)”.

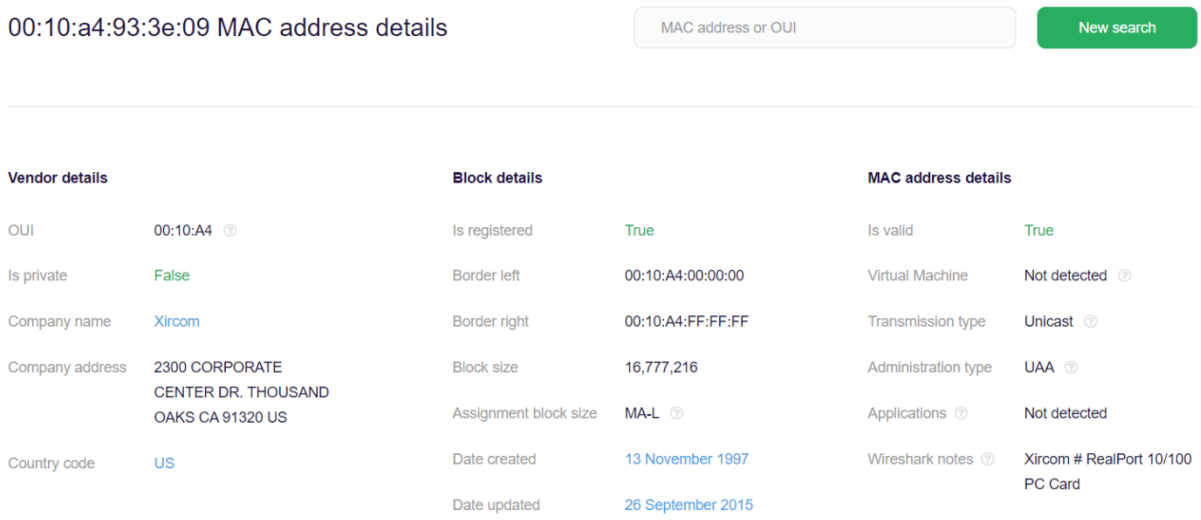
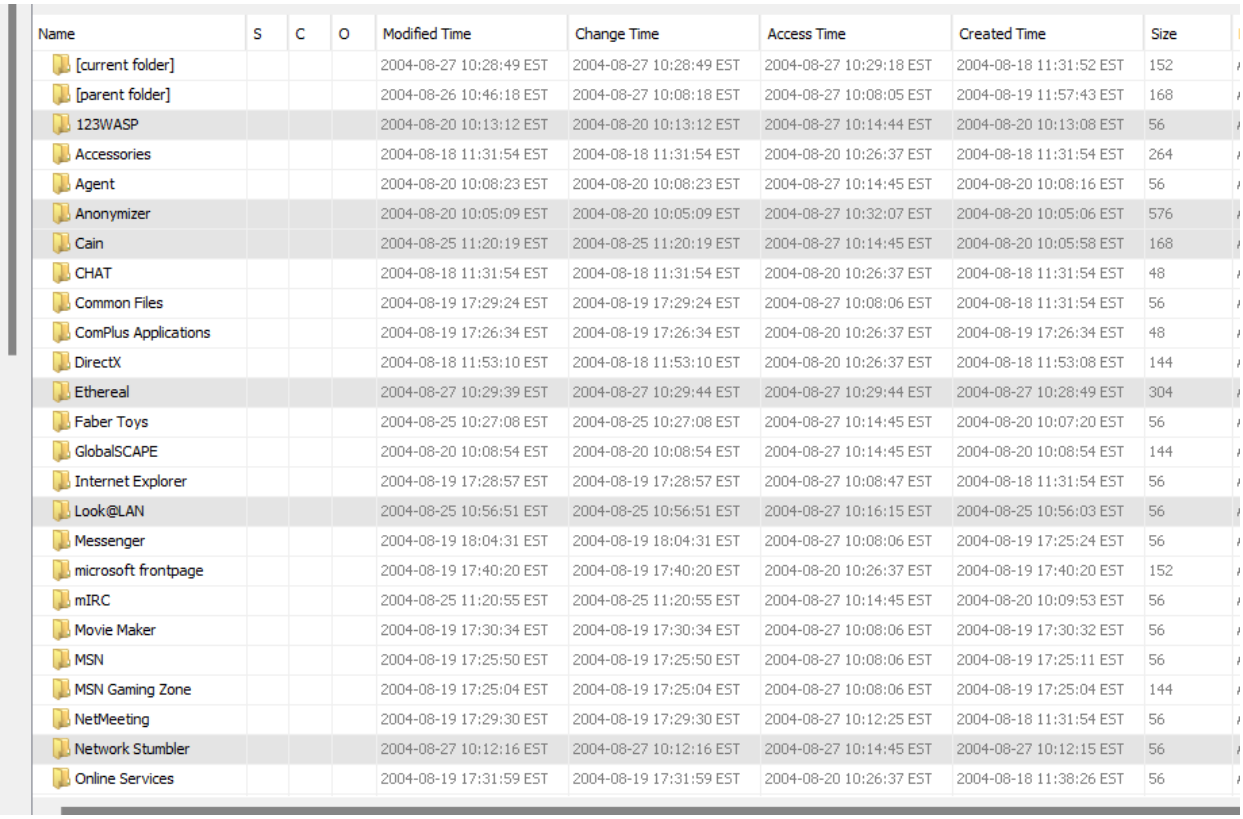


Figure 29. Network card vendor based on MAC address

Hacking Softwares installed



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2004-08-27 10:28:49 EST	2004-08-27 10:28:49 EST	2004-08-27 10:29:18 EST	2004-08-18 11:31:52 EST	152
[parent folder]				2004-08-26 10:46:18 EST	2004-08-27 10:08:18 EST	2004-08-27 10:08:05 EST	2004-08-19 11:57:43 EST	168
123WASP				2004-08-20 10:13:12 EST	2004-08-20 10:13:12 EST	2004-08-27 10:14:44 EST	2004-08-20 10:13:08 EST	56
Accessories				2004-08-18 11:31:54 EST	2004-08-18 11:31:54 EST	2004-08-20 10:26:37 EST	2004-08-18 11:31:54 EST	264
Agent				2004-08-20 10:08:23 EST	2004-08-20 10:08:23 EST	2004-08-27 10:14:45 EST	2004-08-20 10:08:16 EST	56
Anonymizer				2004-08-20 10:05:09 EST	2004-08-20 10:05:09 EST	2004-08-27 10:32:07 EST	2004-08-20 10:05:06 EST	576
Cain				2004-08-25 11:20:19 EST	2004-08-25 11:20:19 EST	2004-08-27 10:14:45 EST	2004-08-20 10:05:58 EST	168
CHAT				2004-08-18 11:31:54 EST	2004-08-18 11:31:54 EST	2004-08-20 10:26:37 EST	2004-08-18 11:31:54 EST	48
Common Files				2004-08-19 17:29:24 EST	2004-08-19 17:29:24 EST	2004-08-27 10:08:06 EST	2004-08-18 11:31:54 EST	56
ComPlus Applications				2004-08-19 17:26:34 EST	2004-08-19 17:26:34 EST	2004-08-20 10:26:37 EST	2004-08-19 17:26:34 EST	48
DirectX				2004-08-18 11:53:10 EST	2004-08-18 11:53:10 EST	2004-08-20 10:26:37 EST	2004-08-18 11:53:08 EST	144
Ethereal				2004-08-27 10:29:39 EST	2004-08-27 10:29:44 EST	2004-08-27 10:29:44 EST	2004-08-27 10:28:49 EST	304
Faber Toys				2004-08-25 10:27:08 EST	2004-08-25 10:27:08 EST	2004-08-27 10:14:45 EST	2004-08-20 10:07:20 EST	56
GlobalSCAPE				2004-08-20 10:08:54 EST	2004-08-20 10:08:54 EST	2004-08-27 10:14:45 EST	2004-08-20 10:08:54 EST	144
Internet Explorer				2004-08-19 17:28:57 EST	2004-08-19 17:28:57 EST	2004-08-27 10:08:47 EST	2004-08-18 11:31:54 EST	56
Look@LAN				2004-08-25 10:56:51 EST	2004-08-25 10:56:51 EST	2004-08-27 10:16:15 EST	2004-08-25 10:56:03 EST	56
Messenger				2004-08-19 18:04:31 EST	2004-08-19 18:04:31 EST	2004-08-27 10:08:06 EST	2004-08-19 17:25:24 EST	56
microsoft frontpage				2004-08-19 17:40:20 EST	2004-08-19 17:40:20 EST	2004-08-20 10:26:37 EST	2004-08-19 17:40:20 EST	152
mIRC				2004-08-25 11:20:55 EST	2004-08-25 11:20:55 EST	2004-08-27 10:14:45 EST	2004-08-20 10:09:53 EST	56
Movie Maker				2004-08-19 17:30:34 EST	2004-08-19 17:30:34 EST	2004-08-27 10:08:06 EST	2004-08-19 17:30:32 EST	56
MSN				2004-08-19 17:25:50 EST	2004-08-19 17:25:50 EST	2004-08-27 10:08:06 EST	2004-08-19 17:25:11 EST	56
MSN Gaming Zone				2004-08-19 17:25:04 EST	2004-08-19 17:25:04 EST	2004-08-27 10:08:06 EST	2004-08-19 17:25:04 EST	144
NetMeeting				2004-08-19 17:29:30 EST	2004-08-19 17:29:30 EST	2004-08-27 10:12:25 EST	2004-08-18 11:31:54 EST	56
Network Stumbler				2004-08-27 10:12:16 EST	2004-08-27 10:12:16 EST	2004-08-27 10:14:45 EST	2004-08-27 10:12:15 EST	56
Online Services				2004-08-19 17:31:59 EST	2004-08-19 17:31:59 EST	2004-08-20 10:26:37 EST	2004-08-18 11:38:26 EST	56

Figure 30. Hacking Softwares

After conducting a search of the computer's installed programs, six programs have been identified as potential hacking tools. According to figure 30, The programs are:

Program Name	**Usage**
Cain & Abel v2.5 beta45 [7]	Password cracking tool
Ethereal 0.10.6 v.0.10.6 [8]	Tool for sniffing packets
Network Stumbler 0.4.0 (remove only) [9]	Wireless LAN detection and attack
Look@LAN 2.50 Build 29 [10]	Advanced network monitoring tool
123 Write All Stored Passwords [11]	Displays all passwords of the currently logged on user that are stored in the Microsoft PWL file
Anonymizer Bar 2.0 (remove only) [12]	Attempts to make user's internet activity untraceable (creating proxy)

Table 2. Hacking Tools

SMTP email address

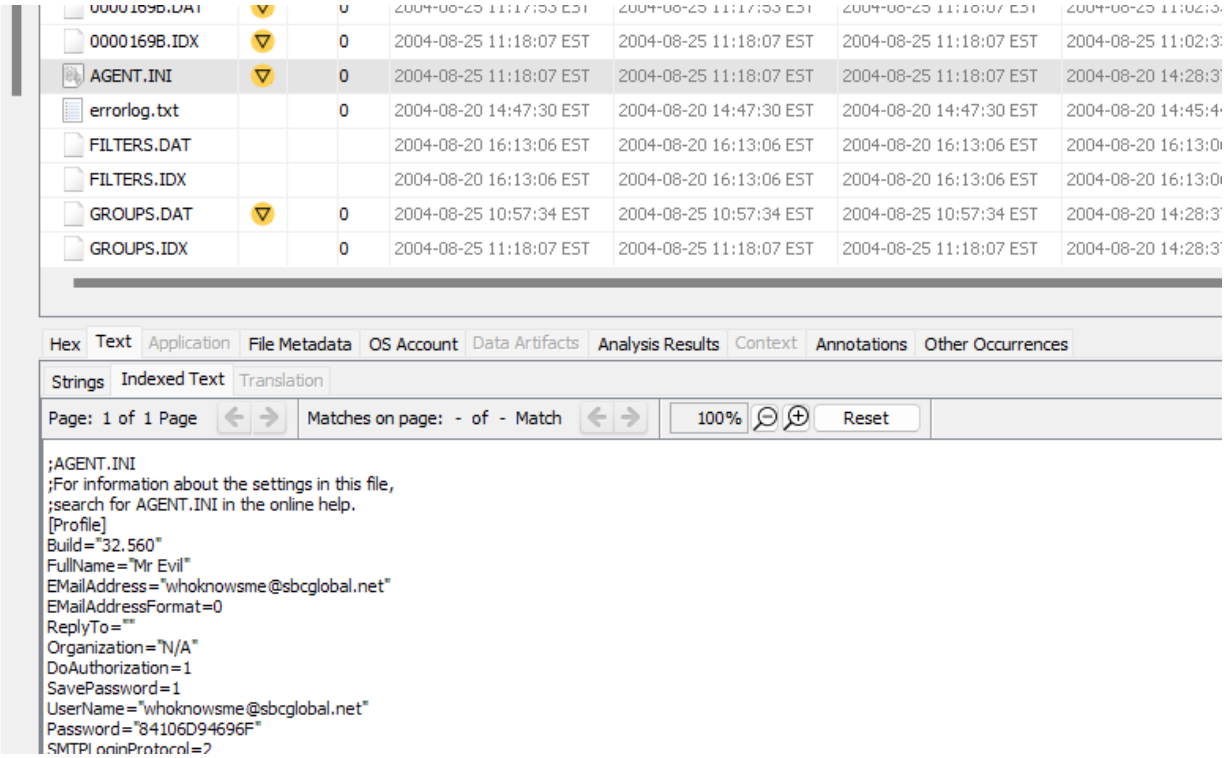


Figure 31. SMTP email address of Mr. Evil

It was necessary to identify the **SMTP** email address of a person of interest known as **"Mr. Evil"**. After a meticulous analysis of the available evidence, it has been determined that the email address associated with **"Mr. Evil"** is **whoknowsme@sbcglobal.net**. This information was obtained through a keyword search of **SMTP**, which led to the identification of the file **NTUSER.DAT**. By clicking on this file and navigating to the Text Tab in the lower pane, the **SMTP** email address was discovered and subsequently verified through multiple sources to ensure the accuracy and validity of the finding. The identification of the **SMTP** email address associated with **"Mr. Evil"** is a significant discovery, as it provides valuable insights into the communication

patterns and potential activities of the individual. The information has been thoroughly analyzed and verified, and the conclusion is deemed credible and reliable**.**

NNTP(news server)

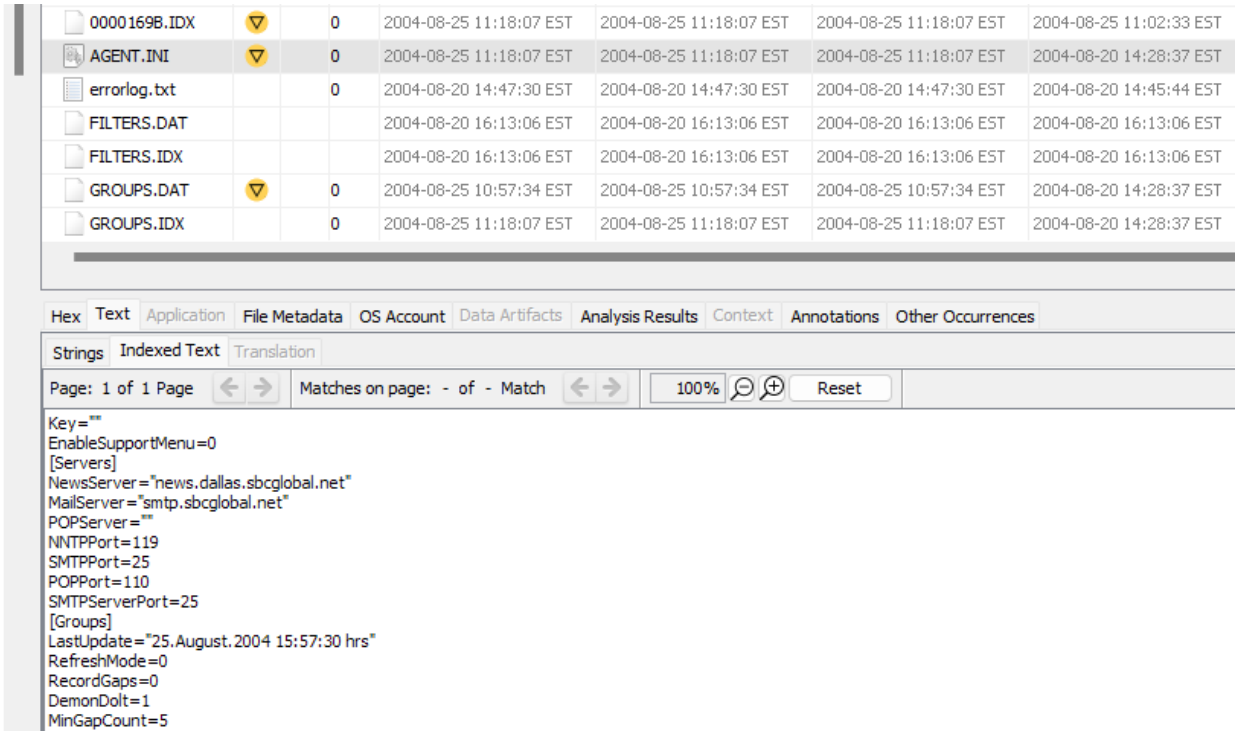


Figure 32. NNTP server settings

The investigation team was able to successfully retrieve **NNTP** settings for the person of interest through a systematic keyword search of **NNTP**. The team located the required information in the file **NTUSER.DAT**, by clicking on the file and selecting the Text Tab in the lower pane. It was determined that the **NNTP (news server)** settings for **Mr. Evil** are: server name is **news.dallas.sbcglobal.net** and the username associated with it is **whoknowsme@sbcglobal.net.** The identification of these **NNTP** settings will allow the team to conduct further analysis of the suspect's communication activities and obtain a deeper understanding of their motives and

intentions. The accuracy and validity of the finding have been verified through cross-referencing with other available evidence

Programs revealing SMTP and NNTP address

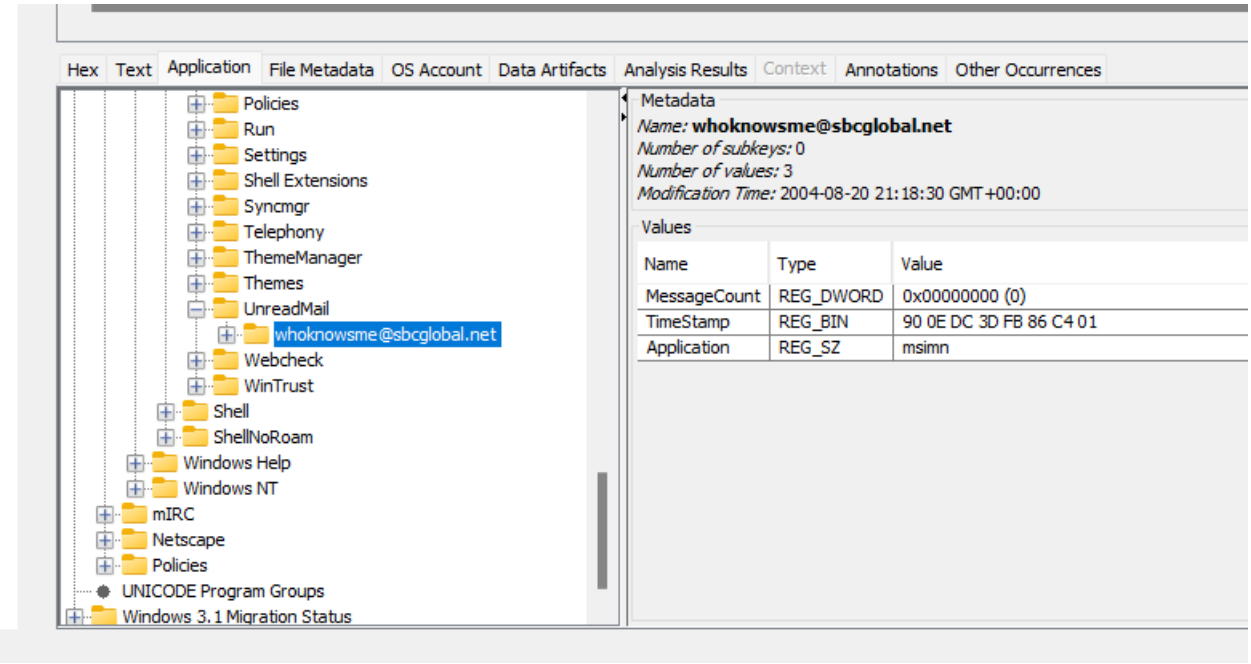


Figure 33. User mail in Outlook Express

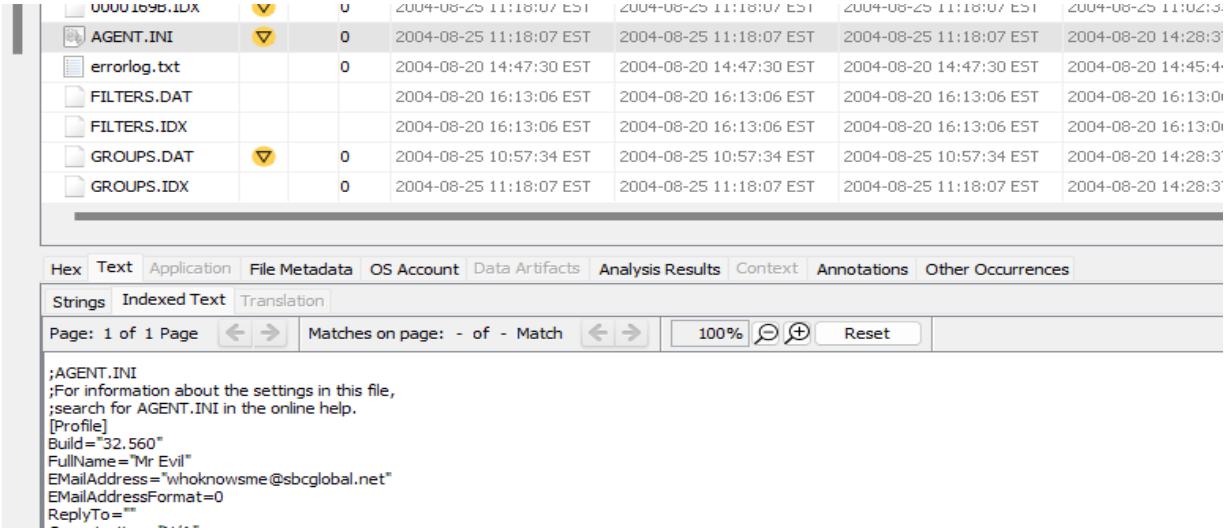
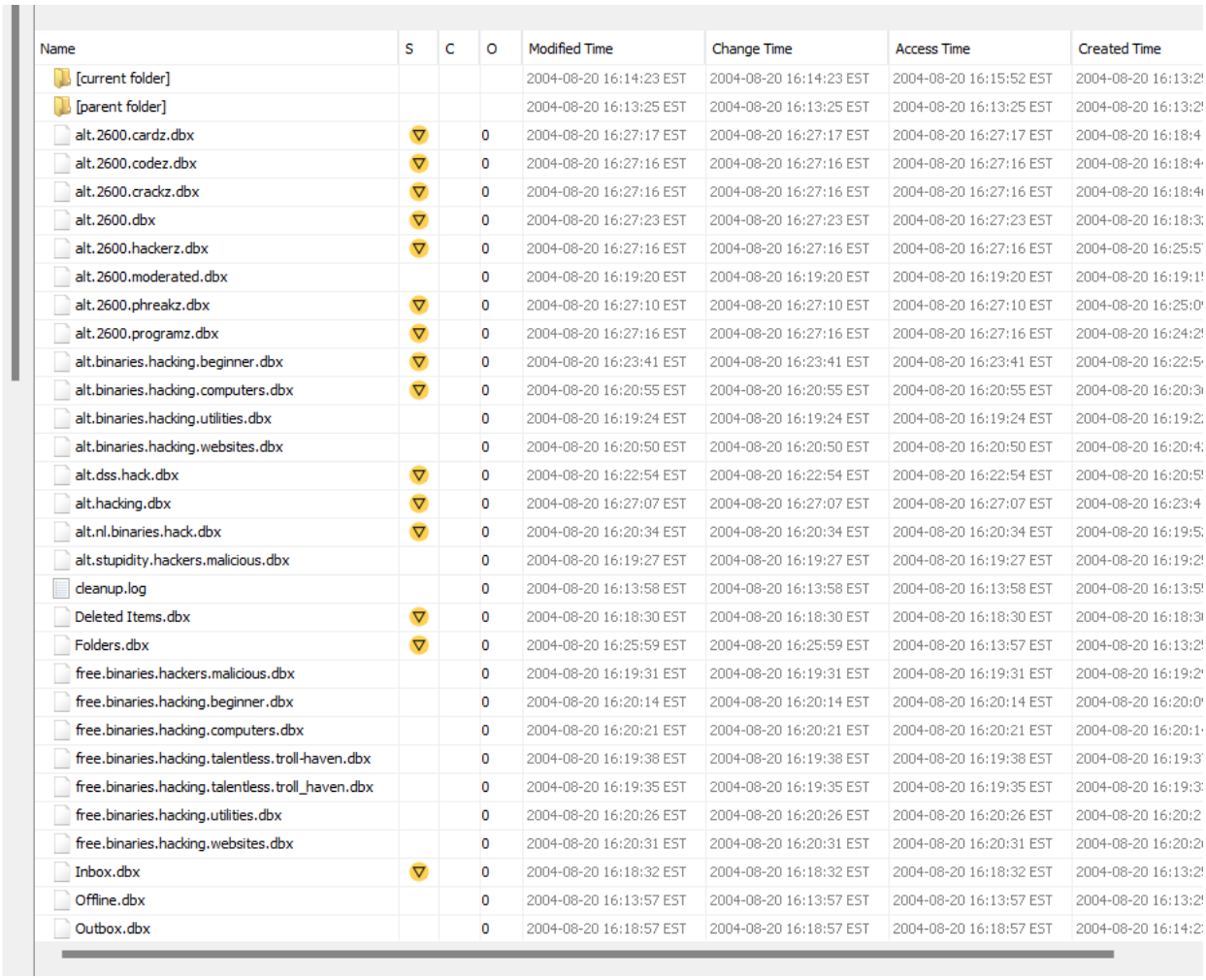


Figure 34. User mail in Forte Agent

According to **Figure 32, 33, 34**, we found two different email services on the computer system, namely **Outlook Express** and **AGENT.ini**. Outlook Express is an email client software that enables users to send, receive, and manage emails. On the other hand, AGENT.ini is a configuration file used by the email client software Forte Agent [13]. These findings suggest that the person of interest may have used both email services for communication purposes, which may be relevant to the investigation. Further analysis of the email data can provide valuable insights into the activities and intentions of the person of interest.

Newsgroups Subscribed

It was discovered that he had subscribed to several newsgroups. These newsgroups were located in the path **C:\Document and Settings\Mr. Evil\Local Settings\Application Data\Identities{EF086998-1115-4ECD-9B13-9ADC067B4929}\Microsoft\Outlook Express**. Five of the newsgroups that **Mr. Evil** had subscribed to were identified as **“alt.anonymous.messages”, “alt.cracks”, “comp.security.firewalls”, “alt.hackers”, and “alt.2600”** . These newsgroups are known to be frequented by individuals interested in hacking and other illicit activities. The information regarding **Mr. Evil's** newsgroup subscriptions can provide valuable insights into his online activities and may help in furthering the investigation.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2004-08-20 16:14:23 EST	2004-08-20 16:14:23 EST	2004-08-20 16:15:52 EST	2004-08-20 16:13:2
[parent folder]				2004-08-20 16:13:25 EST	2004-08-20 16:13:25 EST	2004-08-20 16:13:25 EST	2004-08-20 16:13:2
alt.2600.cardz.dbx	▽		0	2004-08-20 16:27:17 EST	2004-08-20 16:27:17 EST	2004-08-20 16:27:17 EST	2004-08-20 16:18:4
alt.2600.codez.dbx	▽		0	2004-08-20 16:27:16 EST	2004-08-20 16:27:16 EST	2004-08-20 16:27:16 EST	2004-08-20 16:18:4
alt.2600.crackz.dbx	▽		0	2004-08-20 16:27:16 EST	2004-08-20 16:27:16 EST	2004-08-20 16:27:16 EST	2004-08-20 16:18:4
alt.2600.dbx	▽		0	2004-08-20 16:27:23 EST	2004-08-20 16:27:23 EST	2004-08-20 16:27:23 EST	2004-08-20 16:18:3
alt.2600.hackerz.dbx	▽		0	2004-08-20 16:27:16 EST	2004-08-20 16:27:16 EST	2004-08-20 16:27:16 EST	2004-08-20 16:25:5
alt.2600.moderated.dbx			0	2004-08-20 16:19:20 EST	2004-08-20 16:19:20 EST	2004-08-20 16:19:20 EST	2004-08-20 16:19:1
alt.2600.phreakz.dbx	▽		0	2004-08-20 16:27:10 EST	2004-08-20 16:27:10 EST	2004-08-20 16:27:10 EST	2004-08-20 16:25:0
alt.2600.programz.dbx	▽		0	2004-08-20 16:27:16 EST	2004-08-20 16:27:16 EST	2004-08-20 16:27:16 EST	2004-08-20 16:24:2
alt.binaries.hacking.beginner.dbx	▽		0	2004-08-20 16:23:41 EST	2004-08-20 16:23:41 EST	2004-08-20 16:23:41 EST	2004-08-20 16:22:5
alt.binaries.hacking.computers.dbx	▽		0	2004-08-20 16:20:55 EST	2004-08-20 16:20:55 EST	2004-08-20 16:20:55 EST	2004-08-20 16:20:3
alt.binaries.hacking.utilities.dbx			0	2004-08-20 16:19:24 EST	2004-08-20 16:19:24 EST	2004-08-20 16:19:24 EST	2004-08-20 16:19:2
alt.binaries.hacking.websites.dbx			0	2004-08-20 16:20:50 EST	2004-08-20 16:20:50 EST	2004-08-20 16:20:50 EST	2004-08-20 16:20:4
alt.dss.hack.dbx	▽		0	2004-08-20 16:22:54 EST	2004-08-20 16:22:54 EST	2004-08-20 16:22:54 EST	2004-08-20 16:20:5
alt.hacking.dbx	▽		0	2004-08-20 16:27:07 EST	2004-08-20 16:27:07 EST	2004-08-20 16:27:07 EST	2004-08-20 16:23:4
alt.nl.binaries.hack.dbx	▽		0	2004-08-20 16:20:34 EST	2004-08-20 16:20:34 EST	2004-08-20 16:20:34 EST	2004-08-20 16:19:5
alt.stupidity.hackers.malicious.dbx			0	2004-08-20 16:19:27 EST	2004-08-20 16:19:27 EST	2004-08-20 16:19:27 EST	2004-08-20 16:19:2
cleanup.log			0	2004-08-20 16:13:58 EST	2004-08-20 16:13:58 EST	2004-08-20 16:13:58 EST	2004-08-20 16:13:5
Deleted Items.dbx	▽		0	2004-08-20 16:18:30 EST	2004-08-20 16:18:30 EST	2004-08-20 16:18:30 EST	2004-08-20 16:18:3
Folders.dbx	▽		0	2004-08-20 16:25:59 EST	2004-08-20 16:25:59 EST	2004-08-20 16:13:57 EST	2004-08-20 16:13:2
free.binaries.hackers.malicious.dbx			0	2004-08-20 16:19:31 EST	2004-08-20 16:19:31 EST	2004-08-20 16:19:31 EST	2004-08-20 16:19:2
free.binaries.hacking.beginner.dbx			0	2004-08-20 16:20:14 EST	2004-08-20 16:20:14 EST	2004-08-20 16:20:14 EST	2004-08-20 16:20:0
free.binaries.hacking.computers.dbx			0	2004-08-20 16:20:21 EST	2004-08-20 16:20:21 EST	2004-08-20 16:20:21 EST	2004-08-20 16:20:1
free.binaries.hacking.talentless.troll-haven.dbx			0	2004-08-20 16:19:38 EST	2004-08-20 16:19:38 EST	2004-08-20 16:19:38 EST	2004-08-20 16:19:3
free.binaries.hacking.talentless.troll_haven.dbx			0	2004-08-20 16:19:35 EST	2004-08-20 16:19:35 EST	2004-08-20 16:19:35 EST	2004-08-20 16:19:3
free.binaries.hacking.utilities.dbx			0	2004-08-20 16:20:26 EST	2004-08-20 16:20:26 EST	2004-08-20 16:20:26 EST	2004-08-20 16:20:2
free.binaries.hacking.websites.dbx			0	2004-08-20 16:20:31 EST	2004-08-20 16:20:31 EST	2004-08-20 16:20:31 EST	2004-08-20 16:20:2
Inbox.dbx	▽		0	2004-08-20 16:18:32 EST	2004-08-20 16:18:32 EST	2004-08-20 16:18:32 EST	2004-08-20 16:13:2
Offline.dbx			0	2004-08-20 16:13:57 EST	2004-08-20 16:13:57 EST	2004-08-20 16:13:57 EST	2004-08-20 16:13:2
Outbox.dbx			0	2004-08-20 16:18:57 EST	2004-08-20 16:18:57 EST	2004-08-20 16:18:57 EST	2004-08-20 16:14:2

Figure 35. Newsgroups subscribed by Mr. Evil

IRC USER Settings

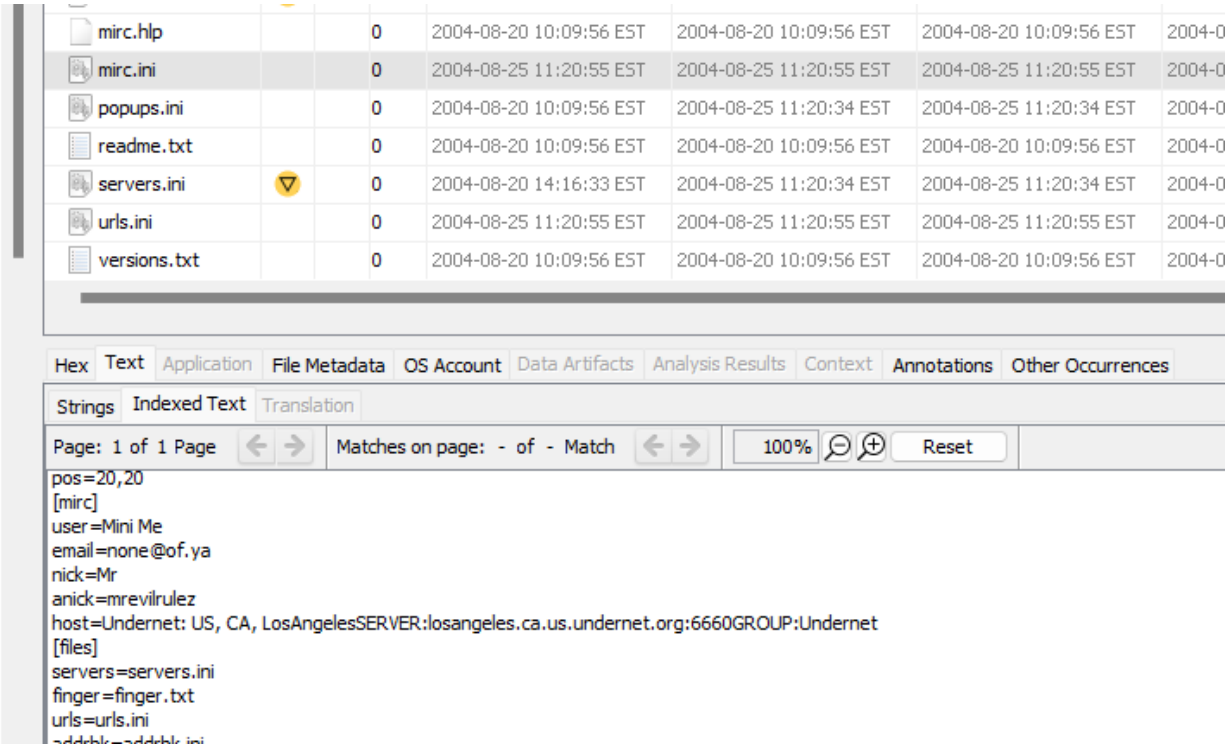
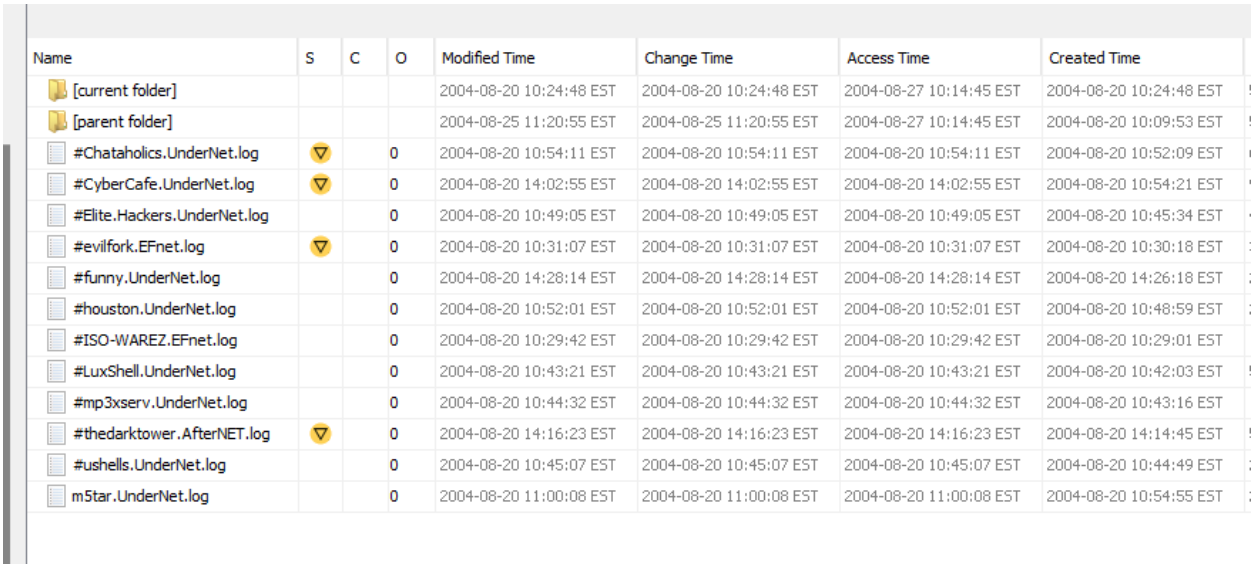


Figure 36. IRC user settings

According to Figure 36, the popular **IRC** program **MIRC** [14] was installed on the system. The user settings for the program were found to be as follows: the user's name was "**Mini Me",** and the email address provided was **"none@of.ya".** The user's nickname was **"Mr"** and the alternative nickname was **"mrevilrulez"** It was also determined that the user was on the Undernet server, specifically the **US and CA, Los Angeles server with the group being Undernet.** This information was retrieved from the **mirc.ini file located in the C:\Program Files\mIRC** directory, and it could be crucial to the investigation in determining the user's activity on the IRC network.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2004-08-20 10:24:48 EST	2004-08-20 10:24:48 EST	2004-08-27 10:14:45 EST	2004-08-20 10:24:48 EST
[parent folder]				2004-08-25 11:20:55 EST	2004-08-25 11:20:55 EST	2004-08-27 10:14:45 EST	2004-08-20 10:09:53 EST
#Chataholics.UnderNet.log			0	2004-08-20 10:54:11 EST	2004-08-20 10:54:11 EST	2004-08-20 10:54:11 EST	2004-08-20 10:52:09 EST
#CyberCafe.UnderNet.log			0	2004-08-20 14:02:55 EST	2004-08-20 14:02:55 EST	2004-08-20 14:02:55 EST	2004-08-20 10:54:21 EST
#Elite.Hackers.UnderNet.log			0	2004-08-20 10:49:05 EST	2004-08-20 10:49:05 EST	2004-08-20 10:49:05 EST	2004-08-20 10:45:34 EST
#evilfork.EFnet.log			0	2004-08-20 10:31:07 EST	2004-08-20 10:31:07 EST	2004-08-20 10:31:07 EST	2004-08-20 10:30:18 EST
#funny.UnderNet.log			0	2004-08-20 14:28:14 EST	2004-08-20 14:28:14 EST	2004-08-20 14:28:14 EST	2004-08-20 14:26:18 EST
#houston.UnderNet.log			0	2004-08-20 10:52:01 EST	2004-08-20 10:52:01 EST	2004-08-20 10:52:01 EST	2004-08-20 10:48:59 EST
#ISO-WAREZ.EFnet.log			0	2004-08-20 10:29:42 EST	2004-08-20 10:29:42 EST	2004-08-20 10:29:42 EST	2004-08-20 10:29:01 EST
#LuxShell.UnderNet.log			0	2004-08-20 10:43:21 EST	2004-08-20 10:43:21 EST	2004-08-20 10:43:21 EST	2004-08-20 10:42:03 EST
#mp3xserv.UnderNet.log			0	2004-08-20 10:44:32 EST	2004-08-20 10:44:32 EST	2004-08-20 10:44:32 EST	2004-08-20 10:43:16 EST
#thedarktower.AfterNET.log			0	2004-08-20 14:16:23 EST	2004-08-20 14:16:23 EST	2004-08-20 14:16:23 EST	2004-08-20 14:14:45 EST
#ushells.UnderNet.log			0	2004-08-20 10:45:07 EST	2004-08-20 10:45:07 EST	2004-08-20 10:45:07 EST	2004-08-20 10:44:49 EST
m5tar.UnderNet.log			0	2004-08-20 11:00:08 EST	2004-08-20 11:00:08 EST	2004-08-20 11:00:08 EST	2004-08-20 10:54:55 EST

Figure 37. IRC log files

The IRC program, MIRC, installed on the user's computer had the capability to log chat sessions. According to Figure 37, upon analyzing the log files located at the path: **C:\Program Files\mIRC\logs**. It was determined that the user accessed several IRC channels. Some of the channels accessed by user are: **ushells.UnderNet.log, mp3xserv.UnderNet.log, and Elite.Hackers.UnderNet.log**

Ethereal's Recent file

According to figure 38, a recent file created by Ethereal was found at the path: **C:\Documents and Settings\Mr. Evil\Application Data\Ethereal\recent.** This file contains information about the location of the file which consists of intercepted data and the name of the file is **"interception".** The path of this file is: **C:\Documents and Settings\Mr. Evil\interception.**

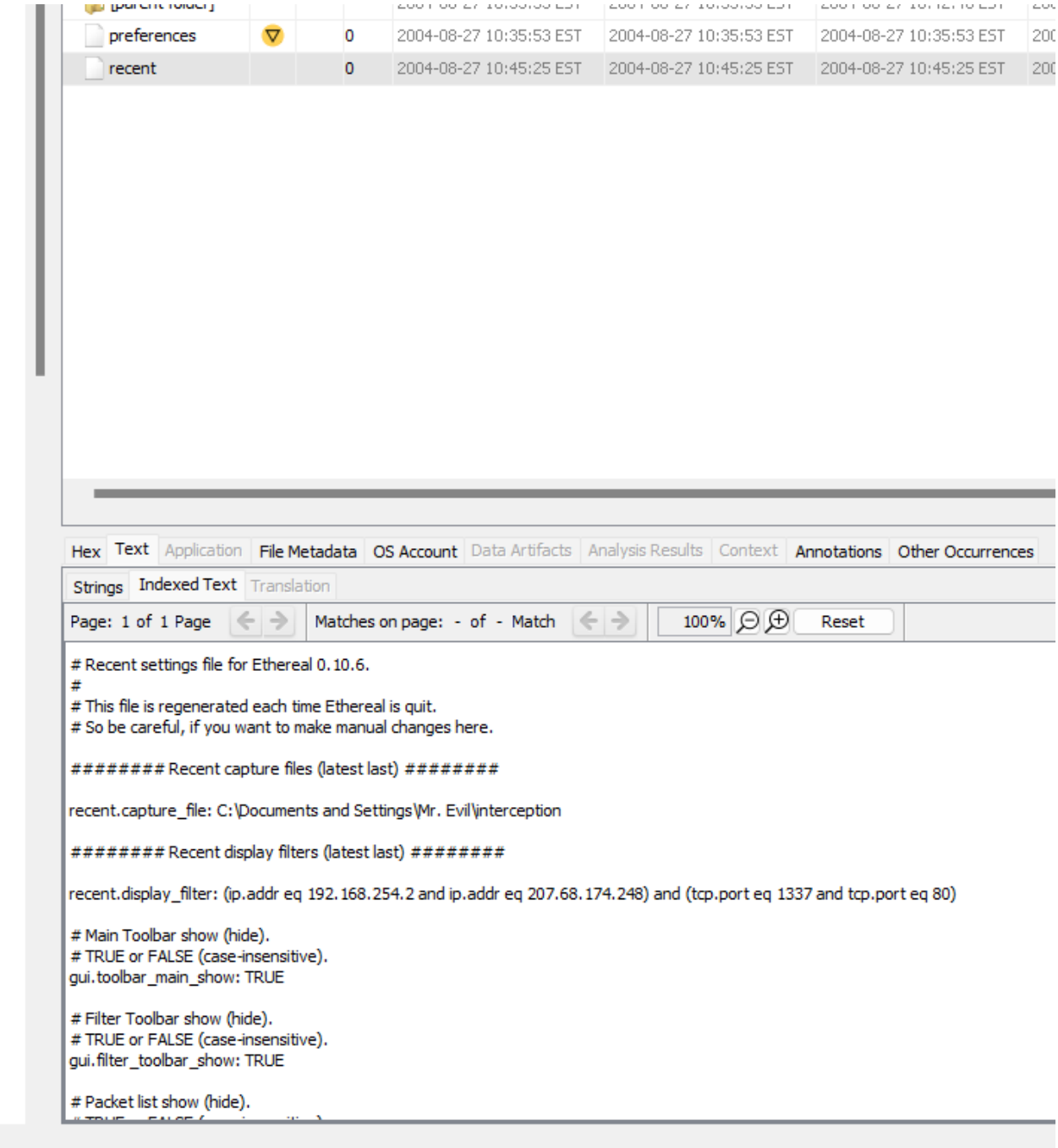


Figure 38. Recent file of Ethereal

The interception file was opened to find out if any important information is present in it. On observing the file and according to figure 39, it was found that the user agent is MSIE

(Microsoft Internet Explorer) 4.01 with Windows CE. It is a wireless pocket sized PC with a display of 240x320 pixels.

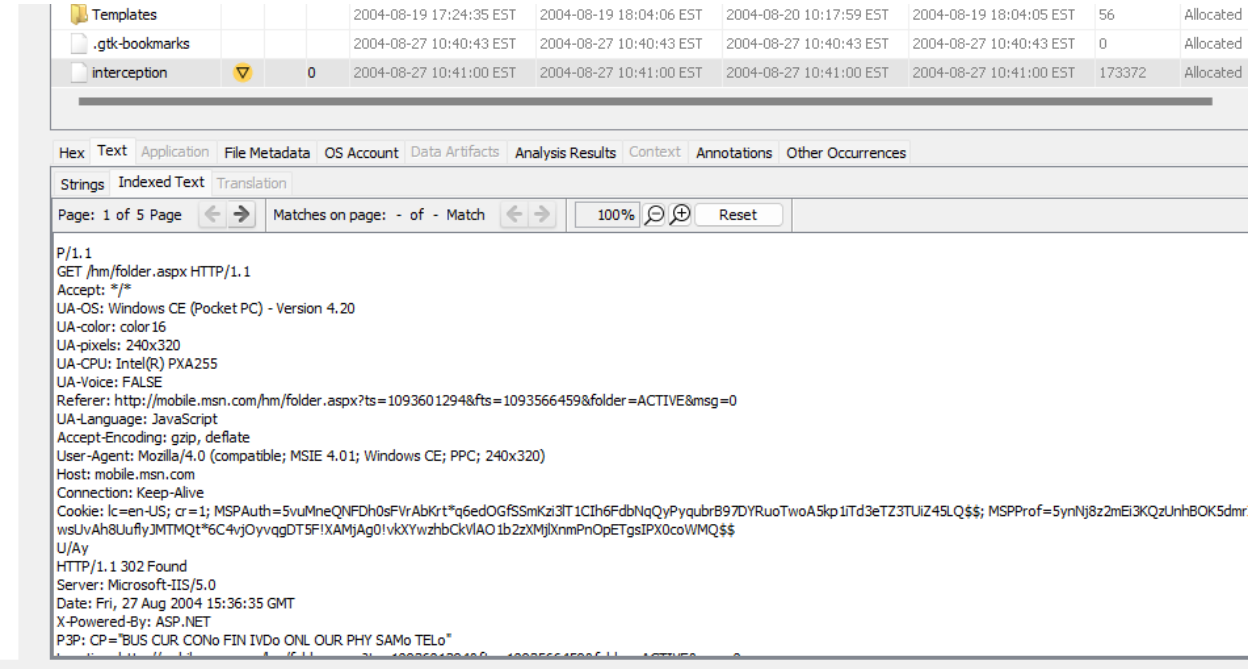


Figure 39. Interception file

The user accessed two websites using the pocket PC which are: **mobile.msn.com** and **MSN Hotmail (email).** This can be observed in figure 40.

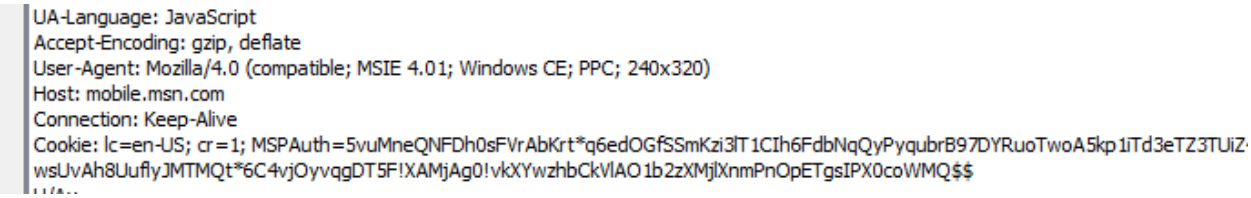


Figure 40. Website accessed

User's web based email address

According to figure 41, the user's web-based email address was identified as **mrevilrulez@yahoo.com**. This was discovered through the examination of the extracted content,

specifically the user's web history. A file was found indicating that the user had logged into FTP service using their email address, which led to the discovery of Yahoo! Mail address.

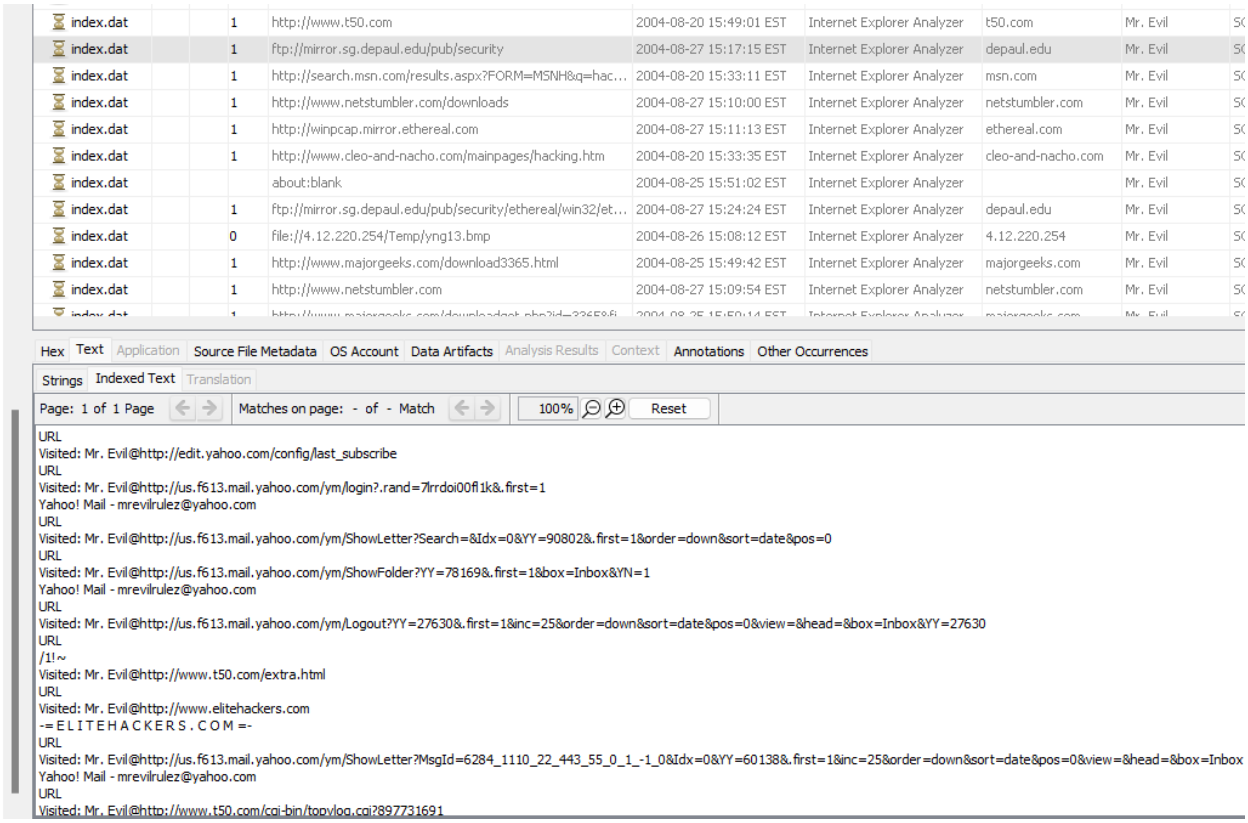


Figure 41. Mr. Evil's web based email address

Saved copies of the email

As we said, Yahoo Mail was being used by the user on the computer. Upon further investigation, it was found that the web-based email copies of email under the file name **"ShowLetter[1].htm".** This information can be useful in locating and reviewing any emails that may be relevant to the investigation.

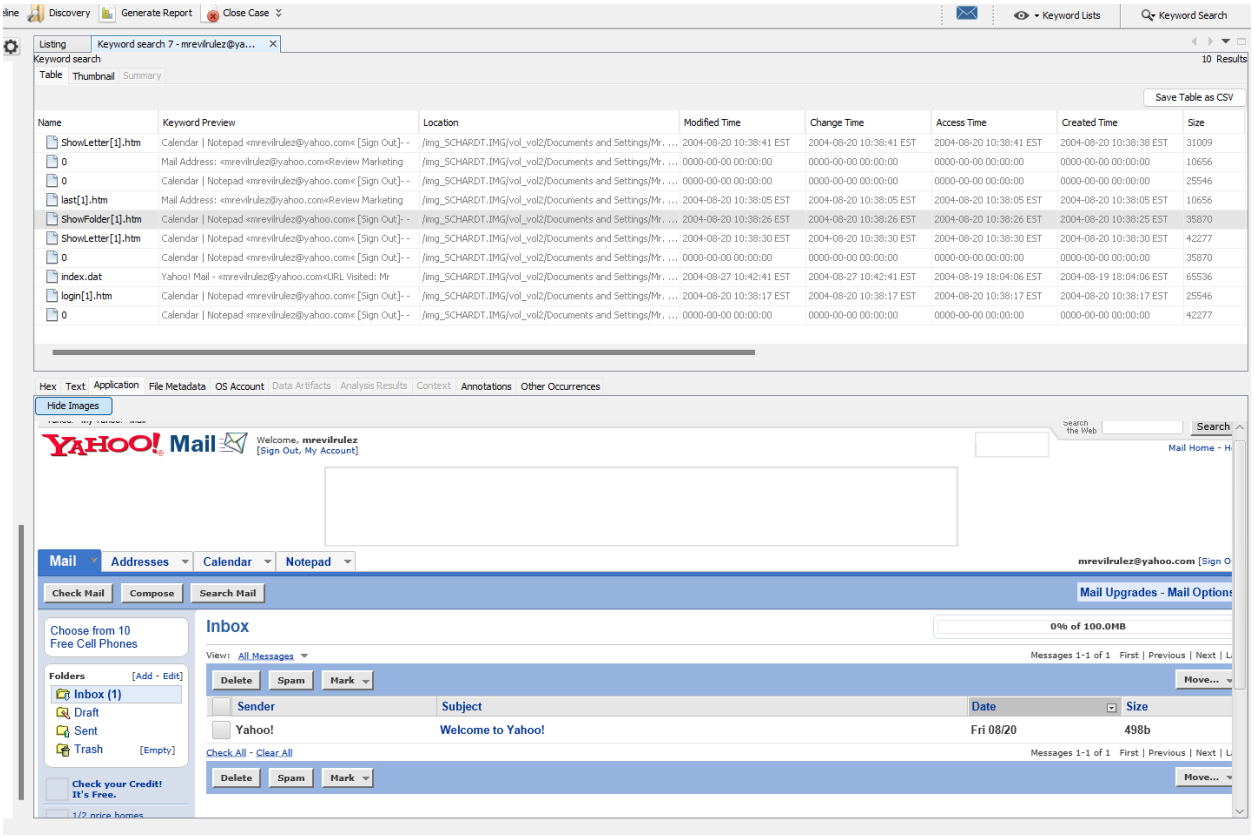
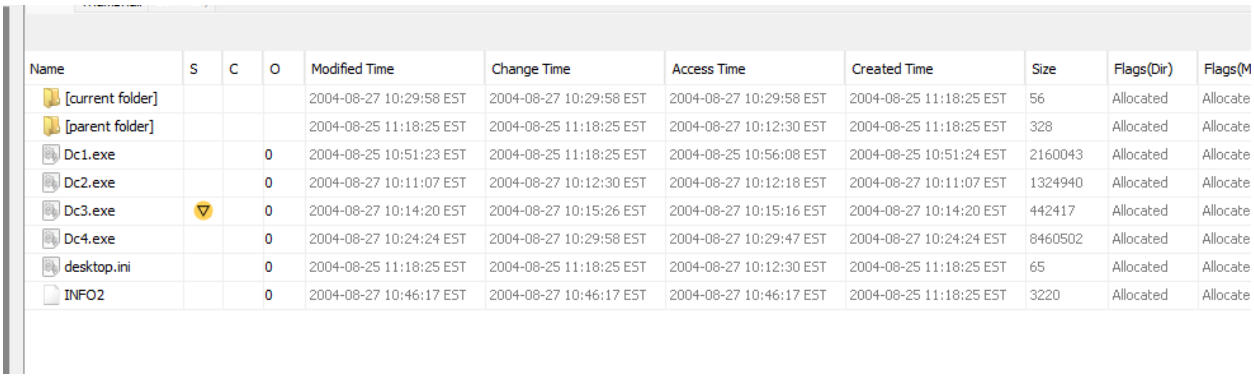


Figure 42. File which stores copies of email

Executable files in Recycle Bin



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(M
[current folder]				2004-08-27 10:29:58 EST	2004-08-27 10:29:58 EST	2004-08-27 10:29:58 EST	2004-08-25 11:18:25 EST	56	Allocated	Allocate
[parent folder]				2004-08-25 11:18:25 EST	2004-08-25 11:18:25 EST	2004-08-27 10:12:30 EST	2004-08-25 11:18:25 EST	328	Allocated	Allocate
Dc1.exe			0	2004-08-25 10:51:23 EST	2004-08-25 11:18:25 EST	2004-08-25 10:56:08 EST	2004-08-25 10:51:24 EST	2160043	Allocated	Allocate
Dc2.exe			0	2004-08-27 10:11:07 EST	2004-08-27 10:12:30 EST	2004-08-27 10:12:18 EST	2004-08-27 10:11:07 EST	1324940	Allocated	Allocate
Dc3.exe			0	2004-08-27 10:14:20 EST	2004-08-27 10:15:26 EST	2004-08-27 10:15:16 EST	2004-08-27 10:14:20 EST	442417	Allocated	Allocate
Dc4.exe			0	2004-08-27 10:24:24 EST	2004-08-27 10:29:58 EST	2004-08-27 10:29:47 EST	2004-08-27 10:24:24 EST	8460502	Allocated	Allocate
desktop.ini			0	2004-08-25 11:18:25 EST	2004-08-25 11:18:25 EST	2004-08-27 10:12:30 EST	2004-08-25 11:18:25 EST	65	Allocated	Allocate
INFO2			0	2004-08-27 10:46:17 EST	2004-08-27 10:46:17 EST	2004-08-27 10:46:17 EST	2004-08-25 11:18:25 EST	3220	Allocated	Allocate

Figure 43. Executable files in recycle bin

According to figure 43, upon checking the folder at path:**C:\RECYCLER\S-1–5–21–2000478354–688789844–1708537768–1003**, it has been found that there are a total of 4

executable files present in it. The names of these executable files are **"Dc1.exe, Dc2.exe, Dc3.exe, Dc4.exe"**.

Deleted files

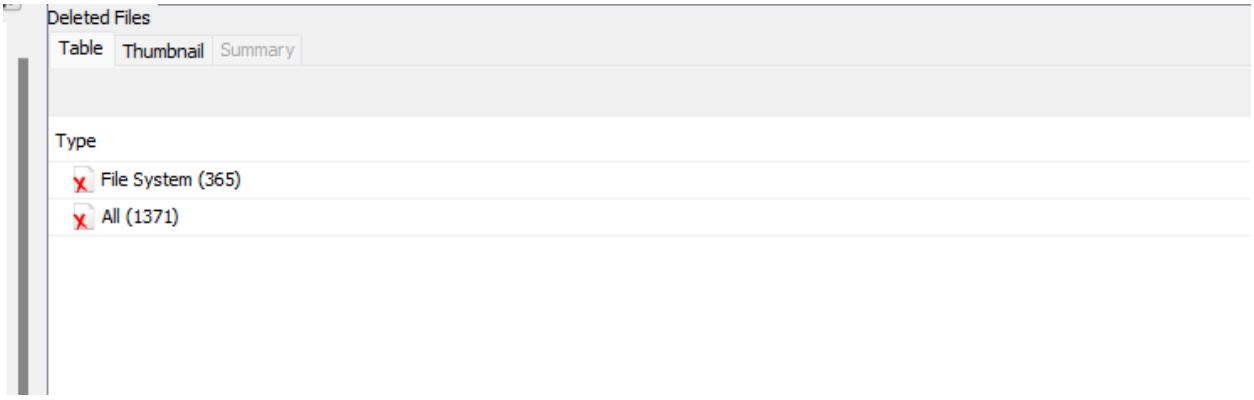


Figure 44. Total number of deleted files

According to Figure 44, there are 1371 total number of files that are actually deleted from the system. Maybe the last user who logged on deleted these files.

Files containing virus

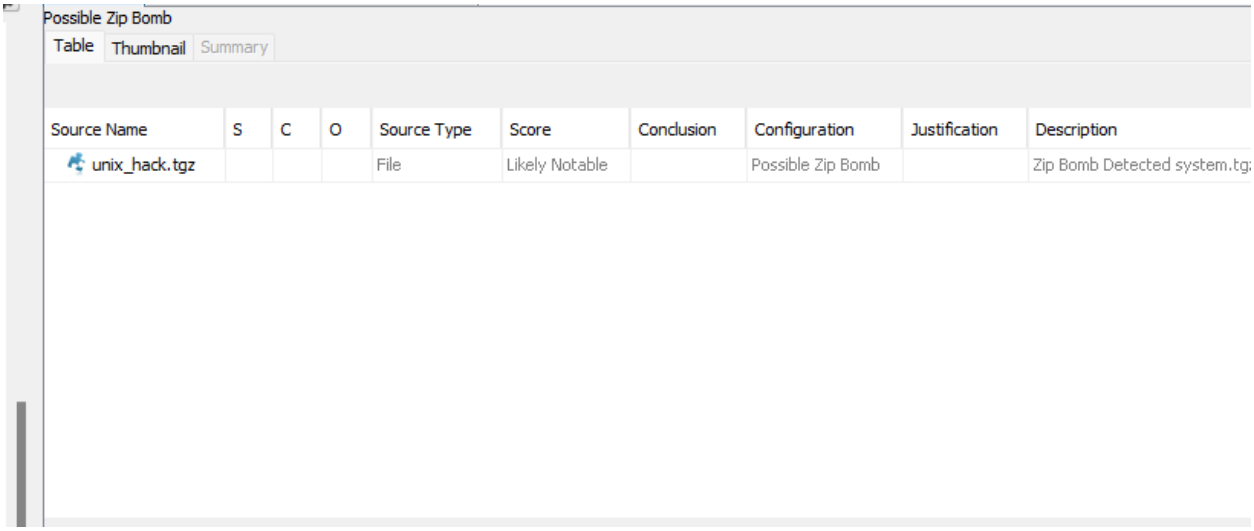


Figure 45. File containing virus

Upon performing an Anti-virus check using Autopsy, it was discovered that there is a zip bomb located at the path: **C:\My Documents\FOOTPRINTING\UNIX\.** Zip bomb "unix_hack.tgz" can be observed in the figure 45.

According to Wikipedia [15], "In computing, a zip bomb, also known as a decompression bomb or zip of death, is a malicious archive file designed to crash or render useless the program or system reading it. It is often employed to disable antivirus software, in order to create an opening for more traditional malware."

Conclusions/Recommendations

Conclusions

We did a thorough and extensive forensic investigation on an abandoned Dell Laptop, wireless PCMCIA card, and handmade 802.11b antenna of a suspected hacking incident case. We were able to find and identify crucial digital data that provided insights into the possible hacking use of the computer by a suspect "Greg Schardt".

On the suspect's laptop we discovered the evidence of several hacking tools and programs, which includes password cracking tools, network sniffers, network scanners, and proxy tools for making any internet activity untraceable. We also discovered a number of websites and online forums that the person visited frequently, which indicated a potential interest in hacking and illicit activity. Although, based upon the evidence and the findings we found so far, we were unable to definitively link the found laptop to the suspect "Greg Schardt". However, regarding the found evidence and insights, it clearly suggested that the suspect also known as "Mr Evil" was involved in the hacking incident.

All in all, our investigation showed that the suspect "Greg Schardt" and "Mr.Evil" are just one single person and all the suspicions about the "Greg Schardt" were true. However, our digital investigation demonstrated that digital forensics methods and processes are essential for investigating any suspected cybercrime incidents and also by analyzing the digital evidence we were able to learn crucial key details about the incidents nature, potential hacker involved and the methods they used.

Our findings highlighted the importance of digital security measures and the need for taking preventive measures to protect their sensitive data.

Recommendations

As for recommendation, to stay ahead of hackers, we recommend law enforcement agencies and the digital security professionals to further invest in latest and highly efficient digital techniques and tools to lessen the harm being caused by the hackers and also recommend to update the software frequently and this way, one can help prevent and reduce the damage caused by the cybercrime incidents.

Exhibits

Based on the investigation:

Exhibit 1: System Details and Web Bookmarks.

This exhibit contains evidence showing that the suspected person “Greg Schardt” is really the one who was disguised as “Mr.Evil”.

	D	E	F
	Program	Domain	Source File
EST	Internet Explorer Analyzer	microsoft.com	/img_SCHARDT.IMG/vol_vol2/Documents and Settings/Mr. Evil/Favorites/Links/Free Hotmail.url
EST	Internet Explorer Analyzer	microsoft.com	/img_SCHARDT.IMG/vol_vol2/Documents and Settings/Mr. Evil/Favorites/Links/Windows.url
EST	Internet Explorer Analyzer	microsoft.com	/img_SCHARDT.IMG/vol_vol2/Documents and Settings/Mr. Evil/Favorites/Links/Windows Media.url
EST	Internet Explorer Analyzer	microsoft.com	/img_SCHARDT.IMG/vol_vol2/Documents and Settings/Mr. Evil/Favorites/Links/Customize Links.url
EST	Internet Explorer Analyzer	microsoft.com	/img_SCHARDT.IMG/vol_vol2/Documents and Settings/Mr. Evil/Favorites/MSN.com.url
EST	Internet Explorer Analyzer	microsoft.com	/img_SCHARDT.IMG/vol_vol2/Documents and Settings/Mr. Evil/Favorites/Radio Station Guide.url

Figure 46. Web Bookmarks

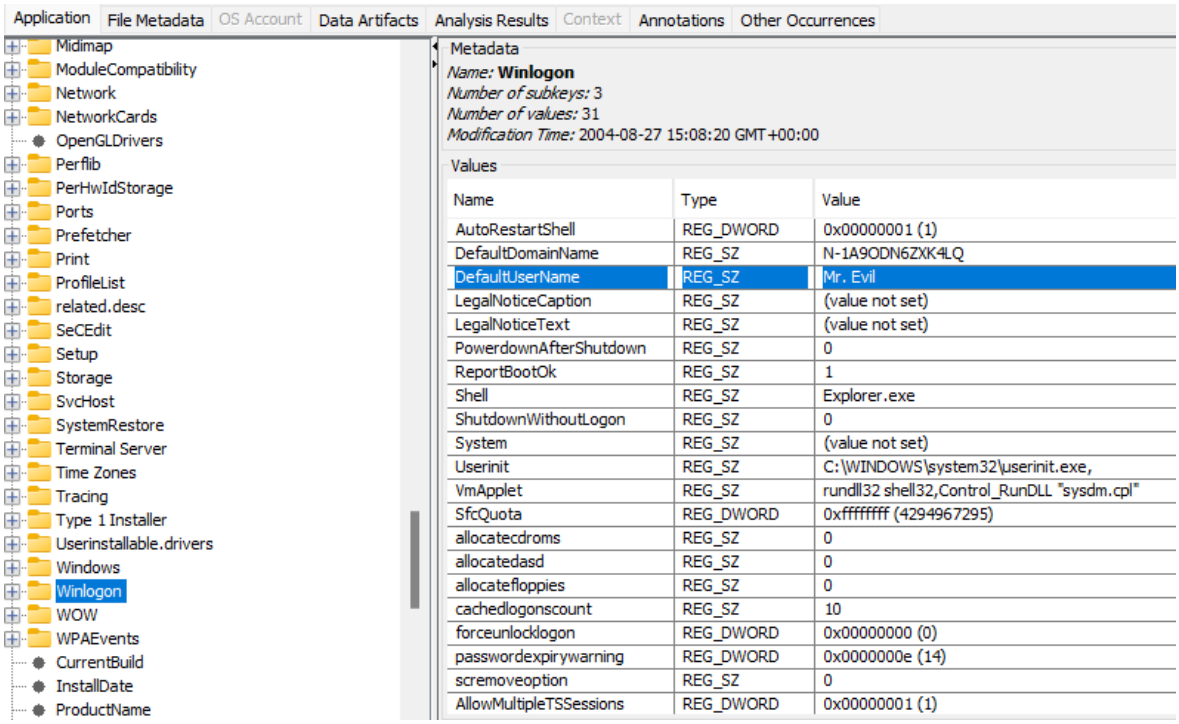


Figure 47. Primary User Account

Exhibit 2: Data Source Summary Report

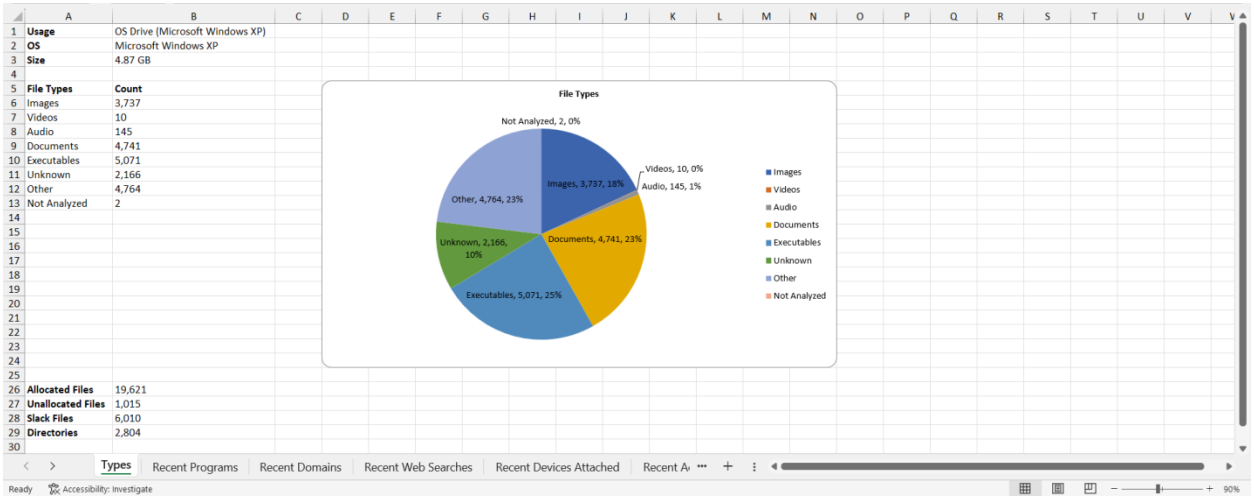


Figure 48. Data source summary report

This exhibit shows that the data source has Windows XP as Operating System, the number of files in the data source according to their file types. It also shows the size of the data source which is 4.87 GB.

Exhibit 3: Network Logs and Internet History

This exhibits shows the network logs recovered from the found Dell laptop and the network history of the user on the laptop

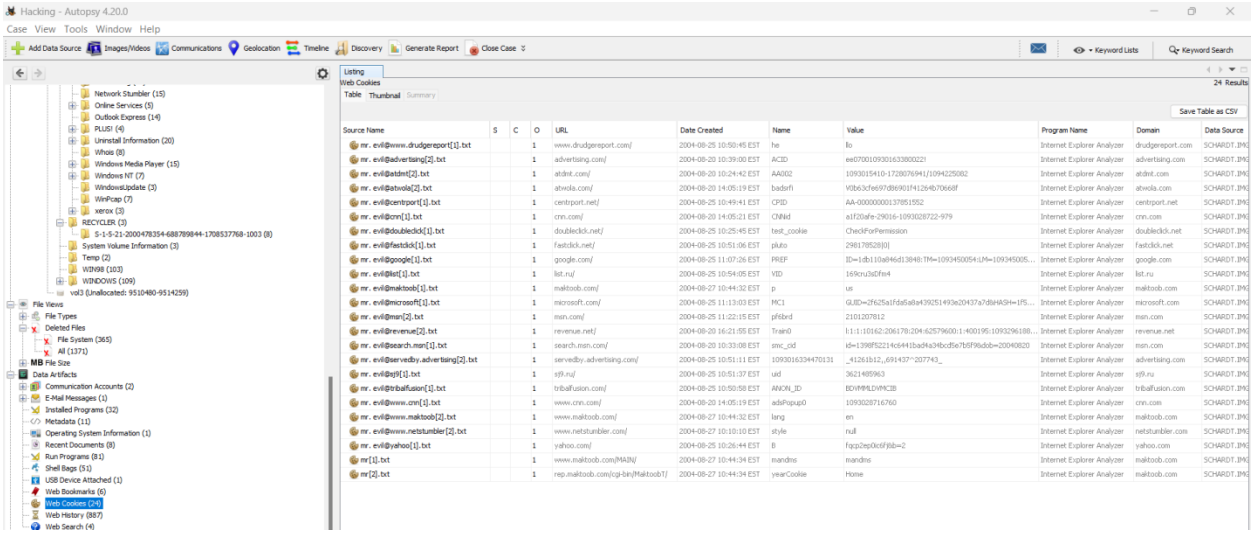


Figure 49. Web Cookies

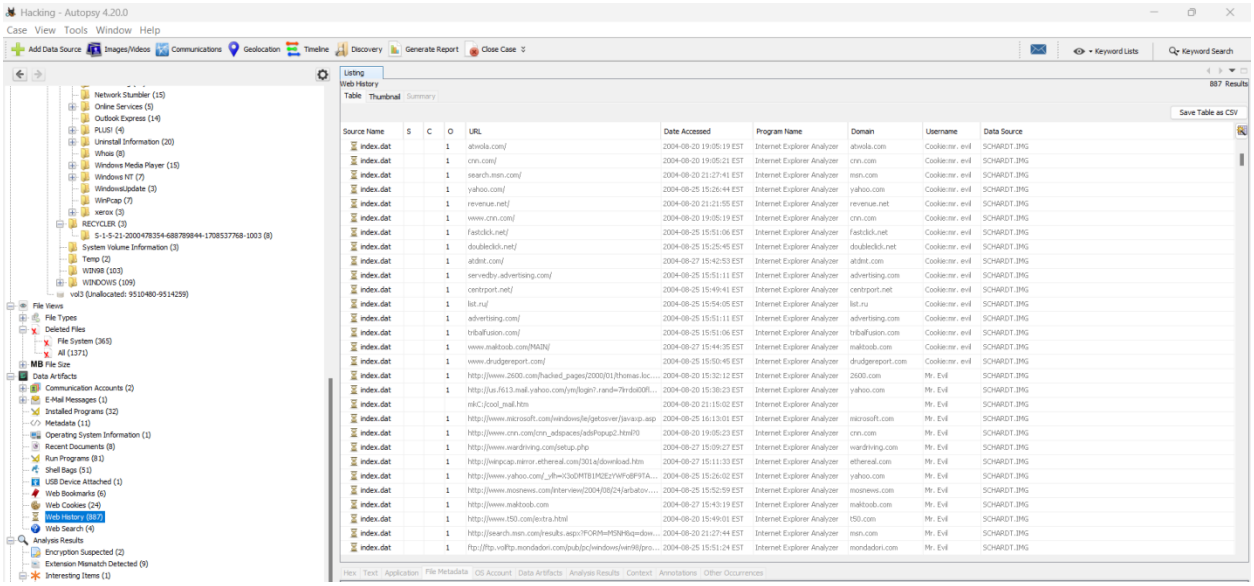


Figure 50. Web History

Exhibit 4: Network Sniffing Tool

This exhibit shows that the user used Ethereal, a network sniffing tool to capture the network traffic which stored the captured data in the interception file created by Ethereal.

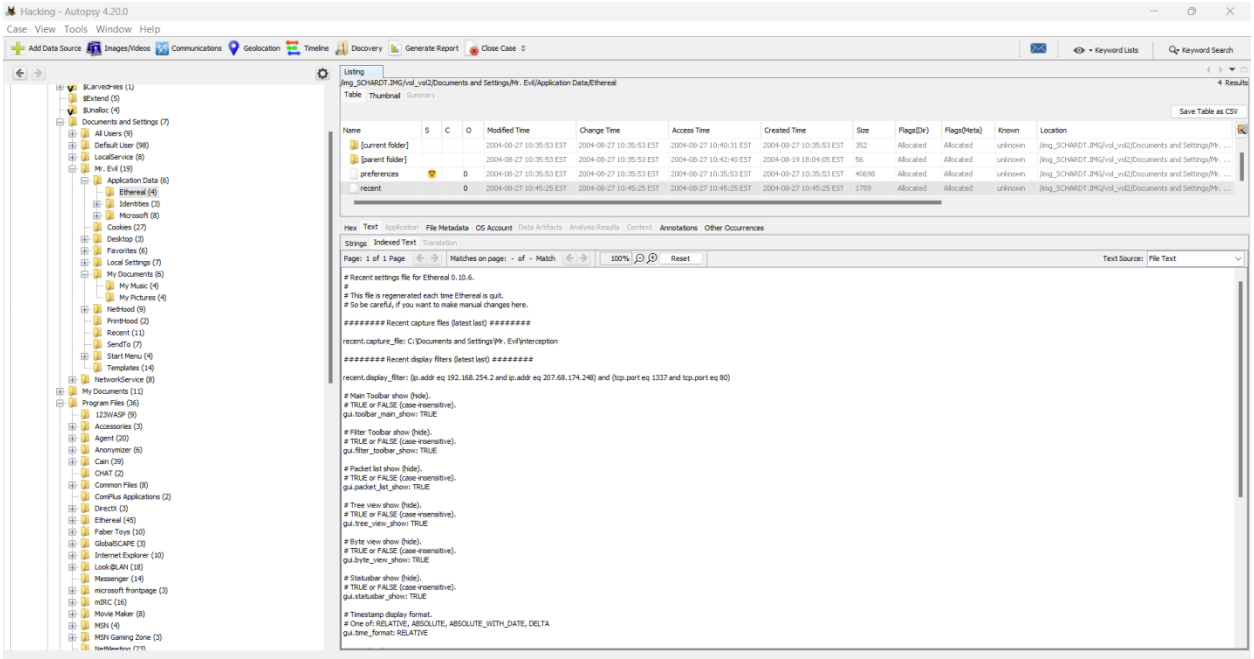


Figure 51. Ethereal's recent file

These four exhibits show that the suspected hacker, 'Greg Schardt' is Mr. Evil.

References

[1] https://cfreds.nist.gov/all/NIST/HackingCase

[2] https://www.autopsy.com/

[3] https://www.kali.org/docs/

[4] https://timestamp.online/

[5] https://doubleblak.com/blogPosts.php?id=7

[6] https://macaddress.io/mac-address-lookup/PRqn06Ke2M

[7] https://en.wikipedia.org/wiki/Cain_and_Abel_(software)

[8] https://hackersonlineclub.com/what-is-ethereal-hacking/

[9] https://en.wikipedia.org/wiki/NetStumbler

[10] https://pendriveapps.com/looklan-portable-network-monitor/

[11] https://www.majorgeeks.com/files/details/123_write_all_stored_passwords.html

[12] https://en.wikipedia.org/wiki/Anonymizer_(company)

[13] https://en.wikipedia.org/wiki/Fort%C3%A9_Agent

[14] https://en.wikipedia.org/wiki/MIRC

[15] https://en.wikipedia.org/wiki/Zip_bomb