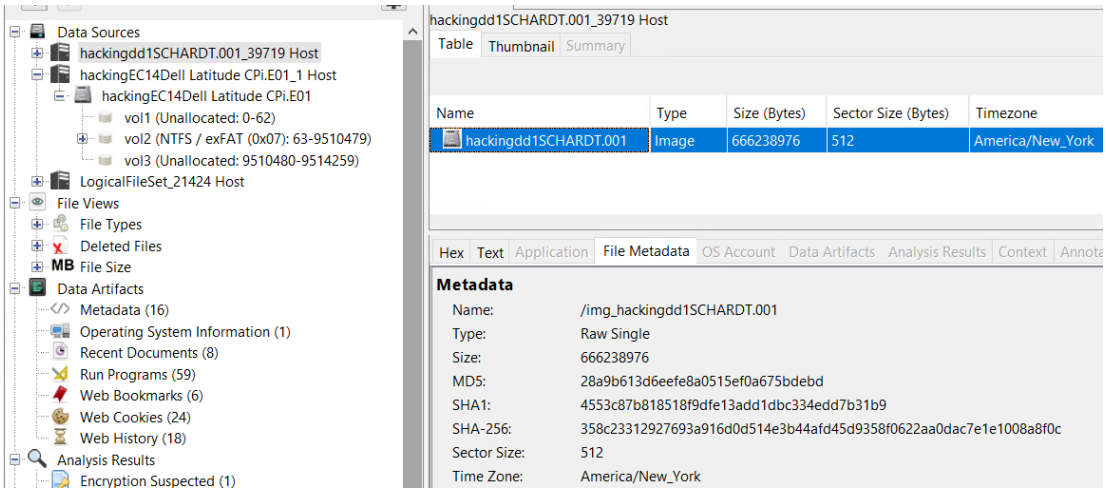
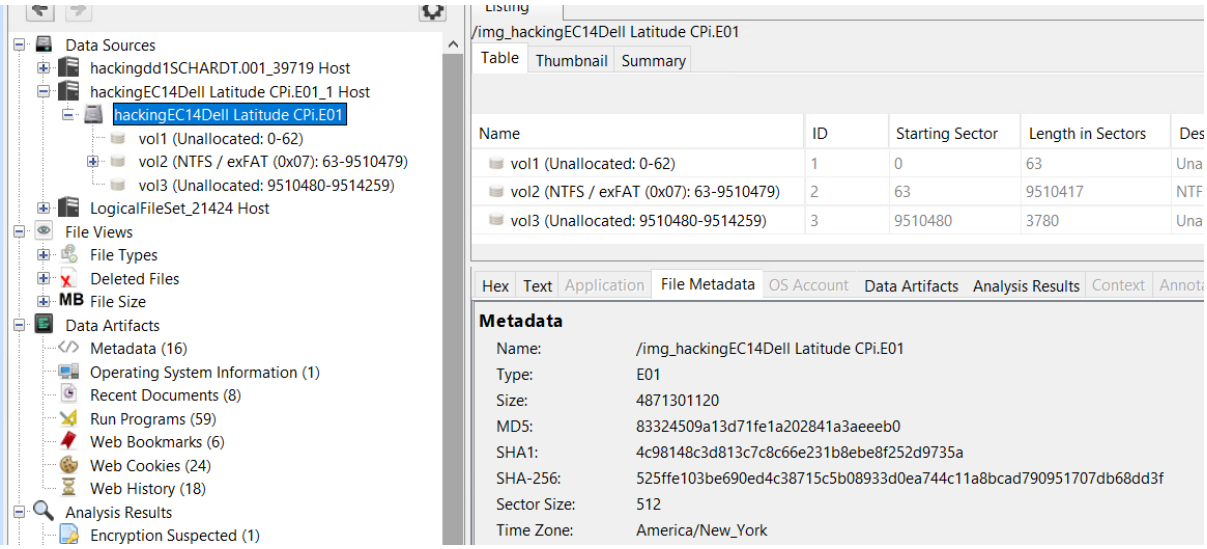
1. What is the image hash? Does the acquisition and verification hash match?

Answer: There are 2 image files related to the case. One is a .dd (Raw/DD) image file named "**hackingEC14Dell Latitude Cpi.dd**" and other is a .E01(EnCase image) image file named "**hackingEC14Dell Latitude Cpi.E01**"

- **MD5 hash of .dd image (hackingEC14Dell Latitude CPi):** 28A9B613D6EEFE8A0515EF0A675BDEBD
- This hash value can be found in the "File Metadata" tab on the home screen of the image.



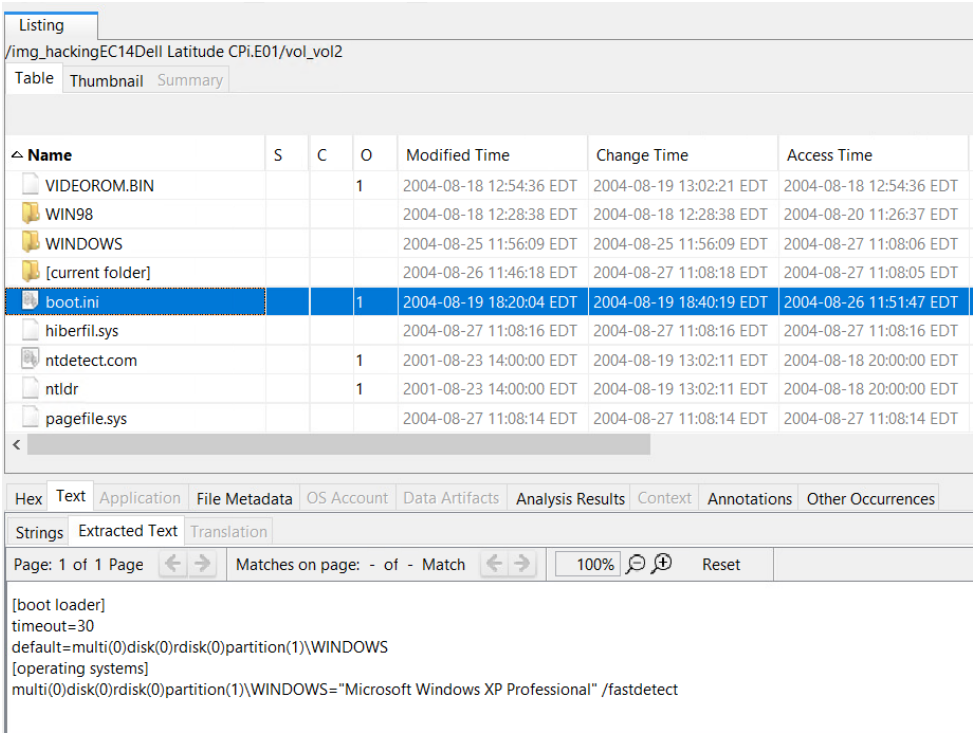
- **MD5 hash of .E01 image (hackingEC14Dell Latitude Cpi.E01):** 83324509a13d71fe1a202841a3aeeeb0.
- This hash value can be found in the "File Metadata" tab on the home screen of the image.



2. What operating system was used on the computer?

Answer: The OS and its version on the computer is "**Microsoft Windows XP Professional.**" This information can be located in the file named **"boot.ini"** inside the C: drive.

- **Path:** /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/boot.ini



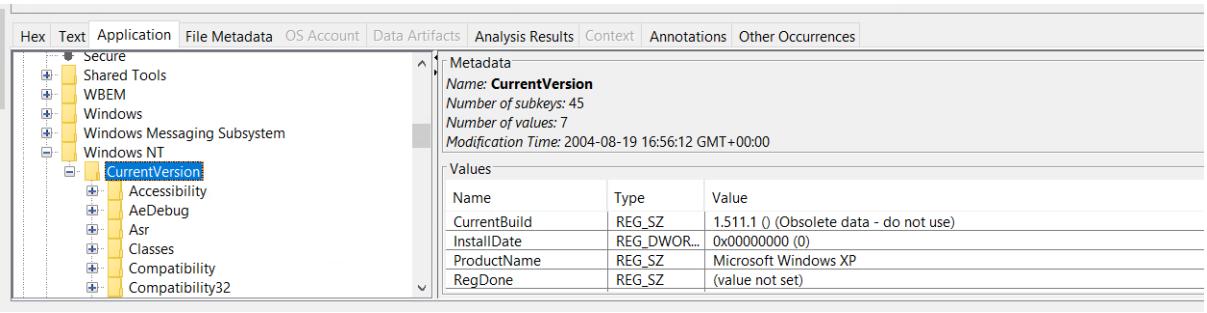
- Why "boot.ini" file and not the other file?

The **boot.ini** file is a text file used by older versions of Windows (Windows NT, 2000, and XP) to control the boot process. It essentially acts as a configuration file for the NTLDR (NT Loader) bootloader. It specifies the available **operating systems on a computer** and allows the user to choose which one to load during startup. It also contains settings that influence how the selected operating system boots.

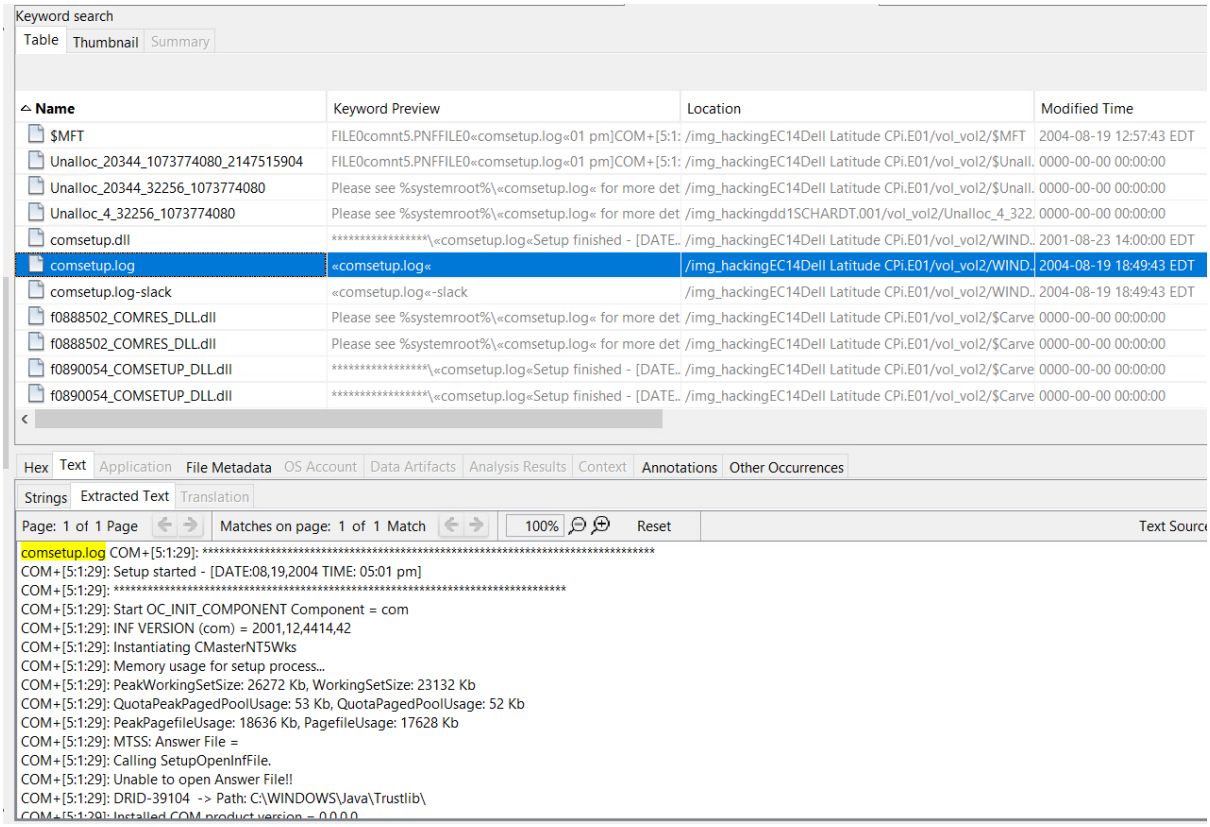
3. When was the install date?

Answer: In a Windows system, the primary file that stores information about the Windows installation date is the **Registry**. Specifically, the following registry key contains the installation date:

- **Path**: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate



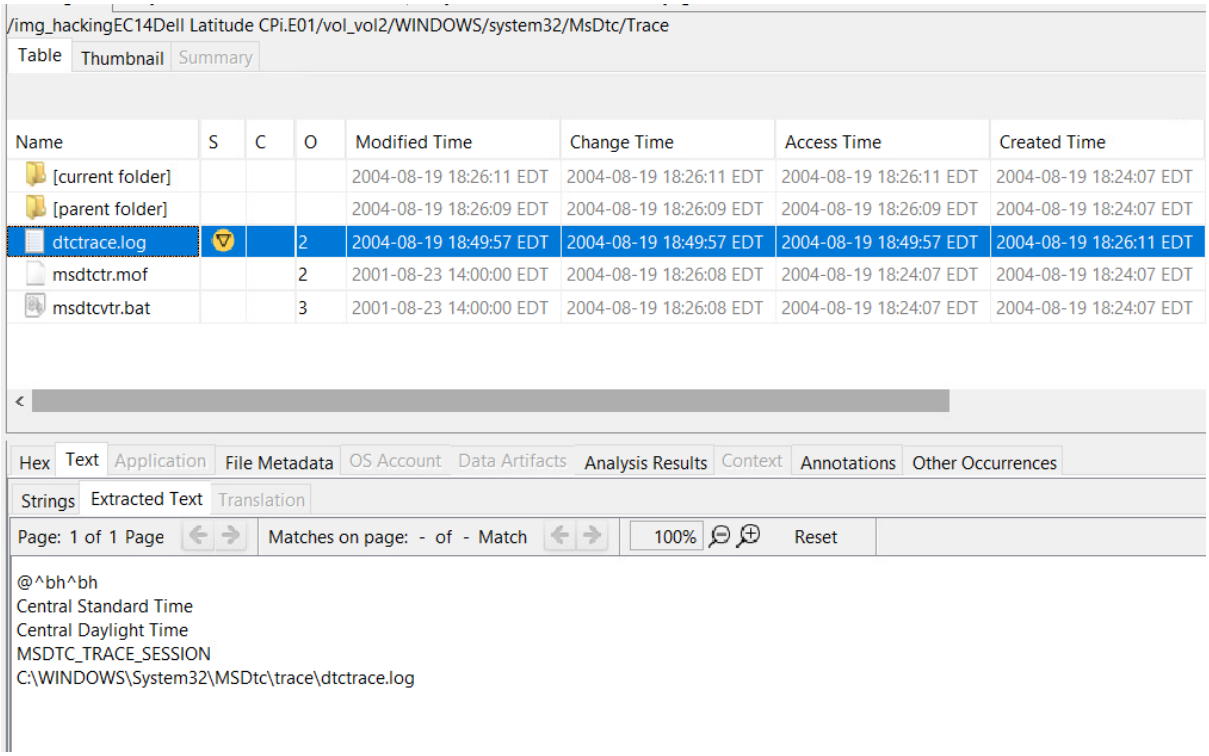
The **InstallDate** value in this key store the installation date as a **Unix timestamp**. But here in this case the value of this key is corrupted or formatted. Thus, now this information can be acquired for the **comsetup.log** file.



4. What is the time zone settings?

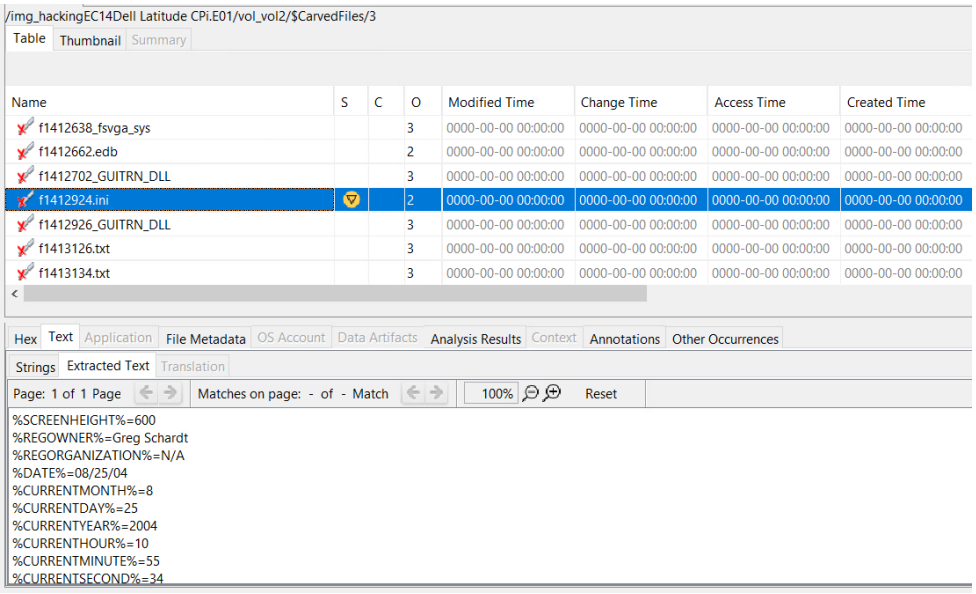
Answer: The time zone of the device is Central Daylight Time (CDT).

- **Path**: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/MsDtc/Trace/dtctrace.log



5. Who is the registered owner?

Answer: The owner of this device is "**Greg Schardt**". This information is derived from a deleted registry file which is named "**f1412924.ini**". Basically, "**.ini**" files are files that store configuration settings in Windows. It is a part of a registary hive in Windows.

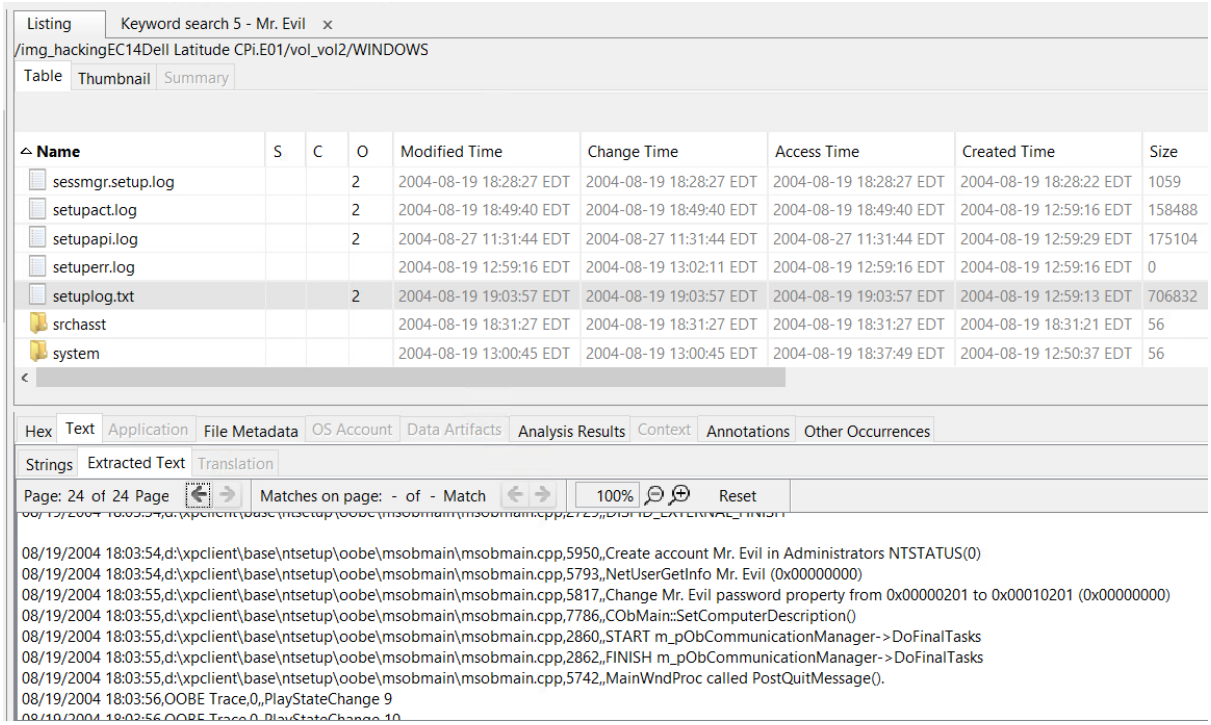


- **Path**:/img_hackingEC14Dell LatitudeCPi.E01/vol_vol2/$CarvedFiles/3/f1412924.ini

6. What is the computer account name?

Answer: The account name on the computer is “**Mr. Evil**”. This data can be found from page **24 of** the “**setup.log**” file, which is a log file generated during the Windows XP Out-of-Box Experience (OOBE) phase.

- The **OOBE** is the initial setup process that a user goes through after installing Windows for the first time. It typically involves tasks such as creating user accounts, setting up network connections, and registering the operating system.
- From this file, it can be known that a user account with the username "Mr. Evil" was created and added to the Administrators group.
- **Path:** /img_hackingEC14Dell LatitudeCPi.E01/vol_vol2/WINDOWS/setuplog.txt



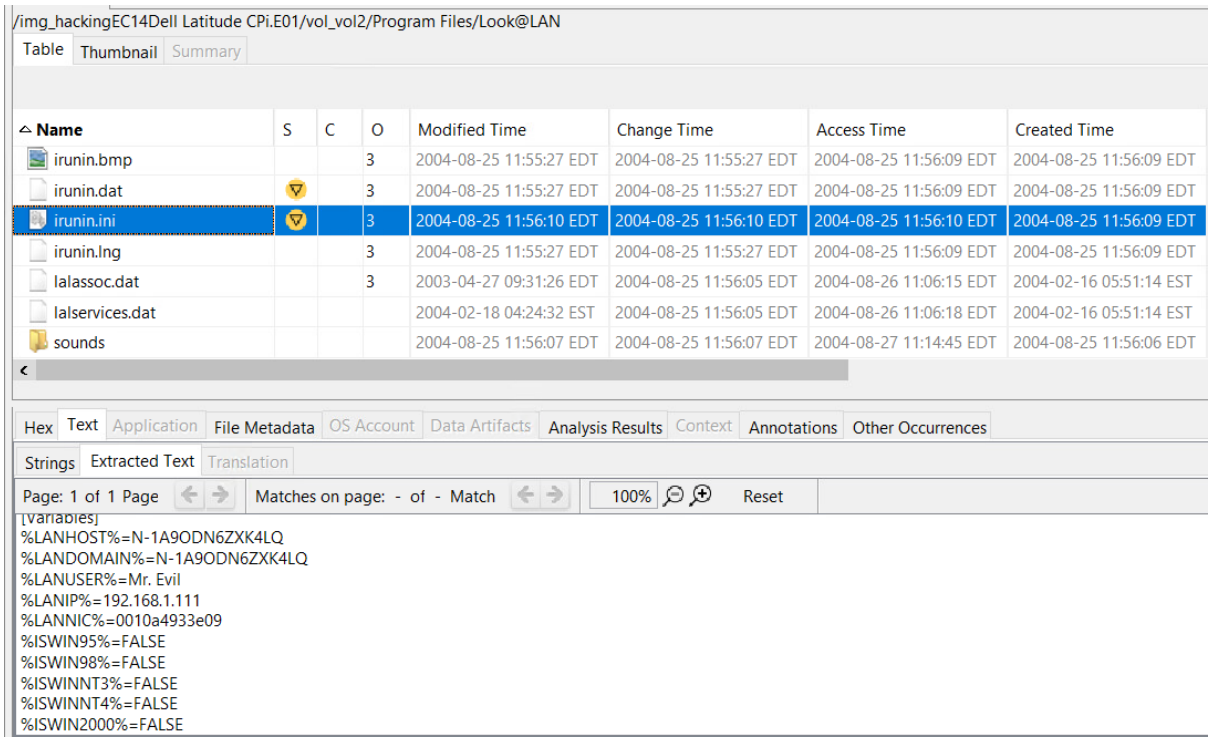
7. What is the primary domain name?

Answer: The primary domain name is “N-1A9ODN6ZXK4LQ”. The evidence for this answer comes from two variables “**%LANHOST%=N-1A9ODN6ZXK4LQ**” and “**%LANDOMAIN%=N-1A9ODN6ZXK4LQ**” found within the **irunin.ini** file.

- **Path**: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN/irunin.ini

Why this evidence:

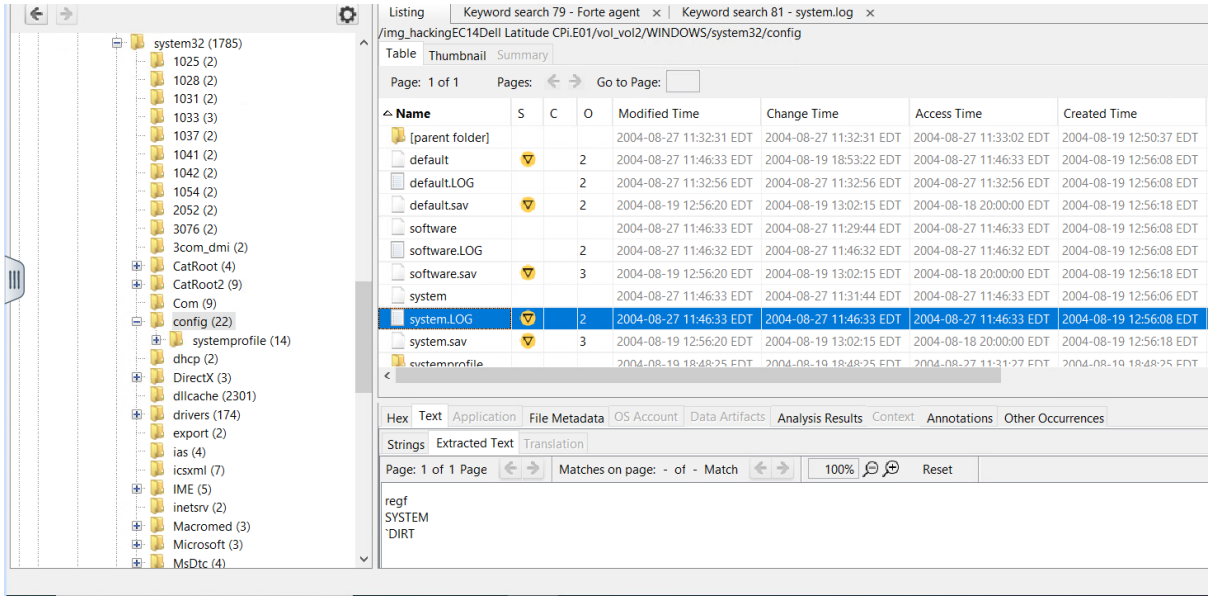
- The file **irunin.ini** appears to be a configuration file for the "Look@LAN" software, which is likely a network monitoring or management tool.
- The variable names %LANHOST% and %LANDOMAIN% strongly suggest they are related to the network environment where the software operates.



8. When was the last recorded computer shutdown date/time?

Answer: The last recorded shutdown time is " 15:46:33.1092164 Z UTC" which means 27-08-2004 11:46 EDT. This evidence can be recovered from the Windows registry, but in this system, the registry is corrupted. Thus, this data can be interpreted from the "**System.log**" file. Here, the access, create and modify time can be used to indicate the system startup and shutdown time.

- **Path**: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/system.log



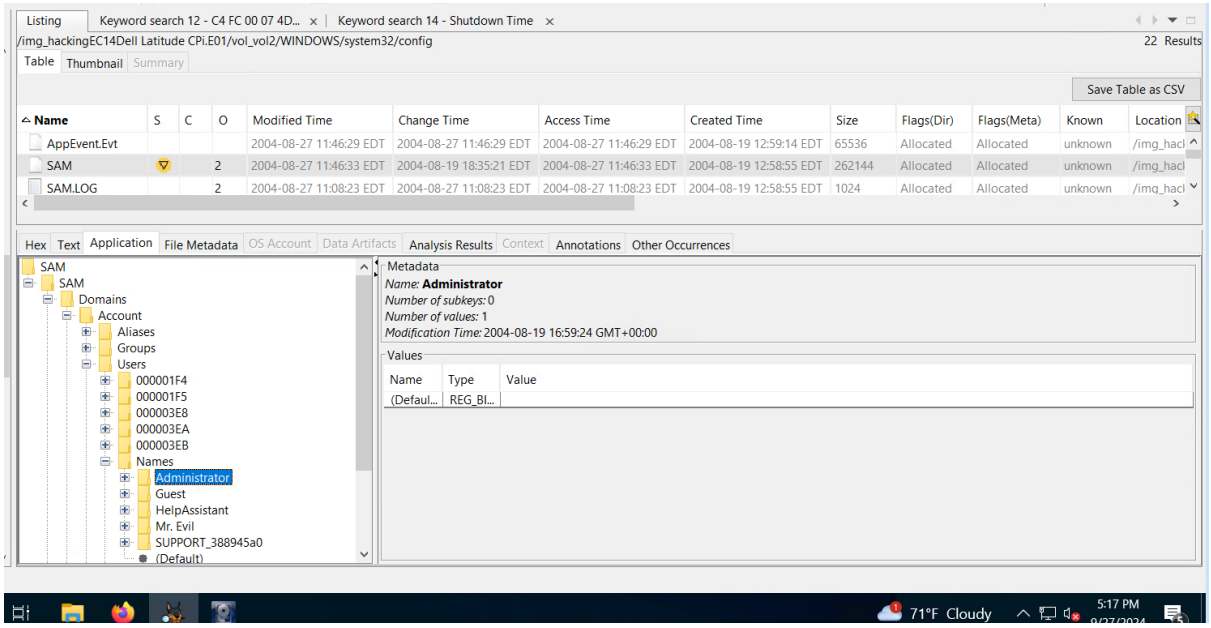
The **system.log** is maintained by the Windows Event Log service. Contains a chronological record of system-level events, including:

- **Startup and shutdown events:** Crucial for tracking system uptime and identifying potential issues during boot or shutdown.
- **Device installations and driver updates:** Useful for understanding hardware changes and potential compatibility problems.
- **Application installations and uninstalls:** Helps track software changes and identify potential malicious activity.
- **Security events:** Logs logon/logoff attempts, policy changes, and other security-related events.
- **Error and warning messages:** Can reveal critical system failures, application crashes, or other issues requiring attention.

9. How many accounts are recorded (total number)?

Answer: The computer has a total of 5 user accounts: Administrator, Guest, HelpAssistant, Mr. Evil and SUPPORT_388945a0. This information can be located in the SAM registry hive of the Windows file system.

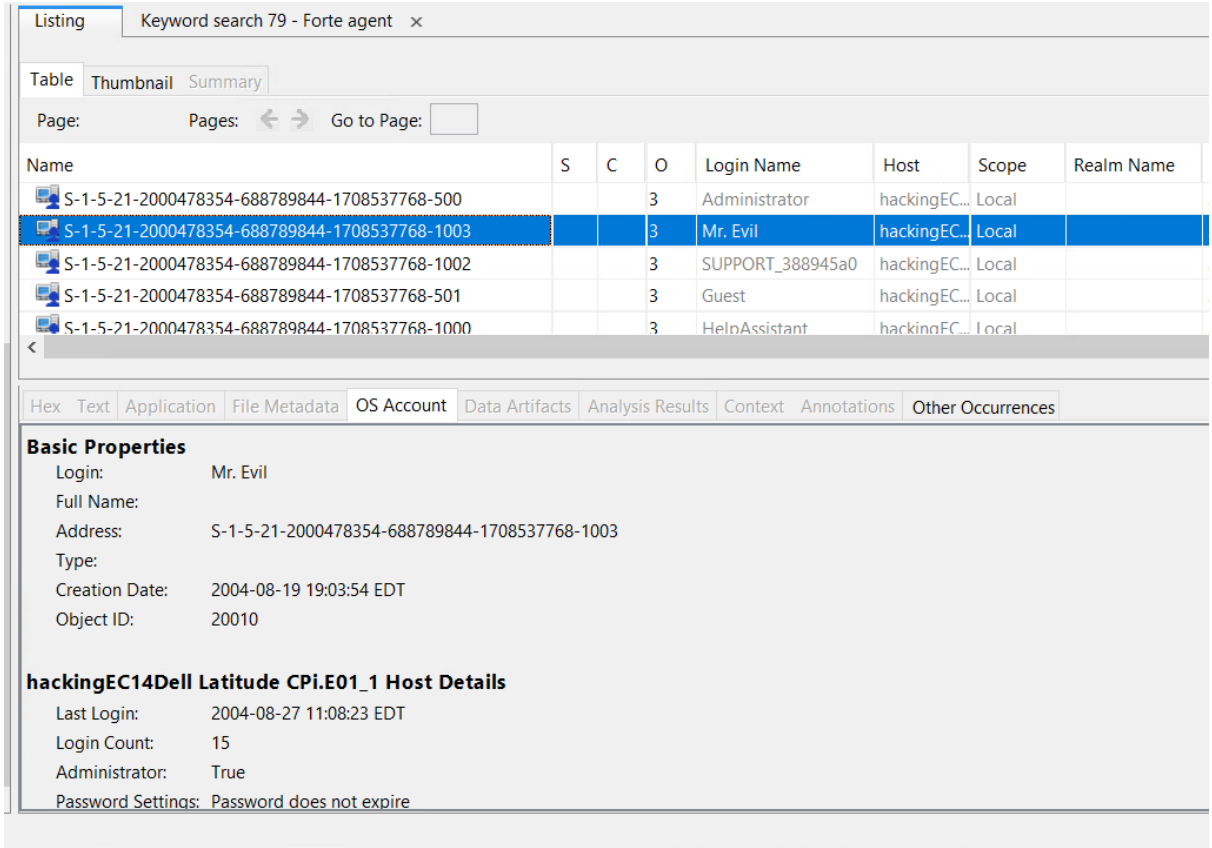
- **Path**:/img_hackingEC14Dell LatitudeCPi.E01/vol_vol2/WINDOWS/system32/config/SAM



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

Answer: The person who mostly uses the computer is Mr. Evil. Because as per the file metadata of his user profile, he has done 15 logins into the system which is the most compared to other users.

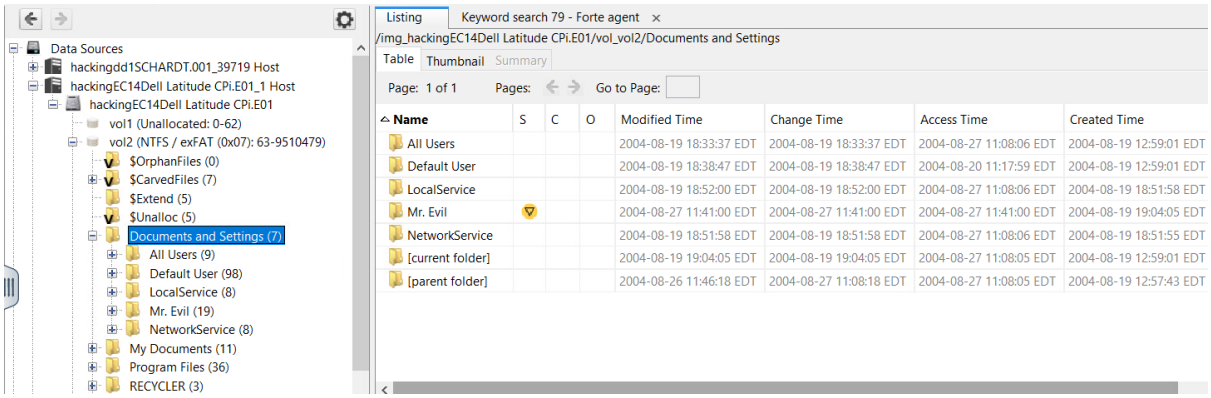
USERS	LOGINS
Administrator	0
Mr. Evil	15
Support_388945a0	0
Guest	0
HelpAssistant`	0



11.Who was the last user to logon to the computer?

Answer**:** The last user who logged into the computer was "**Mr. Evil**". This can be inferred from the user profiles of the system. Out of all the users, the **Modify time** of Mr. Evil's profile is the latest i.e. 27 August 2004 at 11:41 EDT. This it can be interpreted that Mr. Evil was the last person to access the computer.

- **Path**: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil

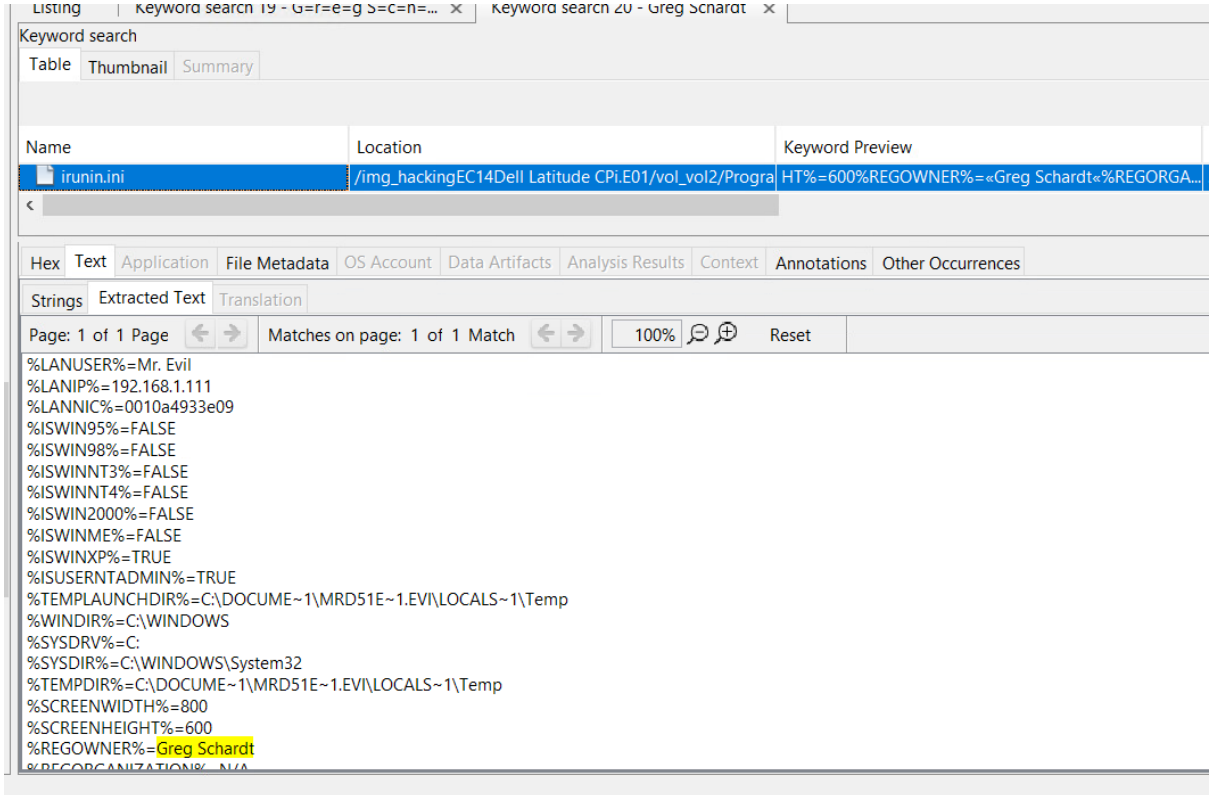


12.. A search for the name of “G=r=e=g S=c=h=a=r=d=t” reveals multiple hits. One of these proves that G=r=e=g S=c=h=a=r=d=t is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to?

Answer: The File name where this evidence is found is “**irunin.ini**”. The file **irunin.ini** appears to be a configuration file for the "Look@LAN" software, which is likely a network monitoring or management tool. The irunin.ini file contains variables that directly link "G=r=e=g S=c=h=a=r=d=t" to both the "Mr. Evil" user account and the administrator role.

- **Verification:**
  - **%LANUSER%**=Mr. Evil shows that "Mr. Evil" is the user associated with Look@LAN.
  - **%REGOWNER%=**Greg Schardt indicates that "Greg Schardt" is the registered owner of the system.
  - **%ISUSERNTADMIN%=**TRUE confirms that the "Mr. Evil" account has administrator privileges.

- **Path:** /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN/irunin.ini



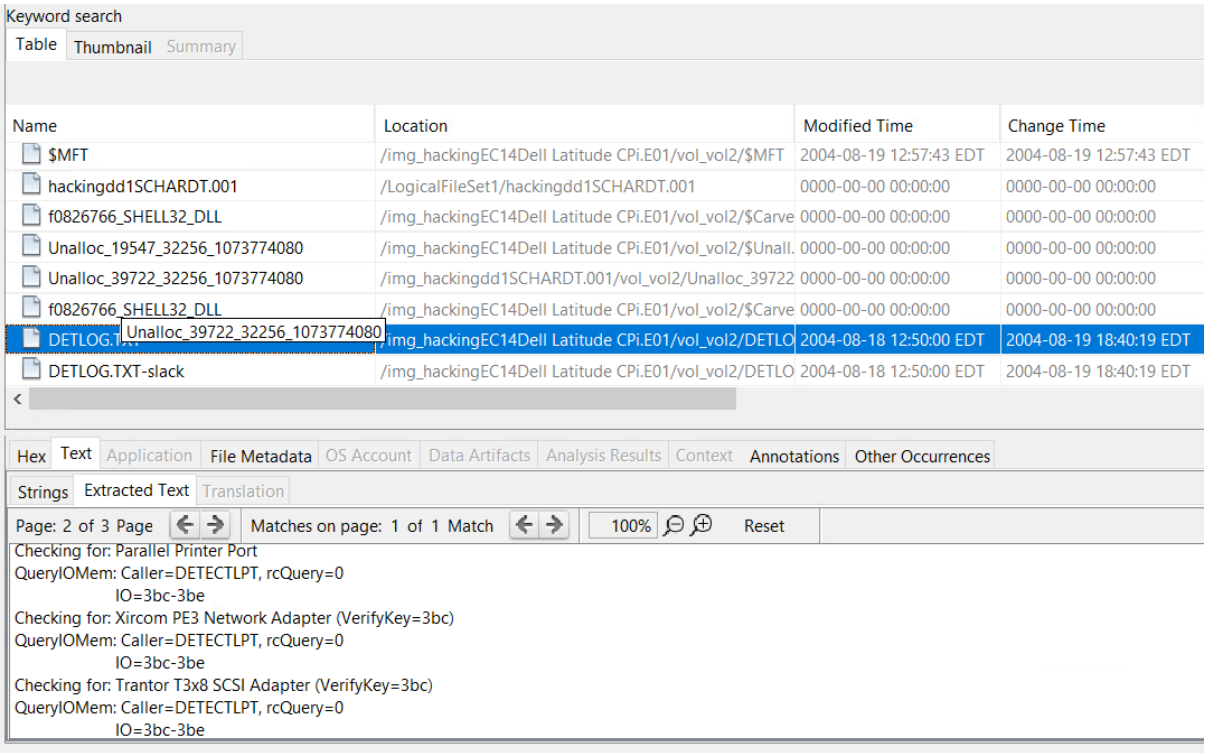
13. List the network cards used by this computer.

Answer: The were 2 network cards used by this computer. They are Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface) & Compaq WL110 Wireless LAN PC Card. Based on the **detlog.txt**, the following network cards were detected on the computer:

1. **Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)**

Evidence location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/DETLOG.TXT

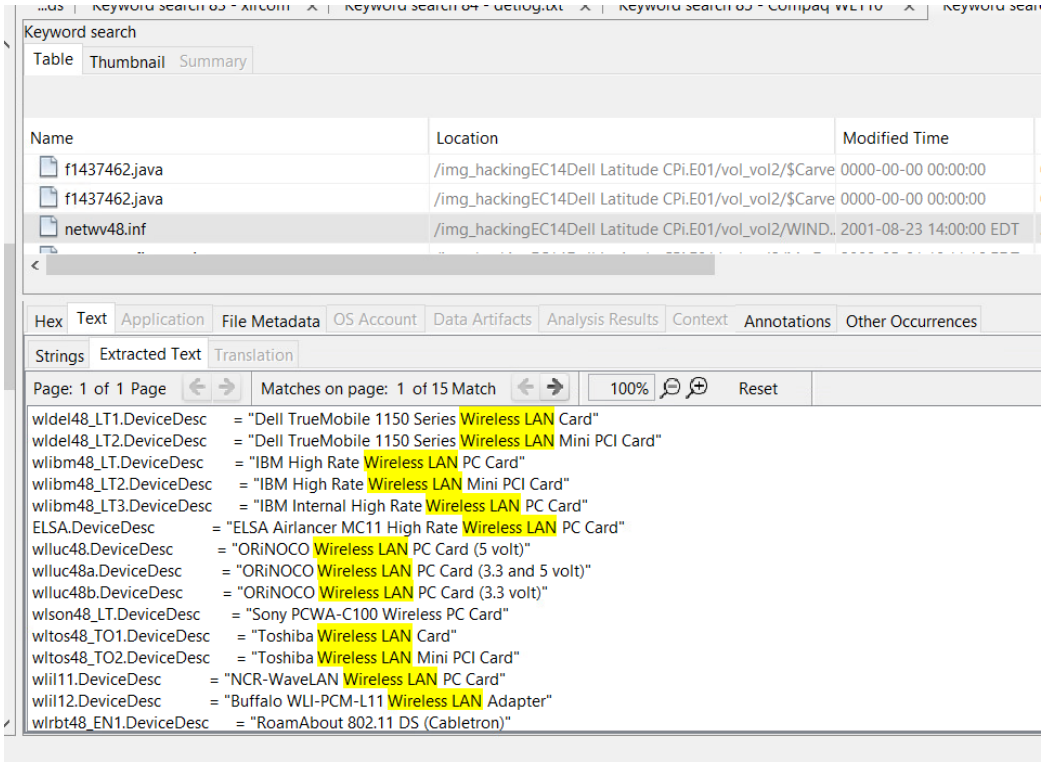
- The log entry [2004/08/19 17:07:10 280.1058 Driver Install] shows a search for hardware IDs related to pci\ven_115d&dev_0003.
- It then finds a match in C:\WINDOWS\inf\netcbe.inf for a device named "Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)".
- Subsequent entries indicate the successful installation of drivers for this device.



2. **Compaq WL110 Wireless LAN PC Card**

Evidence location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/inf/netwv48.inf

- **Device Identification:** The file explicitly lists the "Compaq WL110 Wireless LAN PC Card" under the [Compaq] section, associating it with the driver **wlluc48.Install** and the hardware ID **PCMCIA\COMPAQ-COMPAQ_WL110_PC_CARD-E648**.
- **Driver Installation:** The **[wlluc48.Install]** section details the installation process for this driver, including copying files (wlluc48.CopyFiles) and adding a service (wlluc48.Service) for the wireless card.
- **Service Details:** The [wlluc48.Service] section further confirms the association with the "Wireless LAN PC Card Driver."

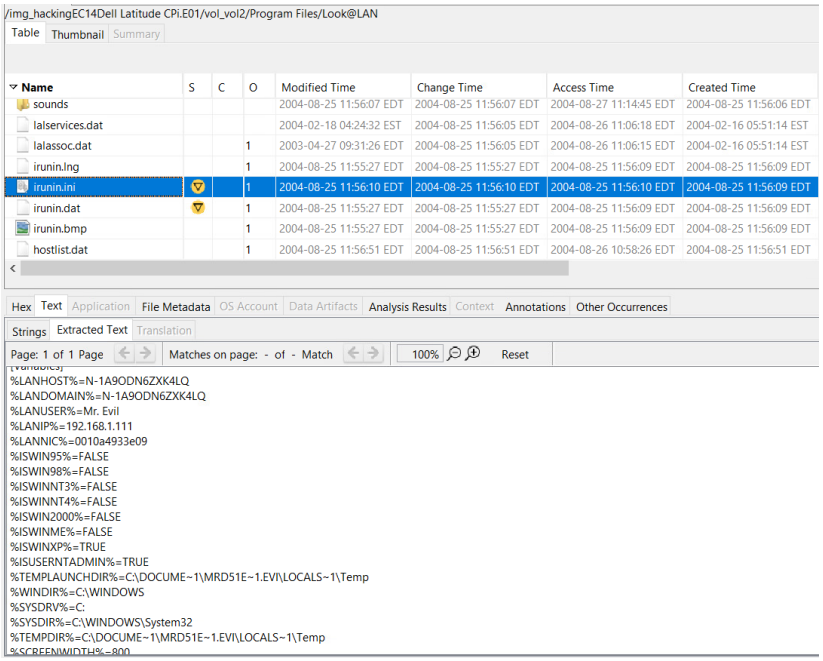


This indicates that the netwv48.inf file contains the necessary information to install drivers for network cards from these various manufacturers, even though the specific log excerpts you provided might not show them being actively installed on this system.

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

Answer: The IP: 192.168.1.111 and MAC: 0010a4933e09

- **File Name:** irunin.ini
- **File Path:** /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN/irunin.ini
- **Evidence:**



- **Why this file and not others:** The *"irunin.ini"* file appears to be a configuration file for the "**Look@LAN**" software, which is likely a network monitoring and management tool. Configuration files often store settings related to the network environment, including network interfaces and their addresses. While this file doesn't explicitly name the network card model, the presence of the MAC and IP address variables suggests it's a good place to look for network-related information.

- **Source of evidence:** The ***irunin.ini*** file provide evidence related to network connectivity:
  - **%LANNIC%=0010a4933e09:** This variable represents the MAC (Media Access Control) address of the network card. A MAC address is a unique identifier assigned to a network interface.

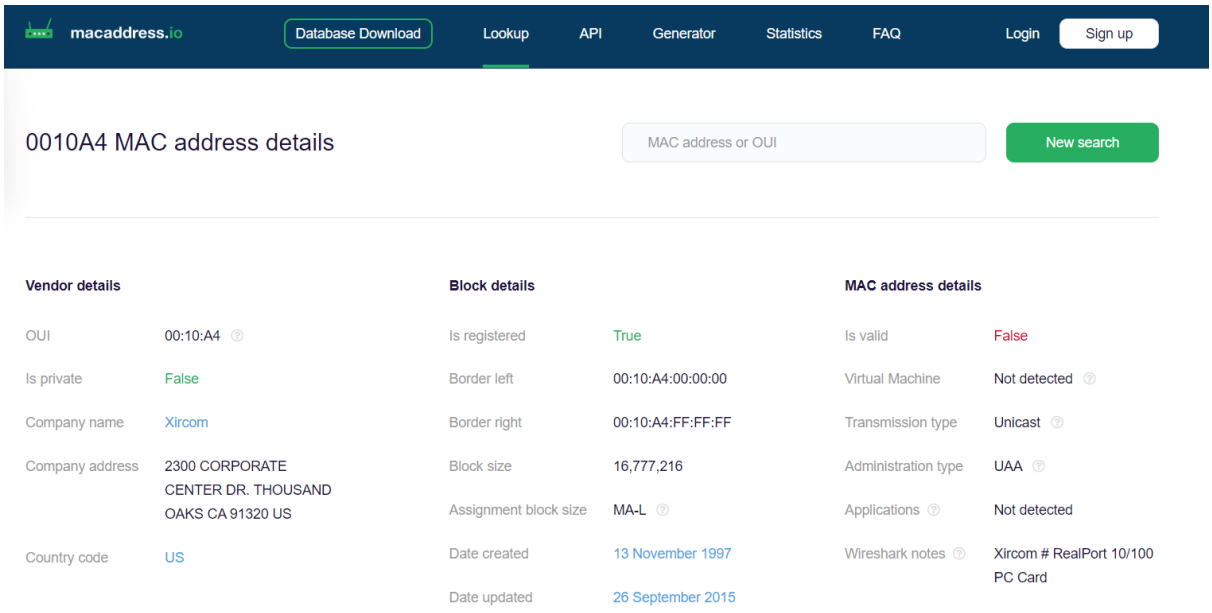
- **%LANIP%=192.168.1.111:** This variable indicates the IP (Internet Protocol) address assigned to the computer on the network.

15. An internet search for vendor name/model of NIC cards by MAC address can be used to find out which network interface was used. In the above answer, the first 3 hex characters of the MAC address report the vendor of the card. Which NIC card was used during the installation and set-up for LOOK@LAN?

Answer: Based on the MAC address information provided in the search result, the NIC card used during the installation and setup for Look@LAN was a **Xircom RealPort 10/100 PC Card**.

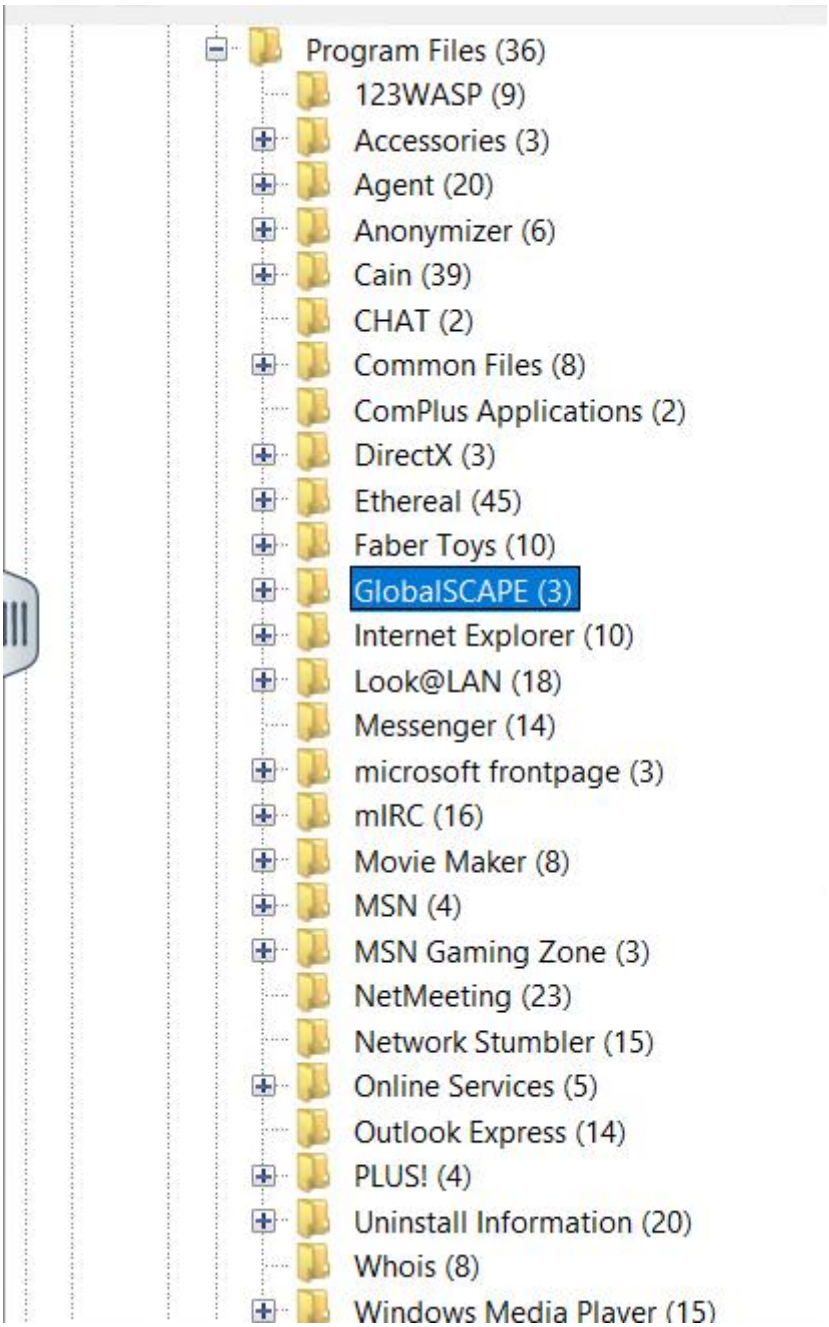
The search result clearly states that the MAC address prefix "00:10:A4" belongs to the vendor "Xircom," and the "Wireshark notes" further specify the model as "RealPort 10/100 PC Card."

This aligns with the information found in the irunin.ini file where the variable %LANNIC% was set to 0010a4933e09. The first three bytes of this MAC address match the "00:10:A4" prefix, confirming the vendor as Xircom.



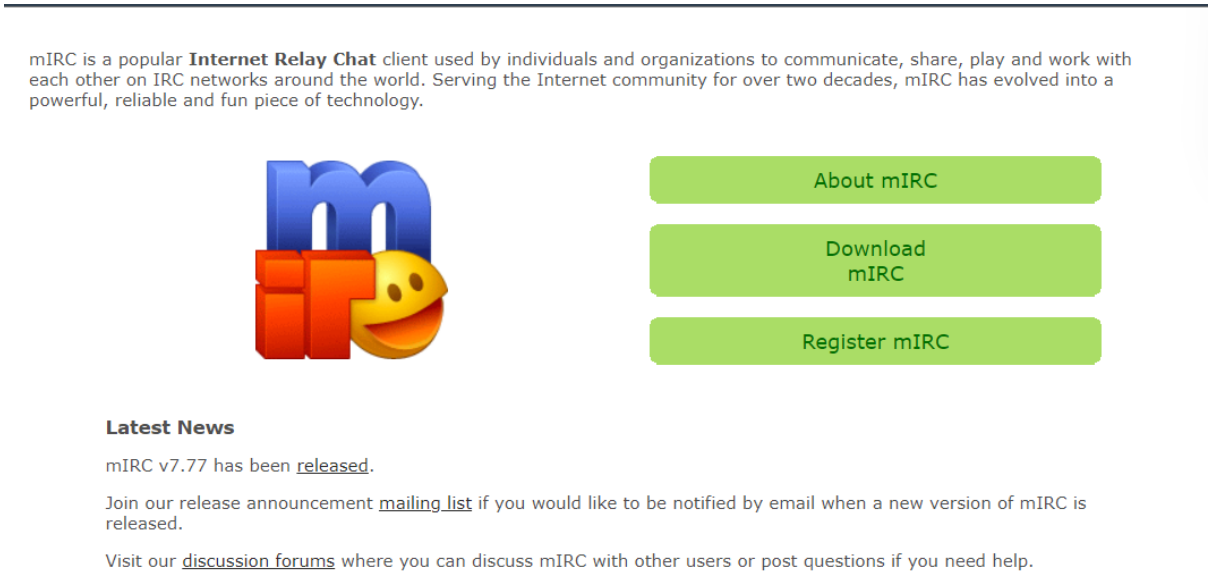
16. Find 6 installed programs that may be used for hacking.

Answer: The list of all the installed files can be found in C:\Program Files and directoriy. Within the directory there are multiple folders with application names or publisher names. These folders typically contain executable files, DLLs, configuration files, and other data related to the installed applications.



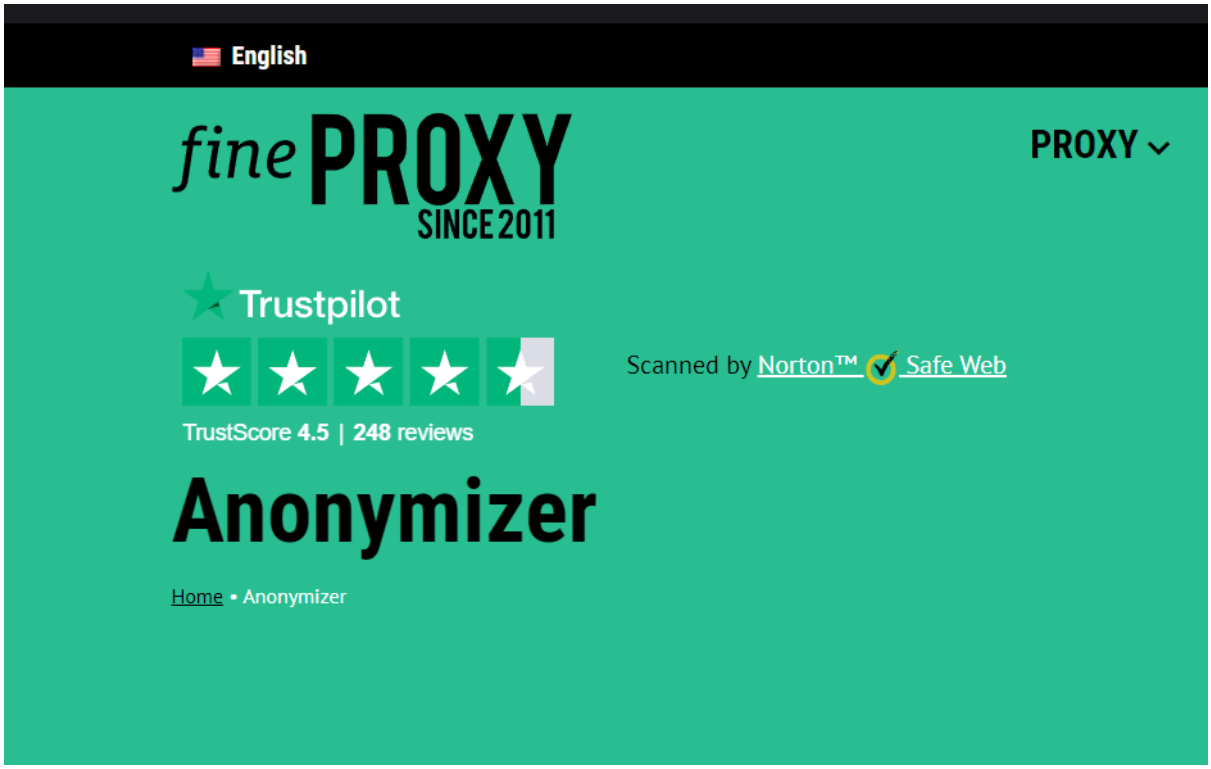
The 6 installed programs are:

1) mIRC: Internet Relay Chat client

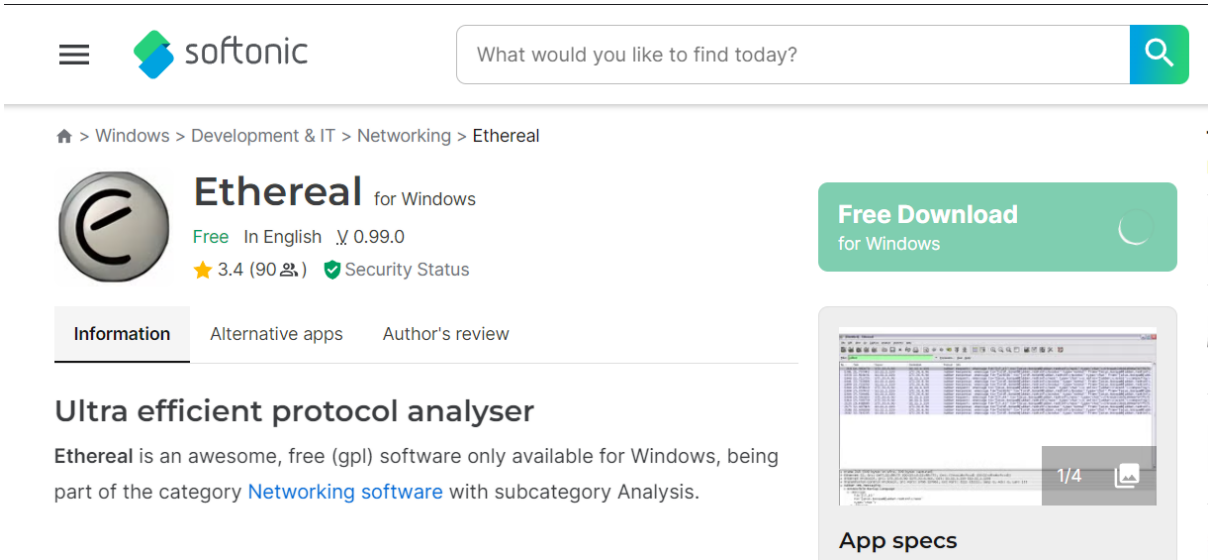


2) Look@LAN:

3) Anonymizer: Proxy tool



4) Ethereal: Packet sniffing tool



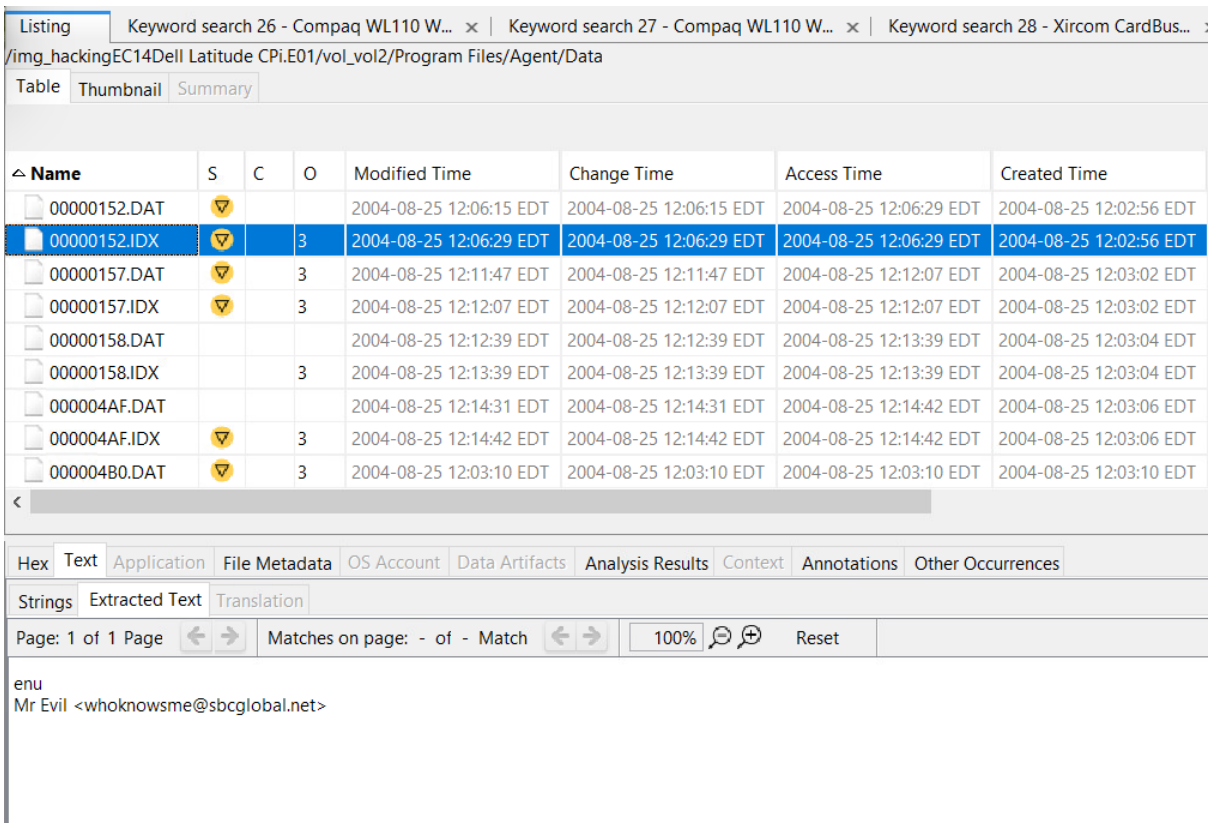
5) 123WASP: display all passwords of the currently logged on user

6) Faber Toys: System utility to know what's going on the personal computer

17. . What is the SMTP email address for Mr. Evil?

Answer: The email address of Mr. Evil is "**whoknowsme@sbcglobal.net**". This can be located in the "**00000152.IDX" file.** An .idx file is an index file for an Outlook Express mailbox. It stores pointers to messages within the mailbox, aiding in faster access and organization.

- **Path:** /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/00000152.IDX

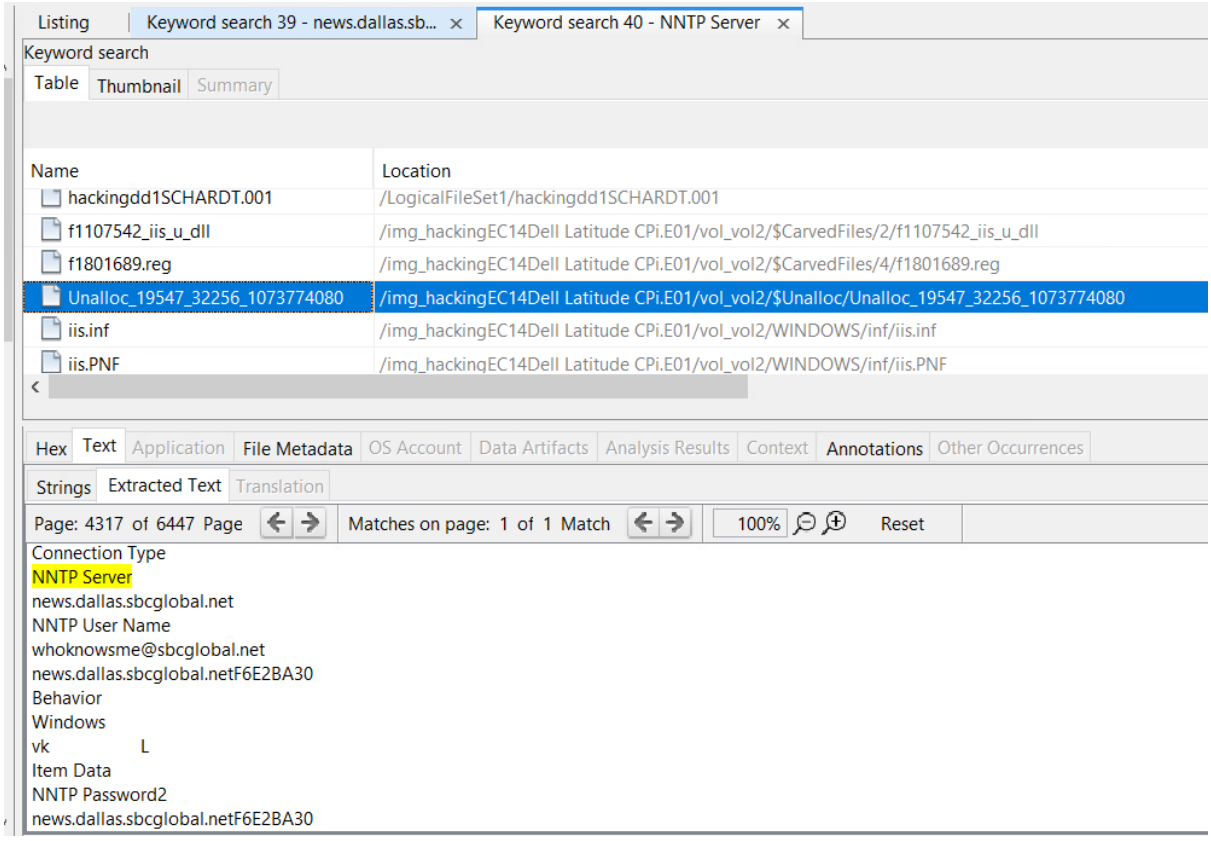


18. What is the NNTP (news server) settings for Mr. Evil?

Answer: The NNTP server information is ad follows:

- **Account Name:** news.dallas.sbcglobal.net
- **Connection Type:** NNTP Server
- **NNTP Server:** news.dallas.sbcglobal.net
- **NNTP User Name:** whoknowsme@sbcglobal.net
- **NNTP Password2:** news.dallas.sbcglobal.netF6E2BA30

➢ **Path**: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/$Unalloc/Unalloc_19547_32256_1073774080



Unallocated space is the area on a hard drive or other storage device that is not currently being used by the file system to store active files. It may contain remnants of previously deleted files or other data that has not yet been overwritten and also contains traces of past activity on the system, including deleted files, internet history, or configuration settings.

19. What two installed programs show this information?

Answer: The 2 installed programs are **Forete Agent** and **Microsoft Outlook Express.**

- **Path:** /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/$Unalloc/Unalloc_19547_1073774080_2147515904

Listing | Keyword search 79 - Forte agent

/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/$Unalloc

Table | Thumbnail | Summary

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

Strings | Extracted Text | Translation

Page: 89 of 106 Page | Matches on page: - of - Match | 100% | Reset

@newsg1.svr.pol.co.uk> <a0LTc.25642$%r.269581@nasal.pacific.net.au> <MPG.1b8b2a6cf5af0c09989690@news.easynews.com>
91@news.easynews.com> <urefi0177k08iecibphbbaju5afk750cii@4ax.com>
Subject: Re: Ad-aware SE Professional Edition v1.03
Lines: 3
X-Priority: 3
X-MSMail-Priority: Normal
X-Newsreader: Microsoft Outlook Express 6.00.2800.1437
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1441
Message-ID: <BxQVc.26094$%r.291654@nasal.pacific.net.au>
Date: Sun, 22 Aug 2004 09:01:45 +1000
NNTP-Posting-Host: 203.143.247.95
X-Complaints-To: news@pacific.net.au
X-Trace: nasal.pacific.net.au 1093129441 203.143.247.95 (Sun, 22 Aug 2004 09:04:01 EST)
NNTP-Posting-Date: Sun, 22 Aug 2004 09:04:01 EST
Organization: Pacific Internet (Australia)
Xref: newsmst01a.news.prodigy.com alt.cracks:872833 alt.binaries.hacking.beginner:57876 alt.hacker:303243
X-Agent-Group: alt.binaries.hacking.beginner
Amber ignore Advanced Feature he is our regular spammer and pain in the ass.
multipart/singleus-ascii
text/plain
acific.net.au 1093129441 203.143.247.95 (Sun, 22 Aug 2004 09:04:01 EST)
NNTP-Posting-Date: Sun, 22 Aug 2004 09:04:01 EST
Organization: Pacific Internet (Australia)
Xref: newsmst01a.news.prodigy.com alt.cracks:872833 alt.binaries.hacking.beginner:57876 alt.hacker:303243
X-Agent-Group: alt.binaries.hacking.beginner

Table | Thumbnail | Summary

Page: 1 of 1 | Pages: | Go to Page:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Unalloc_19547_1073774080_2147515904				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

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

Strings | Extracted Text | Translation

Page: 89 of 106 Page | Matches on page: - of - Match | 100% | Reset

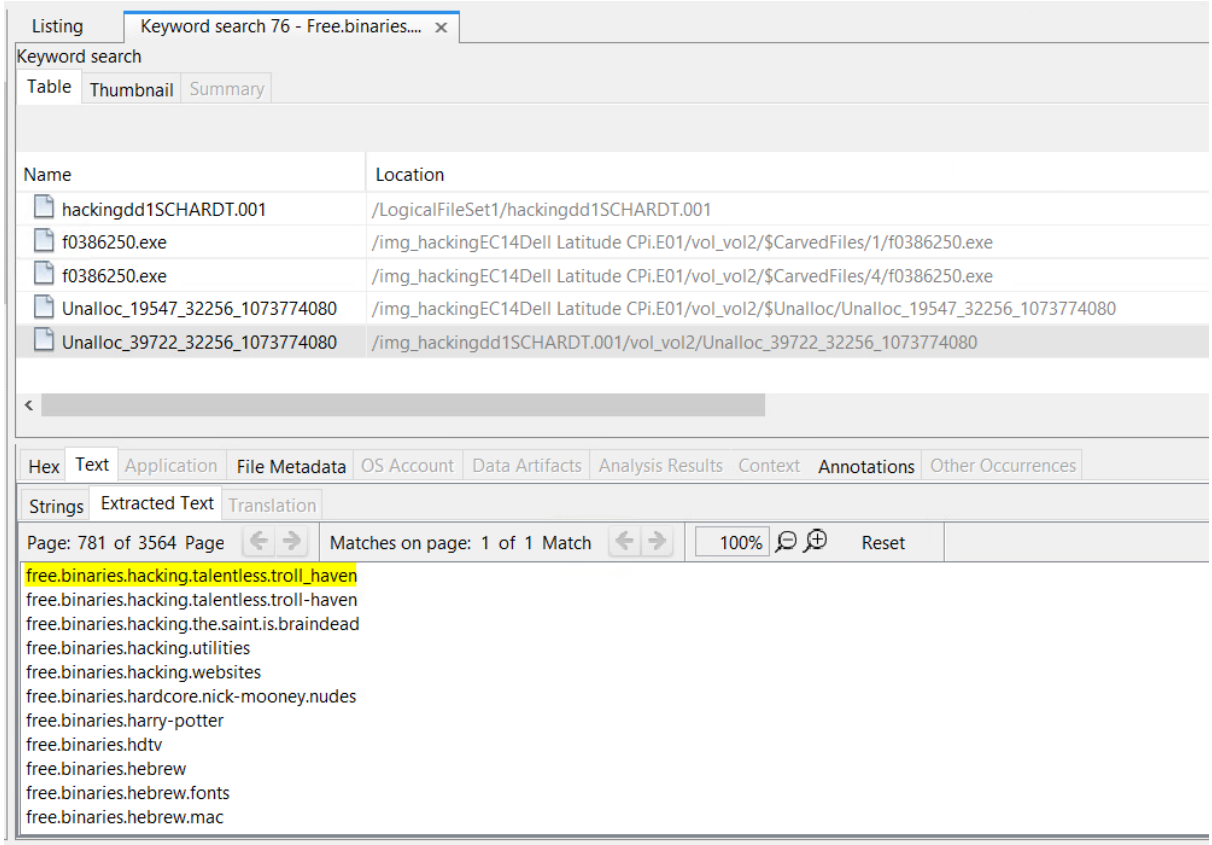
.291654@nasal.pacific.net.au> <MPG.1b91d6f1e9d369cd9896e3@News.100ProofNews.com>
X-Newsreader: Forte Agent 1.93/32.576 English (American)
X-No-Archive: yes
MIME-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 8bit
Lines: 9
NNTP-Posting-Date: Sun, 22 Aug 2004 11:03:33 EST
Date: Sun, 22 Aug 2004 10:08:51 -0600
Xref: newsmst01a.news.prodigy.com alt.cracks:872881 alt.binaries.hacking.beginner:57895 alt.hackers.malicious:477190 alt.hacker:303276
X-Agent-Group: alt.binaries.hacking.beginner
On Sat, 21 Aug 2004 23:02:59 -0230,
<me@use.net> wrote:
>In article <BxQVc.26094$%r.291654@nasal.pacific.net.au>,
>crackthisandcrackthat@hotmail.com says...
>> Amber ignore Advanced Feature he is our regular spammer and pain in the ass.
>...you want I should eat your spammer?
Give it a shot loser

20. List 5 newsgroups that Mr. Evil has subscribed to

Answer: The 5 newsgroups that Mr. Evil has subscribed to are:

I. Free.binaries.hacking.talentless.troll_haven
II. Free.binaries.hacking.utilities
III. Free.binaries.hacking.the.saint.is.braindead
IV. Free.binaries.hacking.websites
V. Free.binaries.hacking.hebrew.mac

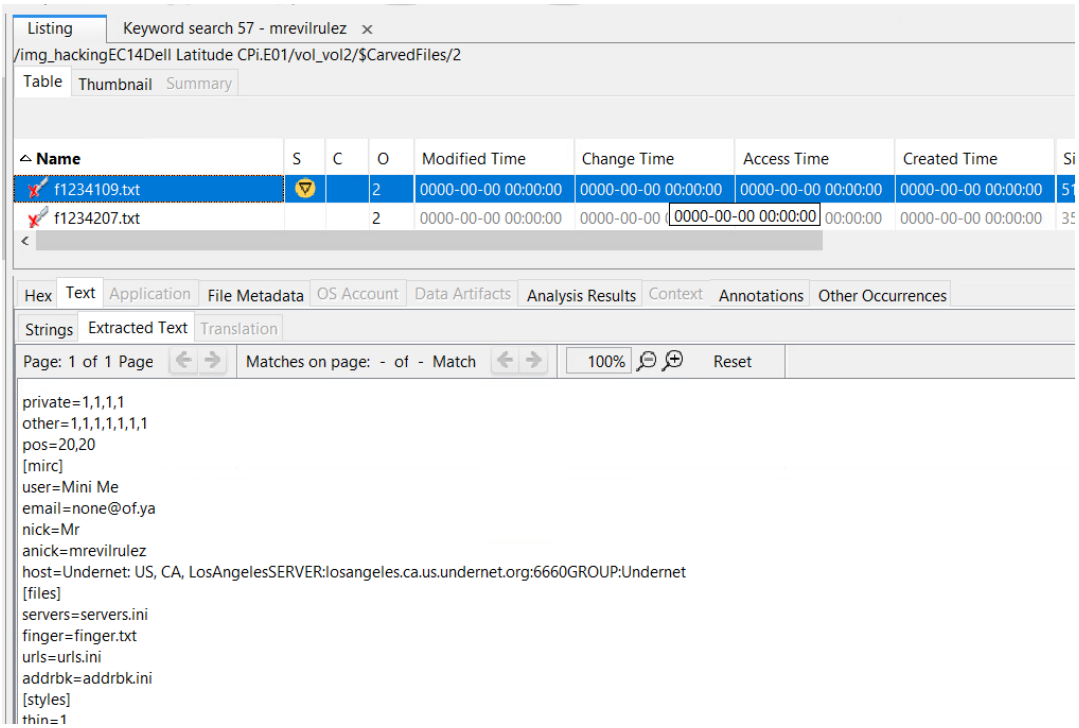
- **Path:** /img_hackingdd1SCHARDT.001/vol_vol2/Unalloc_39722_32256_1073774080



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

Answer: The user named "**Mini Me**" whose email ID is **none@of.ya** and his anic is "**mrevilrulez**" and nick is "**Mr.**" is using the mIRC app has the following account settings:

- **Thin borders:** The thin=1 setting indicates that the chat window borders would have been thin.
- **Font:** While the specific font isn't explicitly mentioned, font=1 suggests a particular font was chosen, likely from mIRC's font selection list.
- **Hidden toolbar:** hide=1 implies the main mIRC toolbar would have been hidden from view.
- **Default colors:** The color=default setting means the chat window would have used the default mIRC color scheme.
- **Small font size:** The size=2 setting points to a small font size being used in the chat window.
- **No buttons:** buttons=0 specifies that no buttons were displayed within the chat window interface.



➢ **Path:** /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/$CarvedFiles/2/f1234109.txt

This file, named "f1234109.txt" and found in the carved files section of the forensic image, likely contains user preferences and settings related to the mIRC application. This file is considered valuable evidence because it reveals how the user configured their IRC client. This information can provide insights into their online behavior, communication preferences, and potential network connections.

22. This IRC program has the capability to log chat sessions. List 3 IRC channels that the user of this computer accessed.

Answer: The 3 chat sessions that the user has accessed are:

i. Houston.UnderNet.log
ii. CyberCafe.UnderNet.log
iii. ISO-WAREZ.EFnet.log

- **Path**:/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/$CarvedFiles/2/f1234109.txt

This evidence is extracted from the log file of the **mIRC** program file.

23. Ethereal, a popular "sniffing" program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data?

Answer: The name of the file that contains the intercepted data is **"interception"**. This file is located: **/img_hackingEC14Dell Latitude**

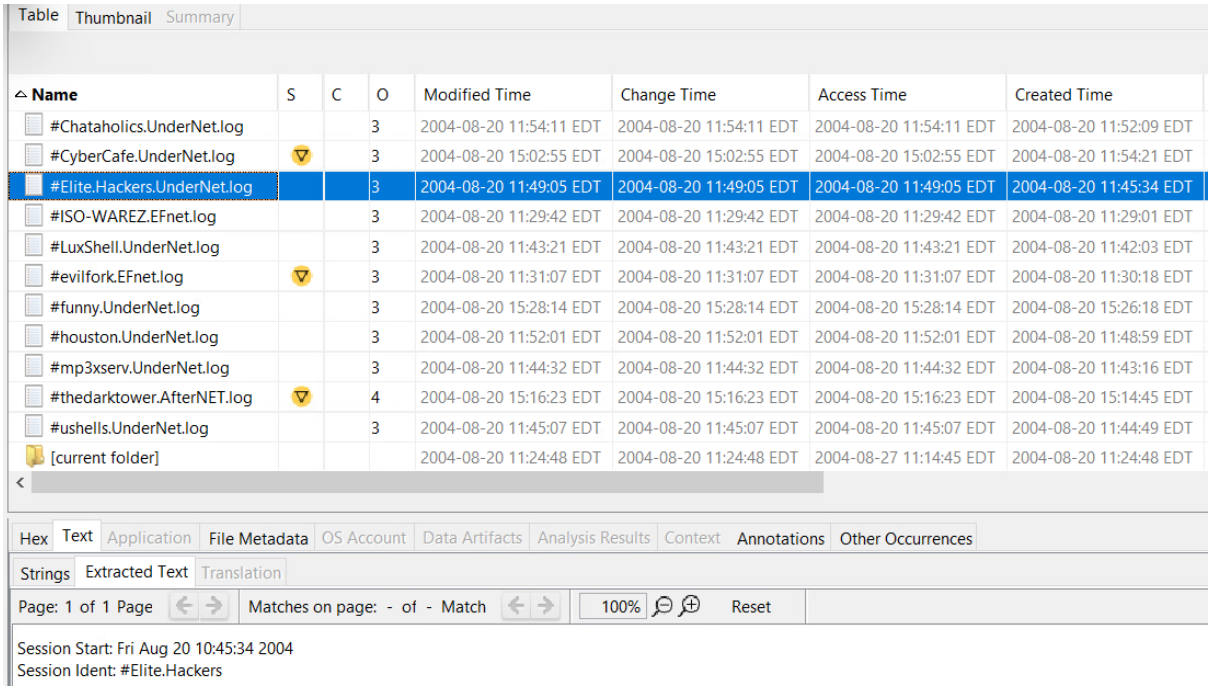


Table | Thumbnail | Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
#Chataholics.UnderNet.log			3	2004-08-20 11:54:11 EDT	2004-08-20 11:54:11 EDT	2004-08-20 11:54:11 EDT	2004-08-20 11:52:09 EDT
#CyberCafe.UnderNet.log			3	2004-08-20 15:02:55 EDT	2004-08-20 15:02:55 EDT	2004-08-20 15:02:55 EDT	2004-08-20 11:54:21 EDT
#Elite.Hackers.UnderNet.log			3	2004-08-20 11:49:05 EDT	2004-08-20 11:49:05 EDT	2004-08-20 11:49:05 EDT	2004-08-20 11:45:34 EDT
#ISO-WAREZ.EFnet.log			3	2004-08-20 11:29:42 EDT	2004-08-20 11:29:42 EDT	2004-08-20 11:29:42 EDT	2004-08-20 11:29:01 EDT
#LuxShell.UnderNet.log			3	2004-08-20 11:43:21 EDT	2004-08-20 11:43:21 EDT	2004-08-20 11:43:21 EDT	2004-08-20 11:42:03 EDT
#evilfork.EFnet.log			3	2004-08-20 11:31:07 EDT	2004-08-20 11:31:07 EDT	2004-08-20 11:31:07 EDT	2004-08-20 11:30:18 EDT
#funny.UnderNet.log			3	2004-08-20 15:28:14 EDT	2004-08-20 15:28:14 EDT	2004-08-20 15:28:14 EDT	2004-08-20 15:26:18 EDT
#houston.UnderNet.log			3	2004-08-20 11:52:01 EDT	2004-08-20 11:52:01 EDT	2004-08-20 11:52:01 EDT	2004-08-20 11:48:59 EDT
#mp3xserv.UnderNet.log			3	2004-08-20 11:44:32 EDT	2004-08-20 11:44:32 EDT	2004-08-20 11:44:32 EDT	2004-08-20 11:43:16 EDT
#thedarktower.AfterNET.log			4	2004-08-20 15:16:23 EDT	2004-08-20 15:16:23 EDT	2004-08-20 15:16:23 EDT	2004-08-20 15:14:45 EDT
#ushells.UnderNet.log			3	2004-08-20 11:45:07 EDT	2004-08-20 11:45:07 EDT	2004-08-20 11:45:07 EDT	2004-08-20 11:44:49 EDT
[current folder]				2004-08-20 11:24:48 EDT	2004-08-20 11:24:48 EDT	2004-08-27 11:14:45 EDT	2004-08-20 11:24:48 EDT

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

Strings | Extracted Text | Translation

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

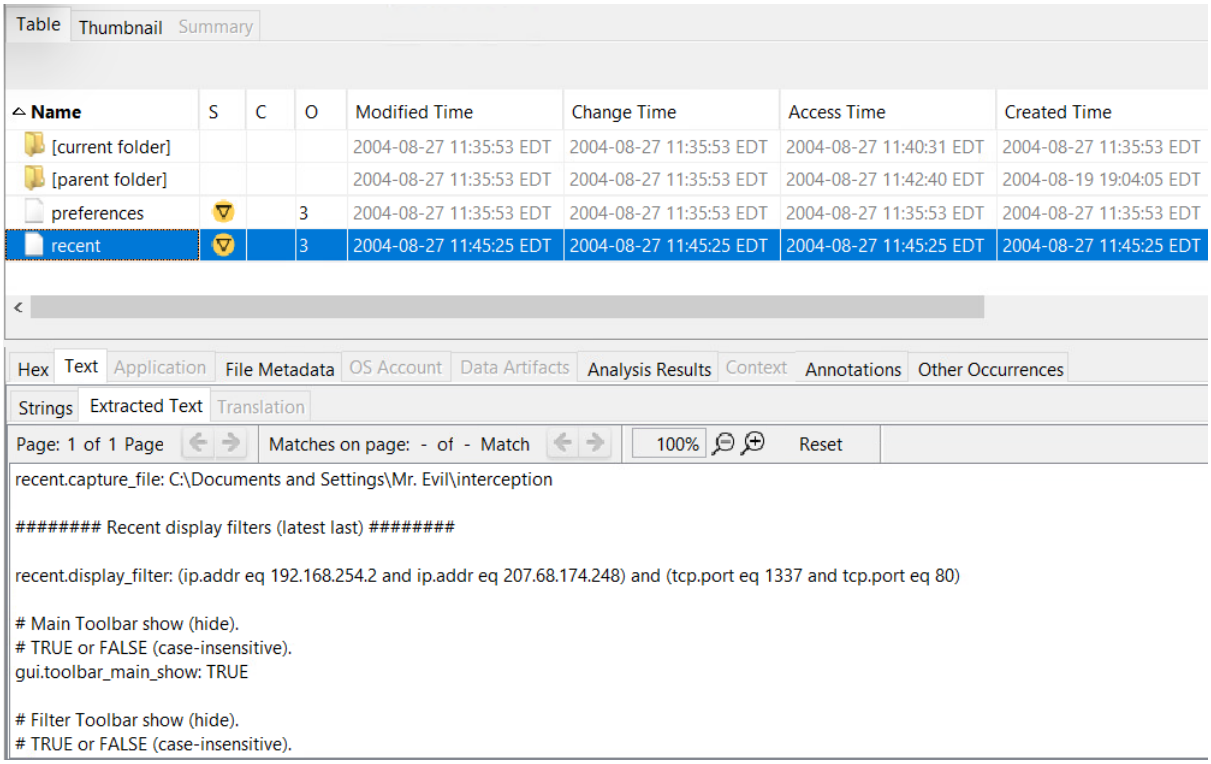
Session Start: Fri Aug 20 10:45:34 2004
Session Ident: #Elite.Hackers

CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Application Data/Ethereal/recent

This is based on the Ethereal configuration file, where the line **recent.capture_file: C:\Documents and Settings\Mr. Evil\interception** indicates the last capture file used. Ethereal, by default, saves captured packet data in the user's "My Documents" directory, and this configuration shows that the user chose the filename "interception" for their capture.

Why this file is considered evidence: This file is significant because it directly contains the network traffic intercepted by Ethereal. Analysing the contents of this file can reveal:

- Websites visited, Login credentials (if transmitted in cleartext), Online conversations, Downloaded files, other network activity



24. Viewing the file in a text format reveals much information about who and what was intercepted. What type of wireless computer was the victim (person who had his internet surfing recorded) using?

Answer: The data captured in the file "**interception**" indicates that the victim was using a **Pocket PC** running **Windows CE version 4.20**.

- **Path:** /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/interception

This information is found within the UA-OS (User-Agent Operating System) field of the HTTP requests:

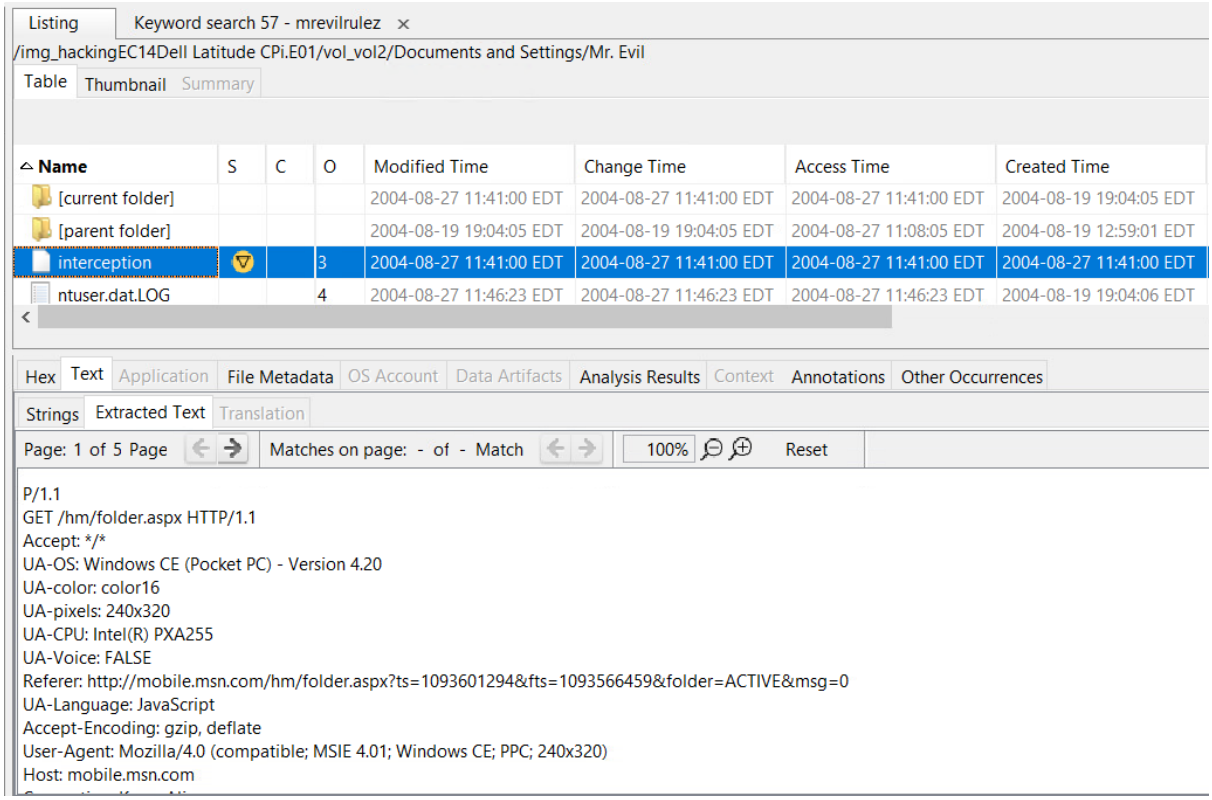
UA-OS: Windows CE (Pocket PC) - Version 4.20

The User-Agent string also tells us they were using **Internet Explorer 4.01** on this device:

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

25. What websites was the victim accessing?

Answer: As per the evidence from the "**intersection**" file, the victim was accessing the following website:



- **mobile.msn.com**

This is evident from the Host header in the HTTP requests. The specific pages or resources accessed within this website include:

- **/hm/folder.aspx** (likely the Hotmail inbox or folder view)
- **/hm/composeppc.aspx** (the page for composing a new email)
- **/content/images/img_ppc_sharkfin_MSNLogo.gif** (an image file, probably the MSN logo)

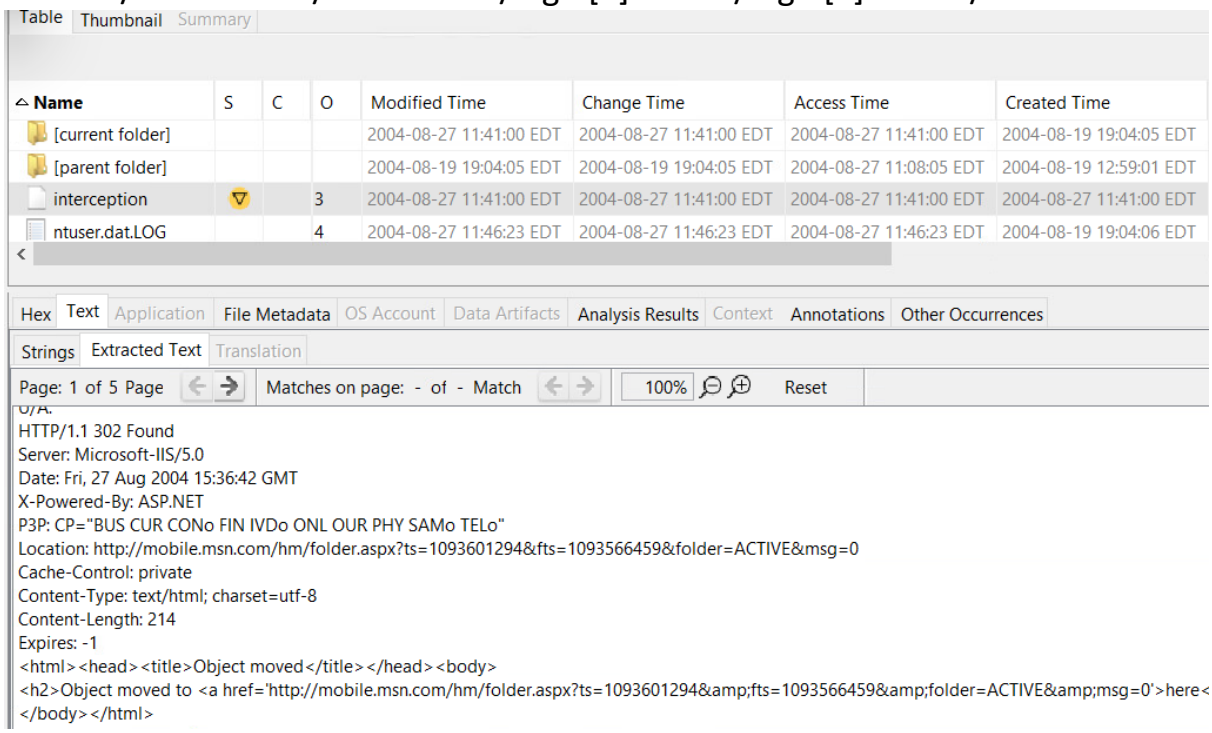
It's important to note that the data also shows interactions with:

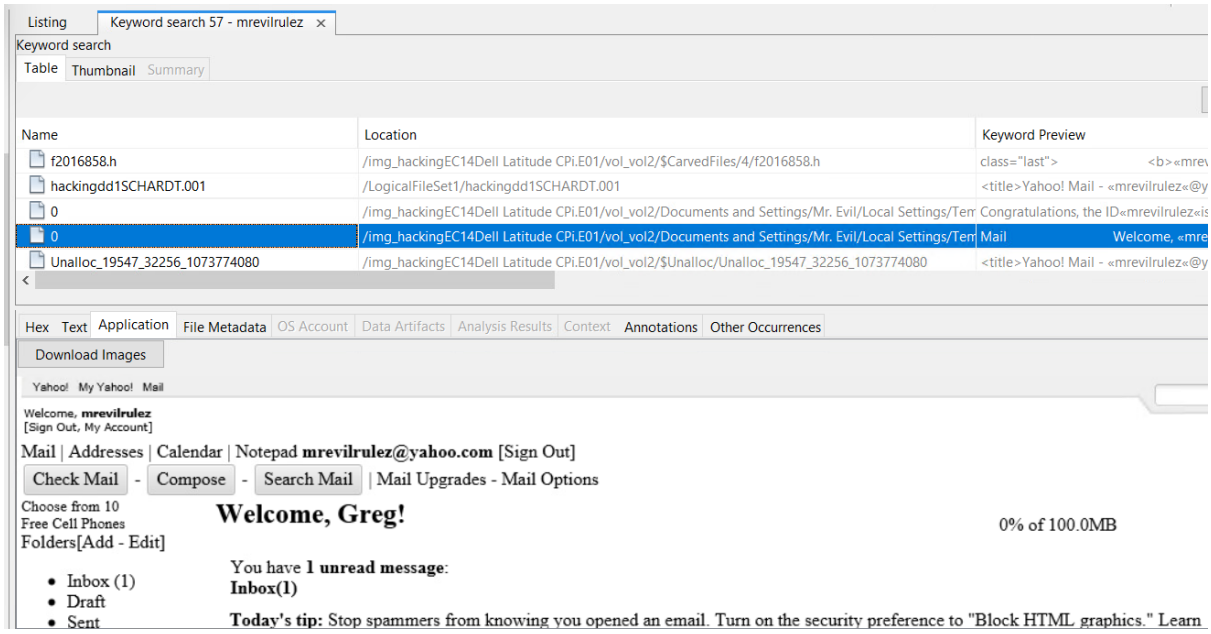
- **login.passport.com** (for authentication/logout purposes)
- **www.passportimages.com** (to load images related to the login/logout process)
- **239.255.255.250 and 192.168.254.254** (these are likely local network addresses, not external websites)

26. Search for the main users' web-based email address. What is it?

Answer: According to the analysis till now, it is observed that Greg is the main user of the computer and while investigating the User account directory, this web-based activity was found in the "**Temporary Internet Files"** folder.

➢ **Path:** /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BON0/login[1].first=1/login[1].first=1/0

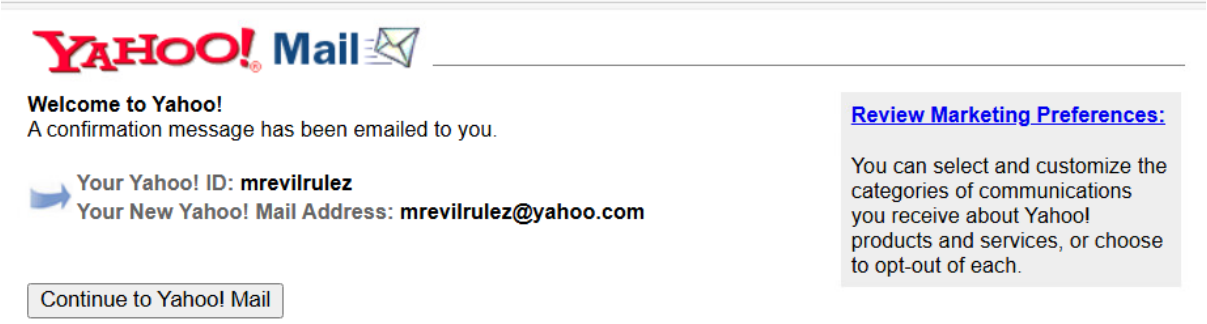




27. Yahoo mail, a popular web-based email service, saves copies of the email under what file name?

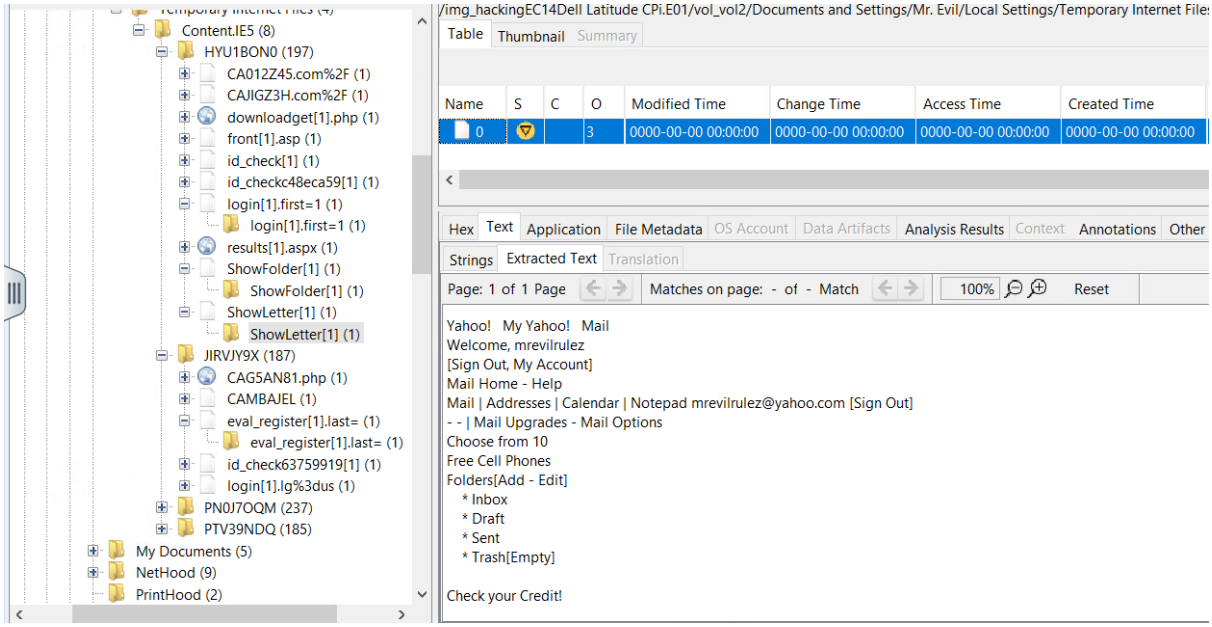
Answer: The yahoo mail stores the email copies in the "**showletter**" folder under the user file "**0**".

- **Path**: Location /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Local



Settings/Temporary Internet Files/Content.IE5/HYU1BON0/ShowLetter[1]/ShowLetter[1]/0

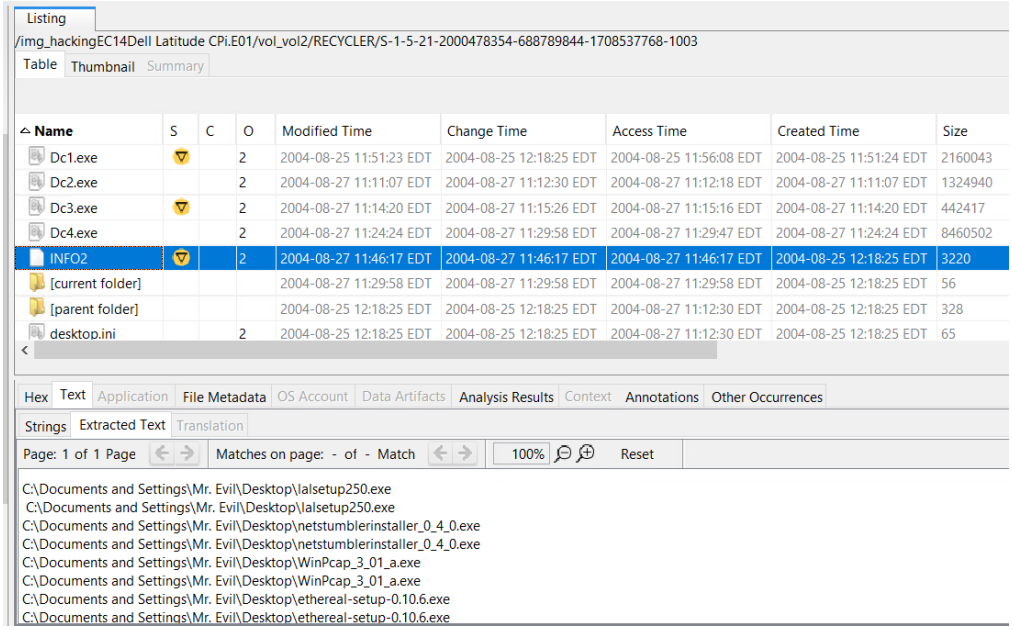
- **ShowLetter:** This specifically refers to the action of displaying or viewing an individual email message. The filename **ShowLetter[1]** likely represents the HTML content or rendered version of an email that the user has opened or is currently viewing. Analysing ShowLetter files can reveal the content of specific emails that the user has accessed, including the sender, recipient, subject, body, and any attachments.



28. How many executable files are in the recycle bin?

Answer: There are 4 executable files deleted from the system named "**Dc1.exe, Dc2.exe, Dc3.exe and Dc4.exe.**" These deleted files can be found in the "**RECYCLER**" directory. There is also a folder named "INFO2" which contains 8 more executable files.

- **Path:** /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003/Dc1.exe

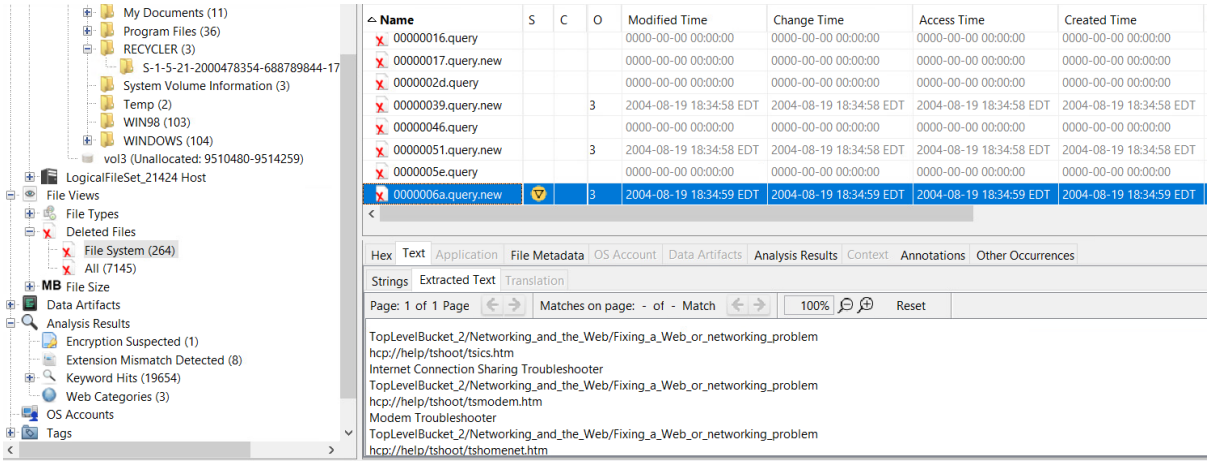


29. . Are these files really deleted?

Answer: There are 264 deleted files from the file system.

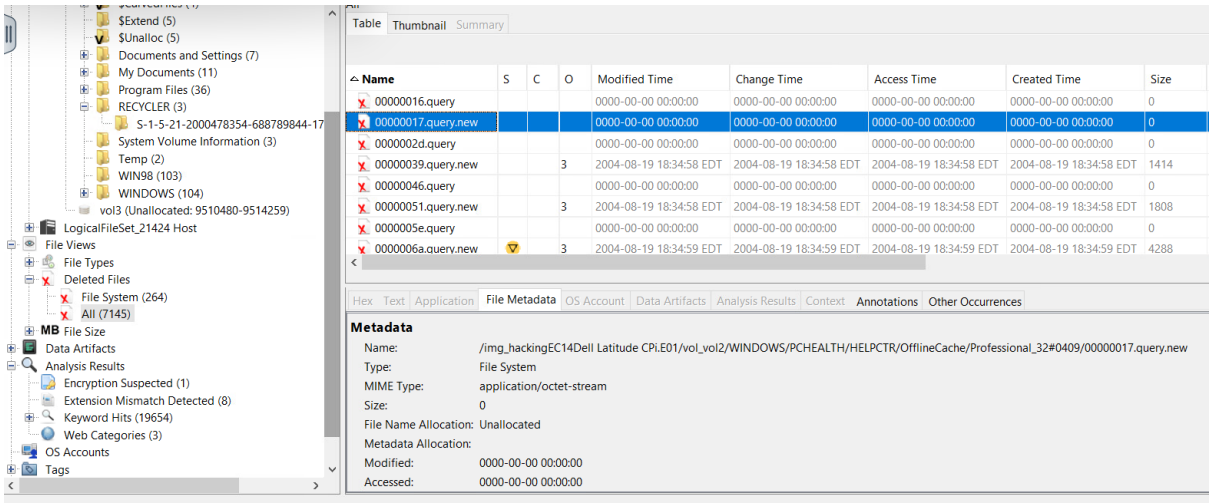
- **Path:** /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/PCHEALTH/HELPCTR/OfflineCache/Professional_32#0409/00000016.query

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



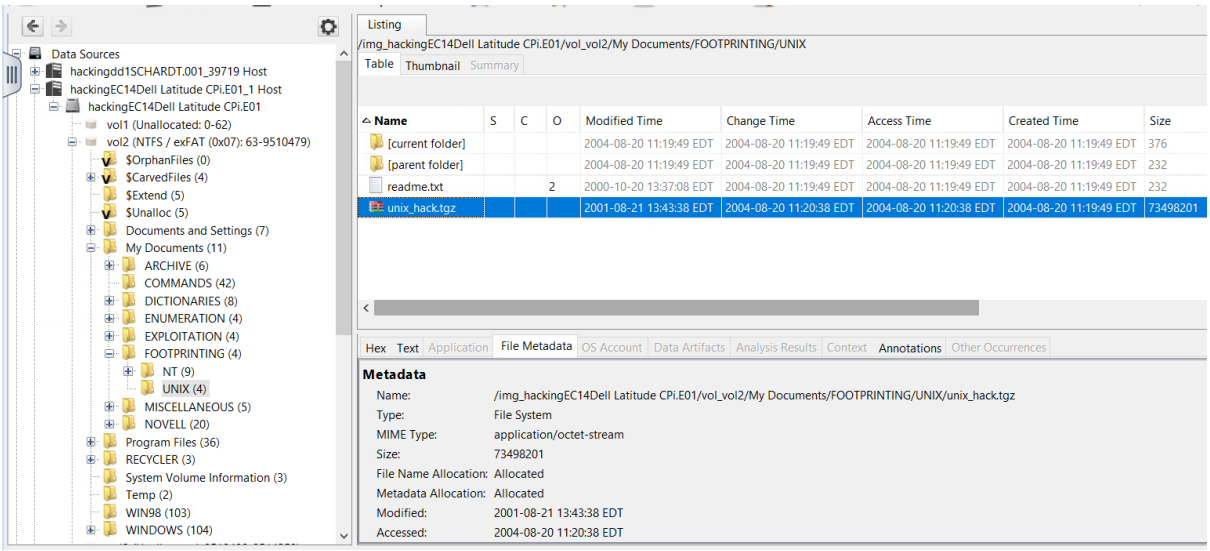
Answer: There are 7145 files reported to be deleted from the system.

- **Path:** img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/PCHEALTH/HELPCTR/OfflineCache/Professional_32#0409/00000016.query



31. Perform an Anti-Virus check. Are there any viruses on the computer?

Answer: Yes, there is a virus on the computer. Autopsy autoruns antivirus scans and any possible actors can be found inside "/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/My Documents/FOOTPRINTING/UNIX/unix_hack.tgz"



This is the specific directory named “FOOTPRINTING” within "My Documents" suggests that this folder might contain information gathered during the footprinting phase of a hacking attempt.

Footprinting, in the context of hacking, refers to the process of gathering information about a target system or network. This information can include:

- **Network topology:** Identifying the network layout, devices, and their IP addresses.
- **Open ports and services:** Discovering open ports and the services running on them.
- **Vulnerabilities:** Finding potential weaknesses in the system or network that could be exploited.
- **User accounts and information:** Gathering information about users, their roles, and potential passwords.