ESCUELA COLOMBIANA DE INGENIERIA
JULIO GARAVITO

IT SECURITY AND PRIVACY
GROUP 1L

LABORATORY 16

SUBMITTED BY:
JUAN PABLO FERNANDEZ GONZALES
MARIA VALENTINA TORRES MONSALVE

SUBMITTED TO:
Eng. DANIEL ESTEBAN VELA LOPEZ

BOGOTÁ D.C.
DATE:
19/05/2025

Introduction

This lab is focused on the analysis of an alleged hacking case related to a Dell CPi laptop, which was found abandoned along with a PCMCIA wireless card and a homemade external antenna compatible with the 802.11b standard. The objective of the investigation is to discover digital artifacts that evidence malicious activities and establish a possible relationship with a suspect identified with the alias "Mr. Evil".

The investigative process begins with the verification of the integrity of the forensic images obtained from the equipment, ensuring that the hash values coincide between the acquisition and verification processes. Subsequently, the operating environment of the system, including the installed software, user accounts, and network configuration, is examined in order to reconstruct the suspect's possible actions.

Special attention is paid to the identification of tools used for hacking, intercepted communications and traces of unauthorized access to networks. Key tasks include reviewing user-generated data, such as email settings, chat logs, and saved files, for the purpose of finding evidence that reveals malicious intent.

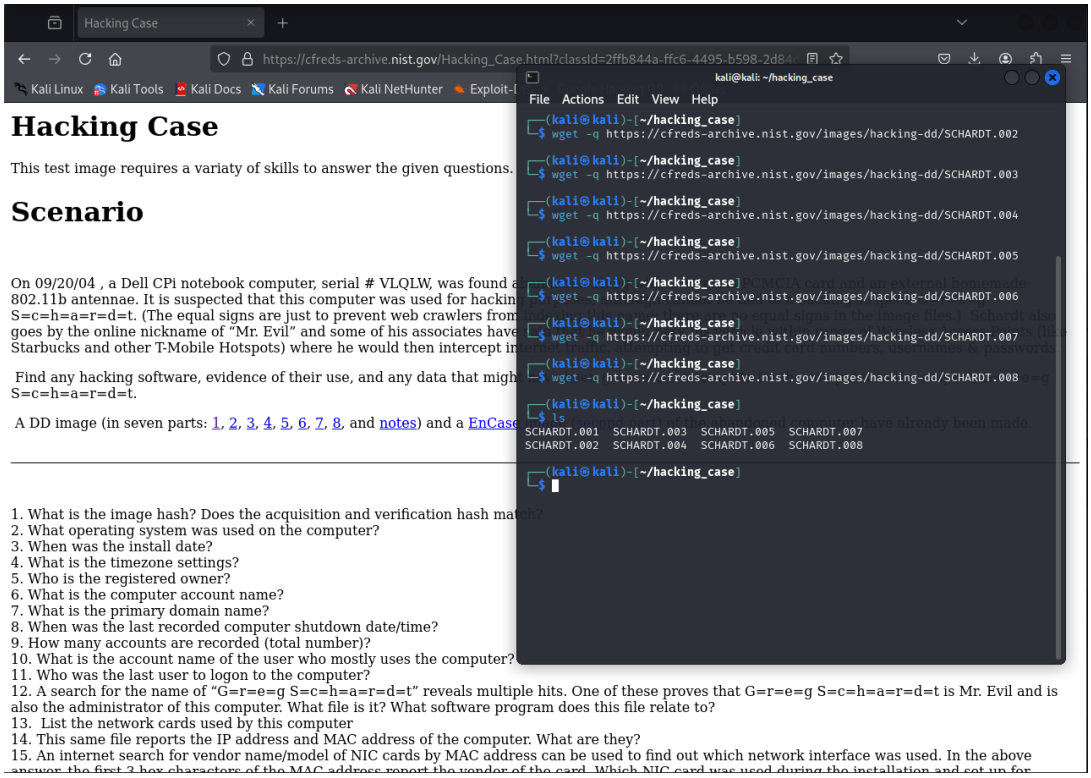
Investigators are also examining the existence of software for network snooping (sniffing) and analyzing the recovered logs to identify intercepted packets and the activity of potential victims. Throughout the investigation, forensic techniques are employed to recover deleted files, analyze metadata, and detect the presence of malware or viruses on the system.

This analysis combines a comprehensive set of forensic methodologies to collect evidence, establish a timeline of events, and link the suspect's actions to the incident under investigation. The results provide a clear view of system misuse and support strong findings in line with best forensic practices.

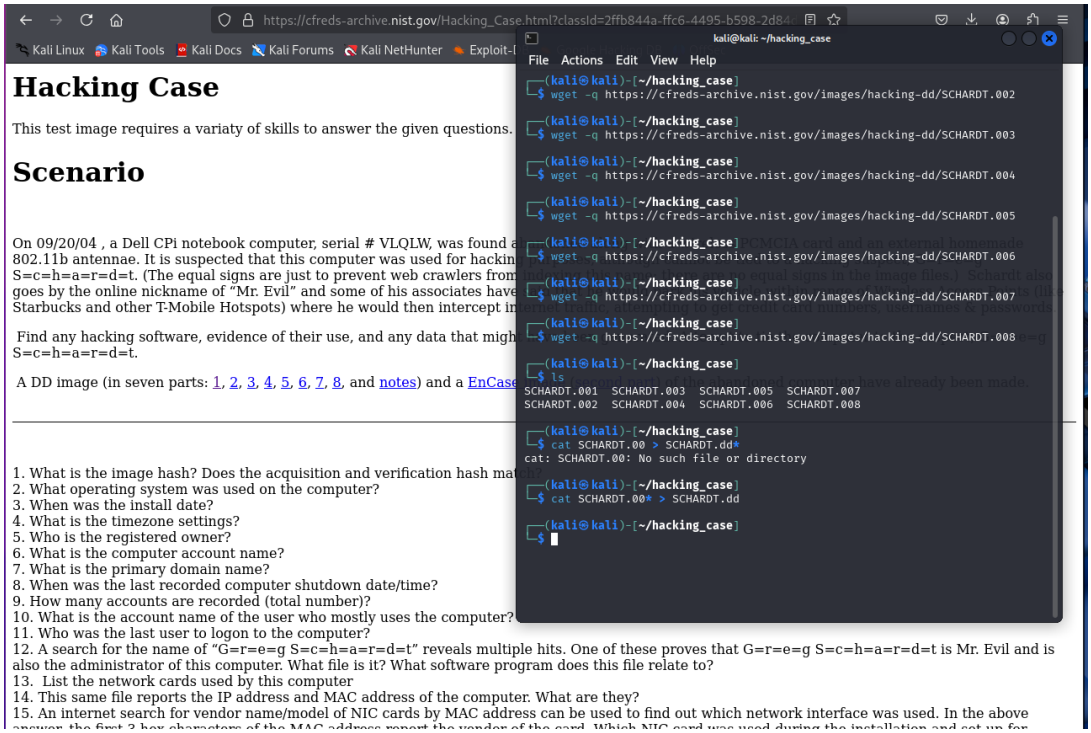
Development

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

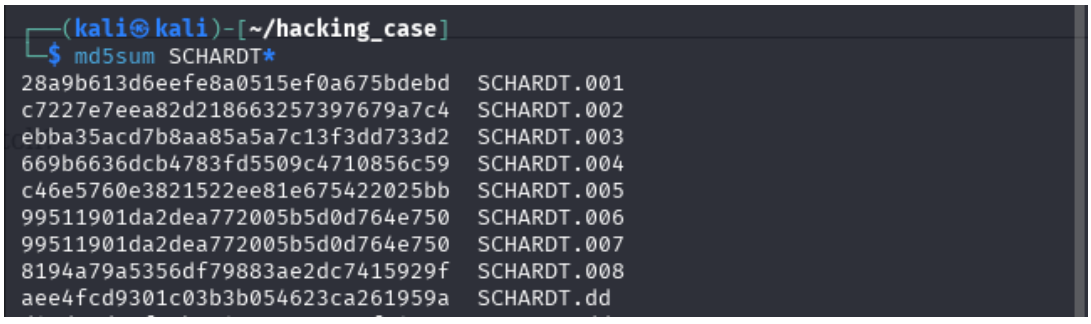
   The first thing we will do is download the images with the ***wget -q command https://cfreds-archive.nist.gov/images/hacking-dd/SCHARDT.00**** executed from the folder we created for this lab with the ***mkdir hacking_case command.***



With the ***cat command SCHARDT.00* > SCHARDT.dd*** we will be mixing all the images into a single file, since this command concatenates all the files whose name begins with ***SCHARDT.00*** (such as ***SCHARDT.001***, ***SCHARDT.002***, etc.) and redirects the combined content to a new file called ***SCHARDT.dd***. This procedure is commonly used to reconstruct a large file that was previously divided into smaller parts.



We'll be checking the hashes of the images with the ***md5sum SCHARDT* command***, which calculates and displays the MD5 hash value of each file whose name begins with ***SCHARDT***. This value is a unique signature generated from the contents of the file, and is used to verify its integrity. If we compare the generated hashes with the originals and they match, it means that the files have not been altered or damaged during the transfer or rebuild process.



We can see that the acquisition and verification hashes match.

2. What operating system was used on the computer?

With the ***mmls SCHARDT.dd*** command we can see the layout and layout of the image partition. Performing this shows that one of the main partitions (Slot 002) has a boot sector of 63 and is labeled with the file system type NTFS/exFAT (0x07).

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ mmls SCHARDT.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  ------    0000000000   0000000062   0000000063   Unallocated
002:  000:000   0000000063   0009510479   0009510417   NTFS / exFAT (0x07)
003:  ------    0009510480   0009514259   0000003780   Unallocated

┌──(kali㉿kali)-[~/hacking_case]
└─$
```

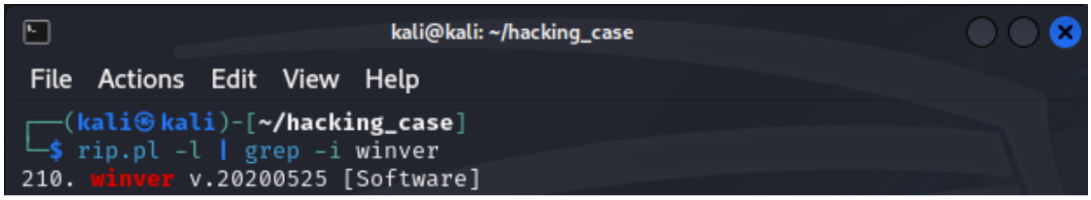
The ***fls -rF -o 63 SCHARDT.dd | grep -i software*** command is used to list paths or names of files and directories that contain the word "software" in the previously identified sector, in this case sector 63 of the ***SCHARDT.dd*** file. The ***fls*** (File List) tool in the Sleuth Kit package allows you to examine the contents of a file system from a specific sector. The ***-r*** option performs a recursive search, ***-F*** displays the full name of the files, and ***-o 63*** indicates the offset in sectors where the file system starts.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | grep -i software
r/r 9895-128-4: Program Files/Anonymizer/Toolbar/Images/software-A.bmp
r/r 9896-128-4: Program Files/Anonymizer/Toolbar/Images/software-D.bmp
r/r 9897-128-4: Program Files/Anonymizer/Toolbar/Images/software-M.bmp
r/r 6375-128-5: WINDOWS/PCHEALTH/HELPCTR/System/sysinfo/sysSoftwareInfo.htm
r/r 6376-128-5: WINDOWS/PCHEALTH/HELPCTR/System/sysinfo/sysSoftwareInfo.js
r/r 9742-128-4: WINDOWS/repair/software
r/r 336-128-4:  WINDOWS/system32/config/software
r/r 466-128-5:  WINDOWS/system32/config/software.LOG
r/r 471-128-3:  WINDOWS/system32/config/software.sav
```


We will extract the contents of the file identified above in the forensic image with the ***command icat -o 63 SCHARDT.dd 336 > software***. This saves the extracted file on our machine with the name ***software***, allowing its subsequent analysis. The command indicates that the file system starts in sector 63 and retrieves the file with inode 336 from the ***SCHARDT.dd image***.

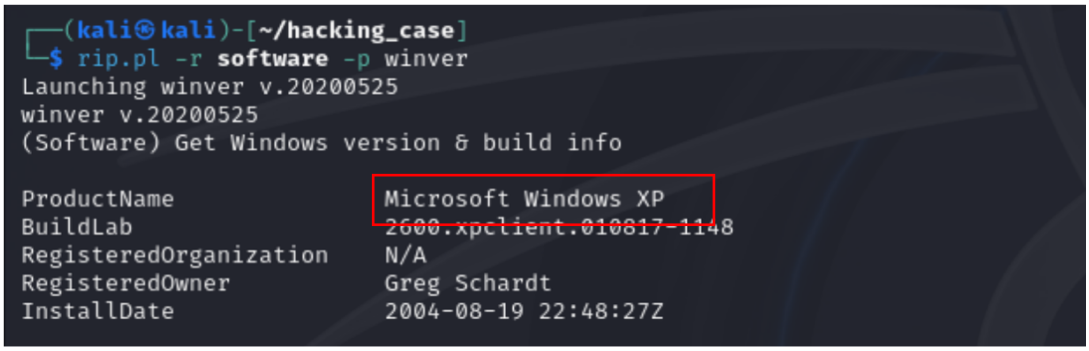
```
┌──(kali㉿kali)-[~/hacking_case]
└─$ icat -o 63 SCHARDT.dd 336 > software

┌──(kali㉿kali)-[~/hacking_case]
└─$ ls
SCHARDT.001  SCHARDT.004  SCHARDT.007  'SCHARDT.dd*'
SCHARDT.002  SCHARDT.005  SCHARDT.008   software
SCHARDT.003  SCHARDT.006  SCHARDT.dd
```

The command ***rip.pl -l | grep -i winver*** is used to list all plugins available in RegRipper and filter only those that contain the word "winver". Here, ***rip.pl -l*** shows the full list of plugins that RegRipper can use to analyze Windows registry files, while ***grep -i winver*** insensitively searches for plugins whose name includes "winver".



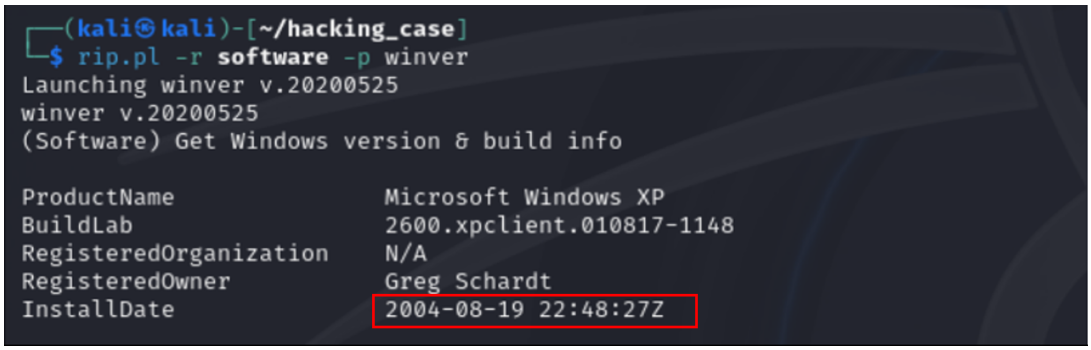
It is noted that the winver plugin is available and correctly located in the RegRipper plugin directory.

With the ***command rip.pl -r software -p winver*** we analyze the software log file using the ***winver plugin***, which extracts information about the Windows version and we can notice that the operating system is Windows XP.



3. When was the install date?

Using the same command used above, it verifies that the installation date is August 19, 2004 at 05:48:27 pm.



4. What is the timezone settings?

The ***fls -rF -o 63 SCHARDT.dd | egrep -i config/system$*** command is used to search for specific files within the ***SCHARDT.dd*** forensic image. The ***fls*** tool lists files and directories in the file system located from sector 63 (option ***-or 63***). The ***-r*** option performs a recursive search and ***-F*** shows complete paths. Then, with ***egrep -i config/system$*** the results are filtered to show only those whose name ends exactly in "config/system". You can see that in inode 334 is the log file system.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | egrep -i config/system$
r/r 334-128-4:  WINDOWS/system32/config/system

┌──(kali㉿kali)-[~/hacking_case]
└─$
```

The contents of the file identified above are saved in a new file called ***system*** on the host system, and a summary of the system's time zone settings is displayed. It is noted that the configured time zone corresponds to Central Daylight Time (GMT -05), which alternates between Central Standard Time (CST) with a deviation of -6 hours from UTC and Central Summer Time (CDT) with a deviation of -5 hours during daylight saving time.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ icat -o 63 SCHARDT.dd 334 > system


┌──(kali㉿kali)-[~/hacking_case]
└─$ rip.pl -r system  -p timezone

Launching timezone v.20200518
timezone v.20200518
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time 2004-08-19 17:20:02Z
  DaylightName    → Central Daylight Time
  StandardName    → Central Standard Time
  Bias            → 360 (6 hours)
  ActiveTimeBias  → 300 (5 hours)
```


5. Who is the registered owner?

   Using the same command mentioned above, ***rip.pl -r software -p winver***, the registered owner of the system is verified to be **Greg Schardt**.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ rip.pl -r software -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName              Microsoft Windows XP
BuildLab                 2600.xpclient.010817-1148
RegisteredOrganization   N/A
RegisteredOwner          Greg Schardt
InstallDate              2004-08-19 22:48:27Z
```

6. What is the computer account name?

   With the system file previously identified, the ***compname*** plugin is used using the ***command rip.pl -r software -p compname*** to verify the name of the computer account. You get the name of the computer being **N-1A9ODN6ZXK4LQ.**

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ rip.pl -r system  -p compname

Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = N-1A9ODN6ZXK4LQ
TCP/IP Hostname = n-1a9odn6zxk4lq
```


7. What is the primary domain name?

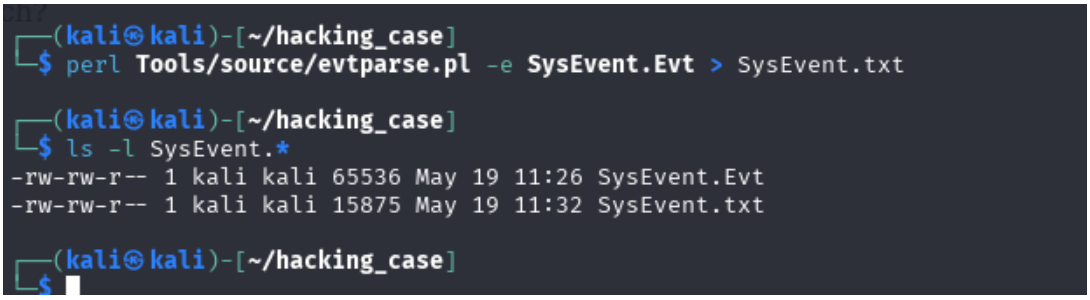
   The process performed earlier is repeated, this time with the goal of locating and analyzing the system event log file. To do this, the ***icat -o 63 SCHARDT.dd 3678 command > SysEvent.Evt*** is used, which extracts the ***SysEvent.Evt*** file from the ***SCHARDT.dd*** forensic image, starting with sector 63, and saves it on the host system. The file is then verified to have been created correctly with the ***ls -l SysEvent.Evt*** command, which displays the details of the file, such as size and date modified.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | egrep -i config/system$
r/r 334-128-4:  WINDOWS/system32/config/system

┌──(kali㉿kali)-[~/hacking_case]
└─$ icat -o 63 SCHARDT.dd 3678 > SysEvent.Evt

┌──(kali㉿kali)-[~/hacking_case]
└─$ ls /j SysEvent.Evt
ls: cannot access '/j': No such file or directory
SysEvent.Evt

┌──(kali㉿kali)-[~/hacking_case]
└─$ ls -l  SysEvent.Evt
-rw-rw-r-- 1 kali kali 65536 May 19 11:26 SysEvent.Evt
```

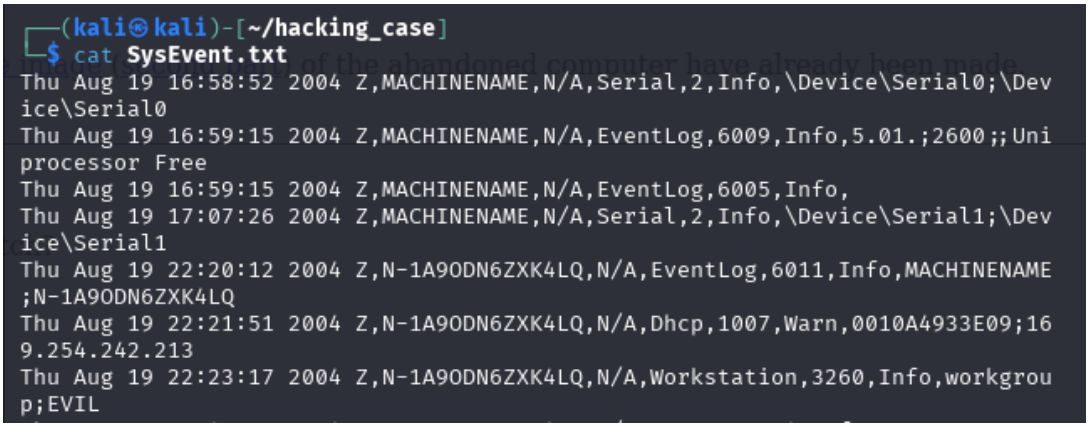
The evtparse ***tool is installed*** with the ***git clone*** [***https://github.com/keydet89/Tools.git***](https://github.com/keydet89/Tools.git) command , which is a script designed to process Windows event files (.evt). Once installed, a test is performed to verify that the evtparse.pl script works properly in the environment, ensuring that it can read and convert event logs into an understandable format.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ ls /j SysEvent.Evt
ls: cannot access '/j': No such file or directory
SysEvent.Evt

┌──(kali㉿kali)-[~/hacking_case]
└─$ ls -l  SysEvent.Evt
-rw-rw-r-- 1 kali kali 65536 May 19 11:26 SysEvent.Evt

┌──(kali㉿kali)-[~/hacking_case]
└─$ git clone https://github.com/keydet89/Tools.git.
Cloning into 'Tools.git.'...
Username for 'https://github.com': Mar972310
Password for 'https://Mar972310@github.com':
remote: Support for password authentication was removed on August 13, 2021.
remote: Please see https://docs.github.com/get-started/getting-started-with-g
it/about-remote-repositories#cloning-with-https-urls for information on curre
ntly recommended modes of authentication.
fatal: Authentication failed for 'https://github.com/keydet89/Tools.git./'

┌──(kali㉿kali)-[~/hacking_case]
└─$ git clone https://github.com/keydet89/Tools.git
Cloning into 'Tools'...
remote: Enumerating objects: 193, done.
remote: Counting objects: 100% (27/27), done.
remote: Compressing objects: 100% (20/20), done.
remote: Total 193 (delta 13), reused 16 (delta 7), pack-reused 166 (from 1)
Receiving objects: 100% (193/193), 8.37 MiB | 7.57 MiB/s, done.
Resolving deltas: 100% (108/108), done.

┌──(kali㉿kali)-[~/hacking_case]
└─$
```

Using the ***evtparse.pl*** script, the Windows event log file called ***SysEvent.Evt*** is processed. To do this, run the ***perl command Tools/source/evtparse.pl -e SysEvent.Evt > SysEvent.txt***, which converts the file to a readable text format. The result is saved in a new file called ***SysEvent.txt***, which allows you to review in detail the information contained in the events, such as identifiers, dates, system actions, and users involved.



The contents of the SysEvent.txt file are examined to analyze the extracted information. When reviewing the logged events, it is identified that the name of the primary domain configured in the system is ***"EVIL".*** This type of information is relevant in a security lab, as it can indicate the environment or network to which the analyzed system belonged.



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

With the system file previously identified, the shutdown snap-in is used to obtain information about the last shutdown of the computer. To do this, the command ***rip.pl -r software -p shutdown*** is executed. It is noted that the last recorded shutdown date was **August 27, 2004 at 10:46:33 a.m.**, which can be relevant in a forensic analysis to establish timelines of use of the system.

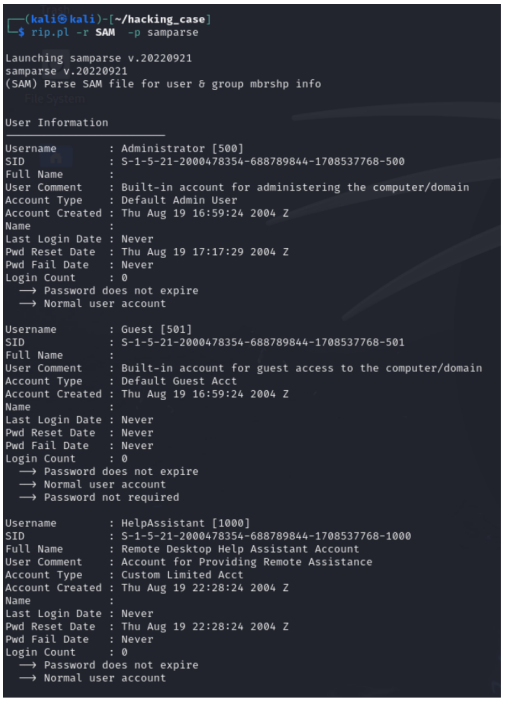
```
┌──(kali㉿kali)-[~/hacking_case]
└─$ rip.pl -r system  -p shutdown

Launching shutdown v.20200518
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2004-08-27 15:46:33Z
ShutdownTime  : 2004-08-27 15:46:33Z
```

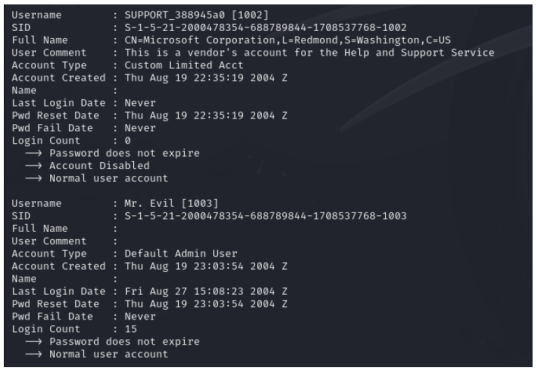
9. How many accounts are recorded (total number)?

The process performed previously is repeated, this time with the aim of locating the Windows account log file known as ***SAM***. To do this, the fls ***-rF -o 63 SCHARDT.dd | egrep -i config/sam command is used***, which allows the file to be located within the forensic image. Then, with the ***icat -o 63 SCHARDT.dd 3667 command > SAM***, the file is extracted and saved to the host system.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | egrep -i config/sam
r/r 3667-128-4: WINDOWS/system32/config/SAM
r/r 3668-128-4: WINDOWS/system32/config/SAM.LOG

┌──(kali㉿kali)-[~/hacking_case]
└─$ icat -o 63 SCHARDT.dd 3667 > SAM

┌──(kali㉿kali)-[~/hacking_case]
└─$
```


Once extracted, the contents of the SAM file are parsed using the ***samparse plug-in*** using the command ***rip.pl -r SAM -p samparse***. The goal is to check the number of accounts registered in the system. As a result of the analysis, it is observed that there are **5 accounts registered**, which can provide valuable information in the context of a forensic investigation.

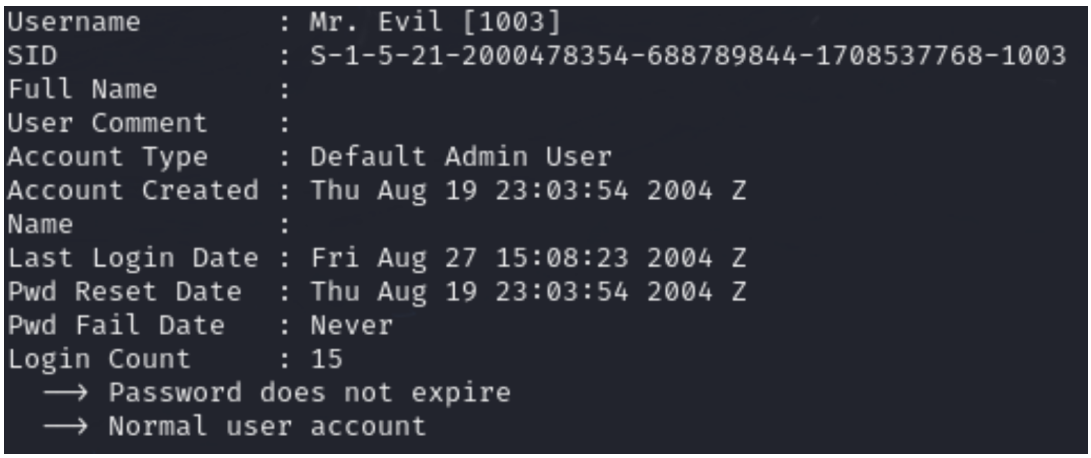




10. What is the account name of the user who mostly uses the computer?

Using the same command previously applied to scan the ***SAM*** file, i.e. ***rip.pl -r SAM -p to be sampled***, not only the number of accounts registered in the system is checked, but also the frequency with which each one has logged in. From the result, it is identified that the account with the highest number of accesses is that of **"Mr Evil",** which has **15 registered logins**.

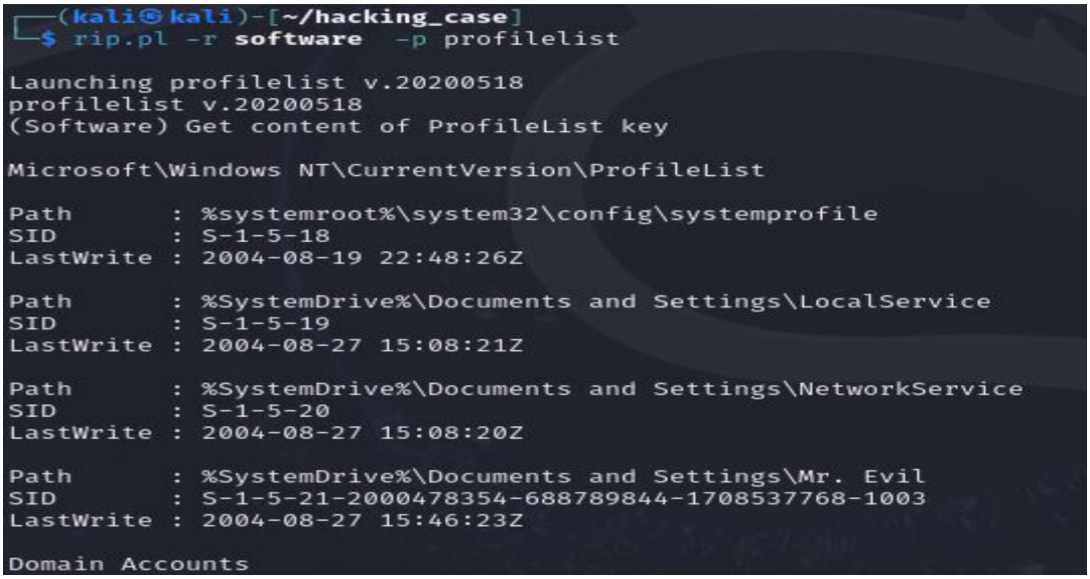
This data is especially relevant since it allows us to infer which account has had the most activity in the system.



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

    With the previously extracted ***software file, the*** profilelist ***plug-in is used*** via the command ***rip.pl -r software -p profilelist*** to obtain detailed information about the user profiles registered in the system. This analysis allows you to identify not only which users have active profiles, but also which one was the last to log in.

    From the results obtained, it can be seen that the last user who logged in to the computer was **Mr Evil**, which can be an important clue within the forensic analysis to relate recent activities to a specific account.



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?

    First, a ***mount point*** is created and the image is associated with a ***loop device***. This operation allows the image to be treated as if it were a physical disk, making it easier to access its contents.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ mkdir /mnt/loop
mkdir: cannot create directory ‘/mnt/loop’: Permission denied

┌──(kali㉿kali)-[~/hacking_case]
└─$ sudo mkdir /mnt/loop

┌──(kali㉿kali)-[~/hacking_case]
└─$ sudo losetup --partscan --find --show --read-only SCHARDT.dd
/dev/loop0

┌──(kali㉿kali)-[~/hacking_case]
└─$
```

Once the connection is established, the image is ***mounted at the mount point*** and the files available in its structure are displayed. This provides a detailed view of the file system that was in use at the time the image was created.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ ls -l /dev/loop0*
brw-rw---- 1 root disk   7, 0 May 19 12:11 /dev/loop0
brw-rw---- 1 root disk 259, 0 May 19 12:11 /dev/loop0p1

┌──(kali㉿kali)-[~/hacking_case]
└─$ sudo mount /dev/loop0p1 /mnt/loop
Error opening '/dev/loop0p1' read-write
Could not mount read-write, trying read-only

┌──(kali㉿kali)-[~/hacking_case]
└─$ ls /mnt/loop
 AUTOEXEC.BAT              hiberfil.sys      RECYCLER
 boot.ini                  IO.SYS            SETUPLOG.TXT
 BOOTLOG.PRV               MSDOS.---         SUHDLOG.DAT
 BOOTLOG.TXT               MSDOS.SYS         SYSTEM.1ST
 BOOTSECT.DOS             'My Documents'    'System Volume Information'
 COMMAND.COM               NETLOG.TXT        Temp
 CONFIG.SYS                ntdetect.com      VIDEOROM.BIN
 DETLOG.TXT                ntldr             WIN98
'Documents and Settings'   pagefile.sys      WINDOWS
 FRUNLOG.TXT              'Program Files'
```

A global search for the name "Greg Schardt" ***is then performed*** on the entire mounted system. As a result, two relevant files containing that name are identified. These files are then examined to find the word ***"evil",*** which allows possible aliases or indications of suspicious activity to be established.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ grep -rn '/mnt/loop/' -e 'Greg Schardt'

/mnt/loop/Program Files/Look@LAN/irunin.ini:29:%REGOWNER%=Greg Schardt
/mnt/loop/Program Files/Look@LAN/irunin.ini:396:%USERNAME%=Greg Schardt
/mnt/loop/WINDOWS/Look@LAN Setup Log.txt:42:Value data = Greg Schardt
```

Finally, a combined search for the keywords "Evil" and "Greg" ***is executed***. This action reinforces the relationship between the user's real name and their possible alternate identity or alias within the system.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ cat "/mnt/loop/Program Files/Look@LAN/irunin.ini" | grep -i "evil"
%LANUSER%=Mr. Evil
%DESKTOP%=C:\Documents and Settings\Mr. Evil\Desktop
%STARTMENU%=C:\Documents and Settings\Mr. Evil\Start Menu
%STARTMENUPROGRAMS%=C:\Documents and Settings\Mr. Evil\Start Menu\Programs
%STARTUP%=C:\Documents and Settings\Mr. Evil\Start Menu\Programs\Startup
%MYDOCUMENTSDIR%=C:\Documents and Settings\Mr. Evil\My Documents
%SRCFILE%=C:\Documents and Settings\Mr. Evil\Desktop\lalsetup250.exe
%SRCDIR%=C:\Documents and Settings\Mr. Evil\Desktop

┌──(kali㉿kali)-[~/hacking_case]
└─$ cat "/mnt/loop/Program Files/Look@LAN Setup Log.txt" | grep -i "evil"
cat: '/mnt/loop/Program Files/Look@LAN Setup Log.txt': No such file or direct
ory

┌──(kali㉿kali)-[~/hacking_case]
└─$ cat "/mnt/loop/WINDOWS/Look@LAN Setup Log.txt" | grep -i "evil"
C:\Documents and Settings\Mr. Evil\Desktop\Look@LAN.lnk
C:\Documents and Settings\Mr. Evil\Desktop\Look@Host.lnk

┌──(kali㉿kali)-[~/hacking_case]
└─$
```


Analysis of the configuration files, browsing history, and folder structure leads to the conclusion that **Greg Schardt** used the alias **"Mr. Evil."** In addition, a clear connection is observed between this user and behaviors that suggest monitoring and possible interception of network traffic. These actions are supported by specific system configurations and logs that strengthen the hypothesis of malicious activities performed by the user.

|

13. List the network cards used by this computer

With the previously identified Software file, the ***plug-in rip.pl -r software -p networkcards*** is used to obtain information about the network cards used in the analyzed computer. As a result, two installed network cards are identified: **Compaq WL110 Wireless LAN PC Card** and **Xircom CardBus Ethernet**. This information is key in a forensic analysis, as it allows us to know the network devices associated with the system and possible connections made.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ rip.pl -r software  -p networkcards

Launching networkcards v.20200518
networkcards v.20200518
(Software) Get NetworkCards Info

NetworkCards
Microsoft\Windows NT\CurrentVersion\NetworkCards

Description                                     Key LastWrite time
Compaq WL110 Wireless LAN PC Card               2004-08-27 15:31:44Z
Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface) 2004-08-19 17:07:19Z
```

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

    A search is performed in the system files to find those text strings that match the format of an IP address. To do this, commands are used to locate IP address patterns in the mounted files of the analyzed image. This action can reveal relevant network connections or assigned addresses during system use.
    egrep -rIl '\b[0-9]{1,3}\. [0-9]{1,3}\. [0-9]{1,3}\. [0-9]{1,3}\b' '/mnt/loop/' > ip.txt

    A similar search is then run to find strings that match the MAC address format. MAC addresses allow you to identify physical or virtual network interfaces that were active in the system.
    egrep -rIl '[^-/]\b[0-9a-fA-F]{12}\b' '/mnt/loop' > mac.txt

    Once the files containing IP and MAC addresses have been located, a comparison is made between them, looking for matches that can associate a specific IP address with a specific network interface.

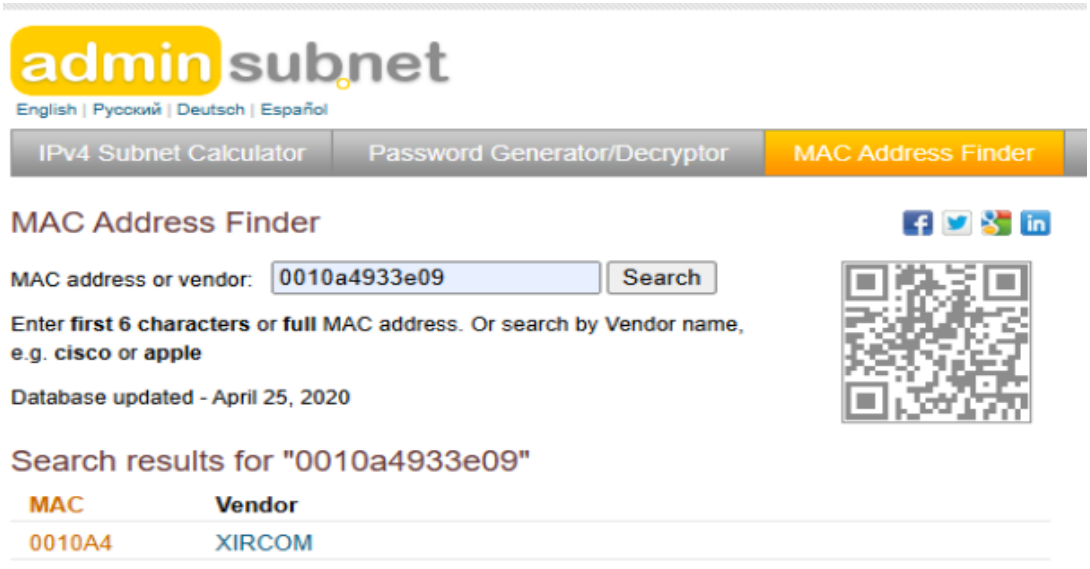
```
┌──(kali㉿kali)-[~/hacking_case]
└─$ egrep -rIl '\b[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\b'  '/mnt/lo
op/' > ip.txt


┌──(kali㉿kali)-[~/hacking_case]
└─$ egrep -rIl '[^-/]\b[0-9a-fA-F]{12}\b'   '/mnt/loop' > mac.txt


┌──(kali㉿kali)-[~/hacking_case]
└─$ comm -12 ip.txt mac.txt

comm: file 1 is not in sorted order
/mnt/loop/Program Files/Look@LAN/irunin.ini
/mnt/loop/Program Files/mIRC/channels/channels.txt
comm: file 2 is not in sorted order
comm: input is not in sorted order
```

    Finally, the identified files are explored in detail to verify and confirm the presence of IP and MAC addresses. This information can provide key evidence about the system's network configuration and its potential connections.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ grep -rP '\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b' '/mnt/loop/Program File
s/Look@LAN/irunin.ini'

%LANIP%=192.168.1.111

┌──(kali㉿kali)-[~/hacking_case]
└─$ egrep -r '[^-/]\b[0-9a-fA-F]{12}\b' '/mnt/loop/Program Files/Look@LAN/iru
nin.ini'

%LANNIC%=0010a4933e09

┌──(kali㉿kali)-[~/hacking_case]
└─$
```

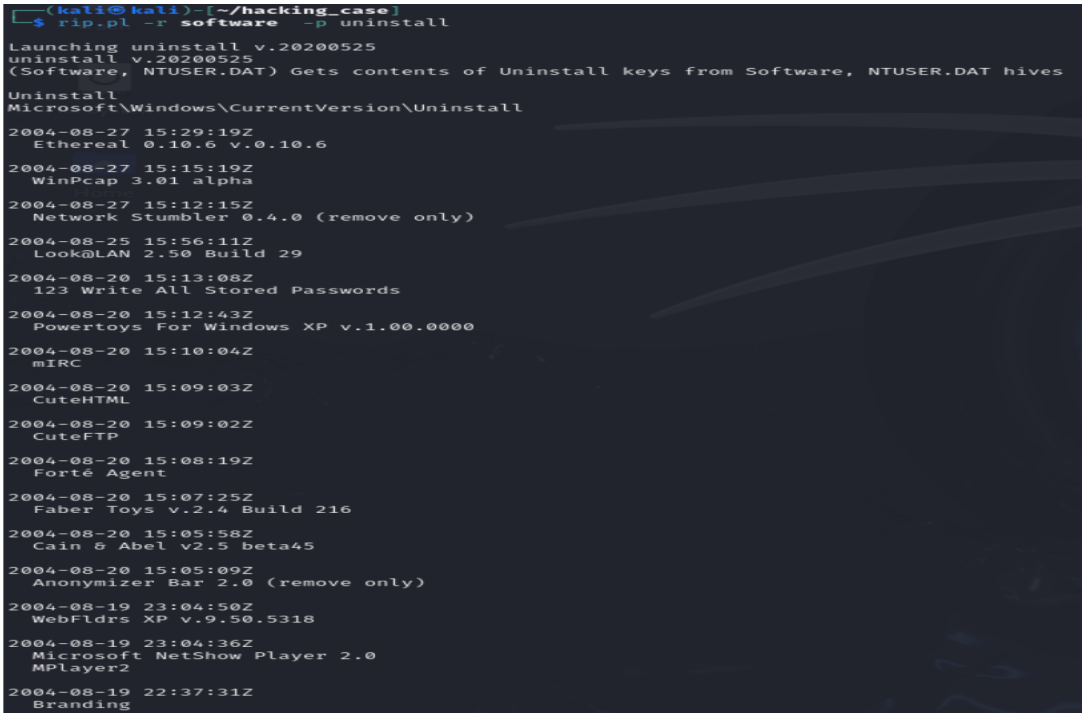
15. An internet search for vendor name/model of NIC cards by MAC address can be used to find out which network interface was used. In the above answer, the first 3 hex characters of the MAC address report the vendor of the card. Which NIC card was used during the installation and set-up for LOOK@LAN?

    Once the MAC address has been obtained through file system forensics, we will access the https://www.adminsub.net/mac-address-finder/ page to identify the manufacturer of the network adapter. When entering the MAC address found, it is observed that it belongs to the company **XIRCOM.** This information is useful in a computer security lab to link identified hardware to potential suspicious behavior or specific users within the analyzed environment.



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

With the ***previously identified software*** file, the uninstall ***add-on*** of the rip.pl command is used to list the programs installed and subsequently uninstalled on the scanned system. This information is key to determining which tools were used by the user, especially if they are related to suspicious activities or of forensic interest.



Among the detected programs are several tools commonly used in analysis or attack tasks within computer networks. For example:

- **Ethereal** is a network sniffer, used to capture packets traveling through the network. This tool allows you to interpret and analyze the captured information, which can reveal tasks that are being performed on the network.
- **Network Stumbler** is a utility for detecting wireless networks that support 802.11a/b/g standards, suggesting possible attempts to monitor or access nearby WiFi networks.
- **WinPcap** allows applications to capture raw packets directly from the network card, which is essential for the operation of sniffers like Ethereal.
- **123 Write All Stored** is a **password cracker** program, designed to crack passwords stored on the system, possibly for unauthorized access purposes.
- **Anonymizer Bar 2.0** is a toolbar that hides the user's real IP address by using proxy servers, making it difficult to track.

- **Cain and Abel** is a powerful password cracking and recovery tool, which also includes sniffing capabilities to intercept network traffic and discover credentials.
- **CuteFTP** is an FTP client that allows the transfer of files between computers, which may have been used to upload or download data related to the user's activities.

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

A forensic image search is performed to locate the **NTUSER file. DAT**, which is located within the profile of each user on Windows systems. This file stores personal settings, user preferences, activity history, and other important data that can be key in a forensic investigation.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | grep -i 'ntuser.dat'
r/r 7324-128-4: Documents and Settings/Default User/NTUSER.DAT
r/r 391-128-4:  Documents and Settings/LocalService/NTUSER.DAT
r/r 418-128-4:  Documents and Settings/LocalService/ntuser.dat.LOG
r/r 345-128-4:  Documents and Settings/Mr. Evil/NTUSER.DAT
r/r 9798-128-4: Documents and Settings/Mr. Evil/ntuser.dat.LOG
r/r 350-128-4:  Documents and Settings/NetworkService/NTUSER.DAT
r/r 377-128-4:  Documents and Settings/NetworkService/ntuser.dat.LOG
r/r 9746-128-4: WINDOWS/repair/ntuser.dat
```


Once the file corresponding to the user **Mr. Evil** has been identified, its contents are extracted with forensic tools, such as icat, for detailed analysis. Subsequently, a search for **email address patterns** within the file is performed using regular expressions or commands such as egrep.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ strings  NTUSER_Evil.DAT | grep -iP '\b^[\w\.-]+@([\w-]+\.)+[\w-]{2,4}\b
pipe quote>
pipe quote>

┌──(kali㉿kali)-[~/hacking_case]
└─$ strings  NTUSER_Evil.DAT | grep -iP "\b^[\w\.-]+@([\w-]+\.)+[\w-]{2,4}\b"


whoknowsme@sbcglobal.net
xe@shdoclc.dll,-866
Look@LAN.lnk
Look@LAN.lnk
Look@LAN.lnk
```

This process allowed us to identify possible email accounts associated with the user, which can be used to track online activities, correspondence, or links to other systems.

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

With the **previously identified software** registry file, the uninstall **add-on** of the RegRipper package is used to list the programs that have been uninstalled or installed on the system. This information allows us to identify that the machine had network adapters such as the **Compaq WL110 Wireless LAN PC Card** and the **Xircom CardBus Ethernet**, useful information to know the connection capabilities of the system.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ rip.pl -r software  -p uninstall

Launching uninstall v.20200525
uninstall v.20200525
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT hives

2004-08-20 15:08:19Z
  Forté Agent

2004-08-19 22:31:51Z
  AddressBook
  ICW
  OutlookExpress
```

A specific search for the **Forte Agent** app, a newsreader, and email is then performed, using keywords such as "forte" or "agent" to track its presence in the system. As a result, the AGENT file is identified**. INI** with **inode 11406**, which contains key program settings.


```
┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | grep -i "forte"


┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | grep -i "agent" | head

r/r 10064-128-1:        Documents and Settings/Mr. Evil/Desktop/Tools/Agent.lnk
r/r 10065-128-4:        Documents and Settings/Mr. Evil/Start Menu/Programs/Agent Newsreader/Agent Help.
lnk
r/r 10066-128-1:        Documents and Settings/Mr. Evil/Start Menu/Programs/Agent Newsreader/Readme.lnk
r/r 10210-128-3:        My Documents/ARCHIVE/Arj/AGENTS.TXT
r/r 10055-128-3:        Program Files/Agent/8859-1.cod
r/r 10057-128-3:        Program Files/Agent/8859-15.cod
r/r 10056-128-3:        Program Files/Agent/8859-1w.cod
r/r 10013-128-3:        Program Files/Agent/agent.cnt
r/r 10009-128-3:        Program Files/Agent/agent.exe
r/r 10012-128-3:        Program Files/Agent/agent.hlp
```

From this file, the configuration of the news server used by Forte Agent is examined, in order to collect evidence about sources of information, communications or discussion groups that the user may have accessed.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | grep -i "Program Files/Agent/"

r/r 10055-128-3:        Program Files/Agent/8859-1.cod
r/r 10057-128-3:        Program Files/Agent/8859-15.cod
r/r 10056-128-3:        Program Files/Agent/8859-1w.cod
r/r 10013-128-3:        Program Files/Agent/agent.cnt
r/r 10009-128-3:        Program Files/Agent/agent.exe
r/r 10012-128-3:        Program Files/Agent/agent.hlp
r/r 10016-128-3:        Program Files/Agent/All_COD/8859-1.cod
r/r 10017-128-3:        Program Files/Agent/All_COD/8859-10.cod
r/r 10018-128-3:        Program Files/Agent/All_COD/8859-11.cod
r/r 10019-128-3:        Program Files/Agent/All_COD/8859-13.cod
r/r 10020-128-3:        Program Files/Agent/All_COD/8859-14.cod
r/r 10021-128-3:        Program Files/Agent/All_COD/8859-15.cod
r/r 10022-128-3:        Program Files/Agent/All_COD/8859-1w.cod
r/r 10023-128-3:        Program Files/Agent/All_COD/8859-2.cod
r/r 10024-128-3:        Program Files/Agent/All_COD/8859-3.cod
r/r 10025-128-3:        Program Files/Agent/All_COD/8859-4.cod
r/r 10026-128-3:        Program Files/Agent/All_COD/8859-5.cod
r/r 10027-128-3:        Program Files/Agent/All_COD/8859-6.cod
r/r 10028-128-3:        Program Files/Agent/All_COD/8859-7.cod
r/r 10029-128-3:        Program Files/Agent/All_COD/8859-8.cod
r/r 10030-128-3:        Program Files/Agent/All_COD/8859-9.cod
r/r 11786-128-3:        Program Files/Agent/Data/00000152.DAT
r/r 11787-128-3:        Program Files/Agent/Data/00000152.IDX
r/r 11788-128-3:        Program Files/Agent/Data/00000157.DAT
r/r 11789-128-3:        Program Files/Agent/Data/00000157.IDX
r/r 11790-128-3:        Program Files/Agent/Data/00000158.DAT
r/r 11791-128-3:        Program Files/Agent/Data/00000158.IDX
r/r 11792-128-3:        Program Files/Agent/Data/000004AF.DAT
r/r 11793-128-3:        Program Files/Agent/Data/000004AF.IDX
r/r 11794-128-3:        Program Files/Agent/Data/000004B0.DAT
r/r 11795-128-3:        Program Files/Agent/Data/000004B0.IDX
r/r 11796-128-3:        Program Files/Agent/Data/000004B1.DAT
r/r 11797-128-3:        Program Files/Agent/Data/000004B1.IDX
r/r 11798-128-3:        Program Files/Agent/Data/00000D28.DAT
r/r 11799-128-3:        Program Files/Agent/Data/00000D28.IDX
r/r 11415-128-3:        Program Files/Agent/Data/0000168F.DAT
r/r 11730-128-3:        Program Files/Agent/Data/0000168F.IDX
r/r 11731-128-3:        Program Files/Agent/Data/0000169B.DAT
r/r 11732-128-3:        Program Files/Agent/Data/0000169B.IDX
r/r 11406-128-4:        Program Files/Agent/Data/AGENT.INI
r/r 11416-128-1:        Program Files/Agent/Data/errorlog.txt
r/r 11420-128-1:        Program Files/Agent/Data/FILTERS.DAT
r/r 11423-128-1:        Program Files/Agent/Data/FILTERS.IDX
r/r 11727-128-3:        Program Files/Agent/Data/GROUPS.DAT
r/r 11728-128-3:        Program Files/Agent/Data/GROUPS.IDX
```

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ icat -o 63 SCHARDT.dd 11406 | more

;AGENT.INI
;
;For information about the settings in this file,
;search for AGENT.INI in the online help.

[Profile]
Build="32.560"
FullName="Mr Evil"
EMailAddress="whoknowsme@sbcglobal.net"
EMailAddressFormat=0
ReplyTo=""
Organization="N/A"
DoAuthorization=1
SavePassword=1
UserName="whoknowsme@sbcglobal.net"
Password="84106D94696F"
SMTPLoginProtocol=2
SMTPUsePOPLogin=0
SMTPUserName="whoknowsme@sbcglobal.net"
SMTPSavePassword=1
SMTPPassword="84106D94696F"
IsRegistered=0
IsRegistered19=0
IsLicensed=3
Key=""
EnableSupportMenu=0

[Servers]
NewsServer="news.dallas.sbcglobal.net"
MailServer="smtp.sbcglobal.net"
POPServer=""
NNTPPort=119
SMTPPort=25
POPPort=110
SMTPServerPort=25
```

Subsequently, files related to **Outlook Express**, another mail and news client, are listed, which provides a second way to analyze possible user activities in messaging services or newsgroups.

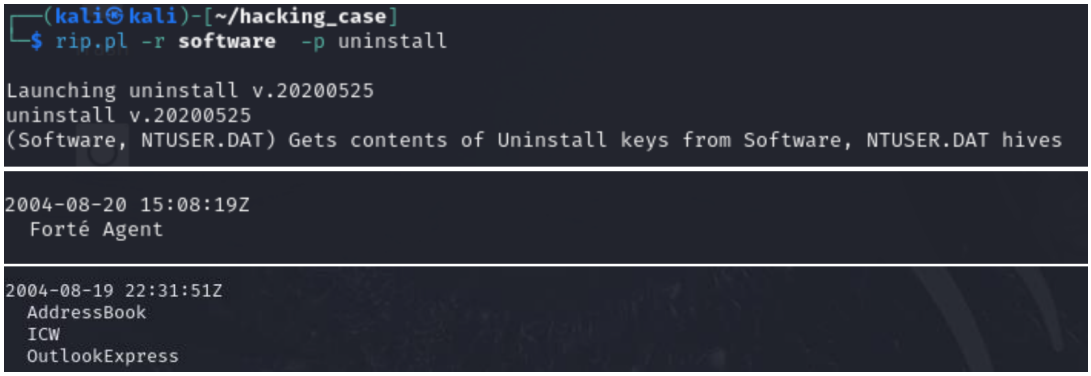
```
┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | grep -i "outlook"

r/r 11431-128-3:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/cleanup.log
r/r 11443-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.cardz.dbx
r/r 11444-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.codez.dbx
r/r 11445-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.crackz.dbx
r/r 11442-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.dbx
r/r 11539-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.hackerz.dbx
r/r 11446-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.moderated.dbx
r/r 11536-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.phreakz.dbx
r/r 11523-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.programz.dbx
r/r 11505-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.binaries.hacking.beginner.dbx
r/r 11457-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.binaries.hacking.computers.dbx
r/r 11447-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.binaries.hacking.utilities.dbx
r/r 11458-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.binaries.hacking.websites.dbx
r/r 11459-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.dss.hack.dbx
r/r 11516-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.hacking.dbx
r/r 11452-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.nl.binaries.hack.dbx
r/r 11448-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF08
6998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.stupidity.hackers.malicious.dbx
```

Finally, the **news server** configured on the system, identified as news.dallas.sbcglobal.net, is specifically searched within files with **a .dbx** extension, which are used by Outlook Express to store messages and configurations. This analysis helps to better understand the external sources with which the user interacted.


```
┌──(kali㉿kali)-[~/hacking_case]
└─$ strings "/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086
998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/alt.2600.cardz.dbx" | grep -i "news.dallas.sb
cglobal.net" | head
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
news.dallas.sbcglobal.net
```

19. What two installed programs show this information?

With the previously identified **software** file, the **RegRipper** uninstall **add-on is used** to obtain a list of programs installed on the system. From this list, drivers or tools related to network cards are identified.



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

    To identify the newsgroups to which the user "Mr. Evil" was subscribed, the directory corresponding to his profile was accessed within the set up system. Specifically, the path /mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express/ was explored, where the .dbx files used by Outlook Express to save information from emails and newsgroup subscriptions are stored. Using analysis tools such as strings and grep, text strings contained in these files were extracted to identify the names of the newsgroups.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ ls '/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Application
 Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Exp
ress/'

 alt.2600.cardz.dbx
 alt.2600.codez.dbx
 alt.2600.crackz.dbx
 alt.2600.dbx
 alt.2600.hackerz.dbx
 alt.2600.moderated.dbx
 alt.2600.phreakz.dbx
 alt.2600.programz.dbx
 alt.binaries.hacking.beginner.dbx
 alt.binaries.hacking.computers.dbx
 alt.binaries.hacking.utilities.dbx
 alt.binaries.hacking.websites.dbx
 alt.dss.hack.dbx
 alt.hacking.dbx
 alt.nl.binaries.hack.dbx
 alt.stupidity.hackers.malicious.dbx
 cleanup.log
'Deleted Items.dbx'
 Folders.dbx
 free.binaries.hackers.malicious.dbx
 free.binaries.hacking.beginner.dbx
 free.binaries.hacking.computers.dbx
 free.binaries.hacking.talentless.troll-haven.dbx
 free.binaries.hacking.talentless.troll_haven.dbx
 free.binaries.hacking.utilities.dbx
 free.binaries.hacking.websites.dbx
 Inbox.dbx
 Offline.dbx
 Outbox.dbx
```


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?

    The fls -rF -o 63 SCHARDT.dd | grep -i 'mirc' command is used to recursively search for all mIRC-related files and folders within the SCHARDT.dd forensic image, specifically on the partition with offset 63. This command allows you to locate the path and inode of the mirc.ini file, which contains the user's settings, including their name, IRC server, and active channels when logged in, which answers the question about the user's settings while online and participating in a chat channel.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | grep -i 'mirc'
r/r 10087-128-4:        Documents and Settings/All Users/Start Menu/Programs/mIRC/IRC Intro.l
nk
r/r 10086-128-4:        Documents and Settings/All Users/Start Menu/Programs/mIRC/mIRC Help.l
nk
r/r 10088-128-4:        Documents and Settings/All Users/Start Menu/Programs/mIRC/Readme.txt.
lnk
r/r 10089-128-4:        Documents and Settings/All Users/Start Menu/Programs/mIRC/Versions.tx
t.lnk
r/r 10085-128-1:        Documents and Settings/Mr. Evil/Desktop/Tools/mIRC.lnk
r/r 10081-128-1:        Program Files/mIRC/aliases.ini
r/r 11072-128-6:        Program Files/mIRC/channels/channels.txt
r/r 10077-128-3:        Program Files/mIRC/ircintro.hlp
r/r 11315-128-4:        Program Files/mIRC/logs/#Chataholics.UnderNet.log
r/r 11316-128-4:        Program Files/mIRC/logs/#CyberCafe.UnderNet.log
r/r 11276-128-1:        Program Files/mIRC/logs/#Elite.Hackers.UnderNet.log
r/r 11074-128-1:        Program Files/mIRC/logs/#evilfork.EFnet.log
r/r 11401-128-1:        Program Files/mIRC/logs/#funny.UnderNet.log
r/r 11306-128-1:        Program Files/mIRC/logs/#houston.UnderNet.log
r/r 11073-128-1:        Program Files/mIRC/logs/#ISO-WAREZ.EFnet.log
r/r 11272-128-4:        Program Files/mIRC/logs/#LuxShell.UnderNet.log
r/r 11273-128-4:        Program Files/mIRC/logs/#mp3xserv.UnderNet.log
r/r 11327-128-4:        Program Files/mIRC/logs/#thedarktower.AfterNET.log
r/r 11275-128-1:        Program Files/mIRC/logs/#ushells.UnderNet.log
r/r 11317-128-1:        Program Files/mIRC/logs/m5tar.UnderNet.log
r/r 10074-128-6:        Program Files/mIRC/mirc.exe
r/r 10073-128-3:        Program Files/mIRC/mirc.hlp
r/r 10080-128-3:        Program Files/mIRC/mirc.ini
r/r 10082-128-3:        Program Files/mIRC/popups.ini
r/r 10078-128-3:        Program Files/mIRC/readme.txt
r/r 10083-128-3:        Program Files/mIRC/servers.ini
r/r 10084-128-5:        Program Files/mIRC/urls.ini
r/r 10079-128-3:        Program Files/mIRC/versions.txt
r/r 11071-128-4:        WINDOWS/Prefetch/MIRC.EXE-0661EC22.pf
r/r 10090-128-4:        WINDOWS/Prefetch/MIRC612.EXE-02791C37.pf
```


Observe the mirc.ini file with the inode 10080. Search for the most importan configuration.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ icat -o 63 SCHARDT.dd 10080 | grep -iE 'user|email|log|ip|server'
n46=#mIRCScripts
n75=#UserGuide,"The official Undernet help channel"
n76=#UserHelp
accept=*.bmp,*.gif,*.jpg,*.log,*.mid,*.mp3,*.png,*.txt,*.wav,*.wma,*.zip
logdir=logs\
userid=Mrevil
useip=yes
status=/lusers
ServerStatus=on
[fileserver]
[dccserver]
user=Mini Me
email=none@of.ya
host=Undernet: US, CA, LosAngelesSERVER:losangeles.ca.us.undernet.org:6660GROUP:Undernet
servers=servers.ini
```

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

    The channels accessed by the user of this computer are searched.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | grep -i 'Program Files/mIRC/logs'

r/r 11315-128-4:        Program Files/mIRC/logs/#Chataholics.UnderNet.log
r/r 11316-128-4:        Program Files/mIRC/logs/#CyberCafe.UnderNet.log
r/r 11276-128-1:        Program Files/mIRC/logs/#Elite.Hackers.UnderNet.log
r/r 11074-128-1:        Program Files/mIRC/logs/#evilfork.EFnet.log
r/r 11401-128-1:        Program Files/mIRC/logs/#funny.UnderNet.log
r/r 11306-128-1:        Program Files/mIRC/logs/#houston.UnderNet.log
r/r 11073-128-1:        Program Files/mIRC/logs/#ISO-WAREZ.EFnet.log
r/r 11272-128-4:        Program Files/mIRC/logs/#LuxShell.UnderNet.log
r/r 11273-128-4:        Program Files/mIRC/logs/#mp3xserv.UnderNet.log
r/r 11327-128-4:        Program Files/mIRC/logs/#thedarktower.AfterNET.log
r/r 11275-128-1:        Program Files/mIRC/logs/#ushells.UnderNet.log
r/r 11317-128-1:        Program Files/mIRC/logs/m5tar.UnderNet.log
```

o Ushells.undernet.logo Elite.hackers.undernet.log o Mp3xserv.undernet.logo Chataholics.undernet.log o Cybercafé.undernet.logo M5tar.undernet.logo Thedarktower.afternet.log o Funny.undernet.logo Luxshell.undernet.logo Evilfork.efnet.logo Iso-warez.efnet.logo Houston.undernet.log

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?

To answer question 23 about the file containing the data intercepted by **Ethereal**, a popular network analysis program (sniffer), the following commands are used:

- ***ls /mnt/loop/Documents\ and\ Settings/Mr.\ Evil***
- ***file /mnt/loop/Documents\ and\ Settings/Mr.\ Evil/interception***.

These commands allow you to examine the contents of the "Mr. Evil" user's home directory, specifically his documents folder, which is the default place where Ethereal saves captured and reassembled TCP packets in .pcap files. By listing the files and verifying their type, it is possible to identify which one contains the intercepted data, thus fulfilling the objective of finding evidence of the espionage activity on the network carried out by this user.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ ls /mnt/loop/Documents\ and\ Settings/Mr.\ Evil
'Application Data'   interception      NTUSER.DAT      Recent
 Cookies            'Local Settings'   ntuser.dat.LOG  SendTo
 Desktop            'My Documents'     ntuser.ini     'Start Menu'
 Favorites           NetHood           PrintHood       Templates

┌──(kali㉿kali)-[~/hacking_case]
└─$ file /mnt/loop/Documents\ and\ Settings/Mr.\ Evil/interception

/mnt/loop/Documents and Settings/Mr. Evil/interception: pcap capture file, microsecond ts (li
ttle-endian) - version 2.4 (Ethernet, capture length 65535)

┌──(kali㉿kali)-[~/hacking_case]
└─$ 
```

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?

To analyze the capture file generated by the Ethereal program and determine what type of wireless device the person whose internet browsing was intercepted was using, the following command was used:

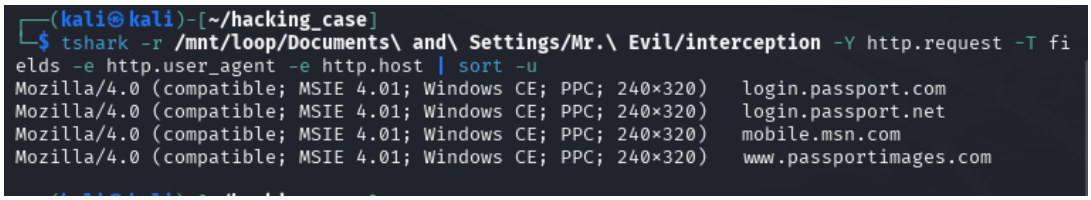
tshark -r /mnt/loop/Documents\ and\ Settings/Mr.\ Evil/interception -Y http.request -T fields -e http.user_agent -e http.host

This command uses **TShark**, the command-line version of Wireshark, to read the capture file (interception) and **filter only the HTTP requests made**, specifically extracting two fields: the **user agent** (browser or device used) and the **target host**. When reviewing the results, a string corresponding to the Windows CE operating system **(Pocket PC)** was identified within the http.user_agent field. This indicates that the victim whose browsing was recorded was using a wireless computer based on **Windows CE,** a common operating system on mobile devices such as PDAs or Pocket PCs, which allows the type of equipment used at the time of the interception to be concluded.

```
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   www.passportimages.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   login.passport.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   login.passport.net
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   login.passport.net
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   login.passport.net
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   login.passport.net
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   login.passport.net
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   www.passportimages.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   www.passportimages.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)   www.passportimages.com
```

25. What websites was the victim accessing?

    To identify the websites that the victim user was visiting, the tshark tool was used to analyze the network capture file called interception. The command executed was ***tshark -r /mnt/loop/Documents\ and\ Settings/Mr.\ Evil/interception -Y http.request -T fields -e http.user_agent -e http.host | sort -u***, which filters the HTTP packets within the file and extracts the http.user_agent and http.host fields to display only the unique data related to the web requests. When executing this command, it was observed that the user accessed the **mobile.msn.com** and **MSN (Hotmail) Email** sites, which shows that email services were used through a mobile platform during the capture of the traffic.



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

    To find the primary user's web-based email address, a search was performed within the personal directory of "Mr. Evil". When examining the contents of the stored files, the mrevilrulez@yahoo.com email address was identified. This address appears in files related to user activity, indicating that it was used to access online email services. This information is relevant within forensic analysis, as it allows links to be established between the user and their possible communications or activities on the network.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ grep -EiorhI '\b[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,6}\b' '/mnt/loop/Documents a
nd Settings/Mr. Evil/'

mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mailbot@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
nightwolf@confine.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
seabach@shaw.ca
NOSPAM-fred@wardriving.com
jim@mcmahon.cc
jim@mcmahon.cc
hacked@2600.com
webmaster@2600.com
you@your-name.com
LmT@marijuana.com
chris@splitinfinity.com
NOSPAM-fred@wardriving.com
123@123.com
info@mosnews.com
info@mosnews.com
Rating@Mail.ru
drudge@drudgereport.com
DRUDGE@DRUDGEREPORT.COM
T50admin@usa.net
jim@mcmahon.cc
chillen@hoo.com
img4i0lqhsh6n7hlqth96lfd5jd1acjrh9@4ax.com
beatnik@mail.gr
teandson@aol.com
9a64i0p9vk73bpmnq4s40iq6asem5k80er@4ax.com
corenode01a@yahoo.removethisfirst.com
mrevilrulez@yahoo.com
mrevilrulez@yahoo.com
```

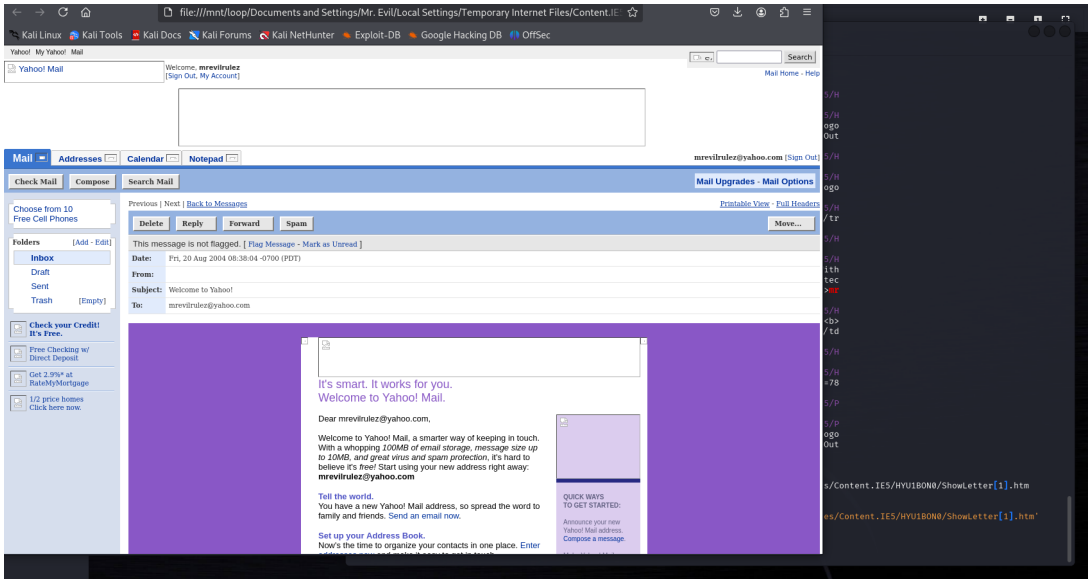
```
cathomas@msn.com
mauddib@dune.com
dqbug010mo29ufsbo4dq491vvihucqfh69@4ax.com
heyjude18@hotmail.com ... as
hp01@mailadded.com
logaritmo50@yahoo.com
logaritmo50@hotmail.com
PASSADMINBOT@HOTMAIL.COM
HERE@HOTMAIL.COM
PASSCODE@HOTMAIL.COM
slim532@hotmail.com
248e504e.0408150655.a30aac9@posting.google.com
PASSADMINBOT@HOTMAIL.COM
HERE@HOTMAIL.COM
PASSCODE@HOTMAIL.COM
slim532@hotmail.com
248e504e.0408150655.a30aac9@posting.google.com
PASSADMINBOT@HOTMAIL.COM
HERE@HOTMAIL.COM
PASSCODE@HOTMAIL.COM
suckme@oyea.lick
president@whitehouse.gov
tmt3i0tnq18gm819ecv27r73vm6hnoddcn@4ax.com
suckme@oyea.lick
info@mosnews.com
info@mosnews.com
Rating@Mail.ru
webmaster@2600.com
webmaster@2600.com
NOSPAM-fred@wardriving.com
frisco@blackant.net
jim@mcmahon.cc
jfoster3@ec.rr.com
tH1.10237466@twister.southeast.rr.com
mikelee@yahoo-inc.com
info@mosnews.com
info@mosnews.com
Rating@Mail.ru
```

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ grep -EiorhI "([[:alnum:]_.-]+@[[:alnum:]_.-]+?\.[[:alpha:].]{2,6})" "/mnt/loop/Documents and Setting
s/Mr. Evil/" | sort | uniq -c | sort -nr
     12 mrevilrulez@yahoo.com
      6 info@mosnews.com
      4 jim@mcmahon.cc
      3 webmaster@2600.com
      3 --Rating@Mail.ru
      3 PASSCODE@HOTMAIL.COM
      3 PASSADMINBOT@HOTMAIL.COM
      3 NOSPAM-fred@wardriving.com
      3 HERE@HOTMAIL.COM
      2 suckme@oyea.lick
      2 slim532@hotmail.com
      2 248e504e.0408150655.a30aac9@posting.google.com
      1 you@your-name.com
      1 tmt3i0tnq18gm819ecv27r73vm6hnoddcn@4ax.com
      1 tH1.10237466@twister.southeast.rr.com
      1 teandson@aol.com
      1 T50admin@usa.net
      1 seabach@shaw.ca
      1 president@whitehouse.gov
      1 nightwolf@confine.com
```


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

To determine under which file name Yahoo Mail stores copies of the emails, a search was performed in the personal directory of "Mr. Evil" using the previously identified email address. When searching for files containing this address, it was found that Yahoo Mail stores copies of emails in a file called **Showletter[1].htm**. This finding allows us to understand how email messages are organized and stored in the system, which is useful for analyzing user activity and retrieving relevant information during the investigation.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ grep -ir 'mrevilrulez@yahoo.com' '/mnt/loop/Documents and Settings/Mr. Evil/'

/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/H
YU1BON0/ShowFolder[1].htm:Yahoo! Mail - mrevilrulez@yahoo.com</title>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/H
YU1BON0/ShowFolder[1].htm:                          <b>mrevilrulez@yahoo.com</b> [<a href="/ym/Logo
ut?YY=60138&.first=1&inc=25&order=down&sort=date&pos=0&view=&head=&box=Inbox&YY=60138">Sign Out
</a>]
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/H
YU1BON0/ShowLetter[1].htm:Yahoo! Mail - mrevilrulez@yahoo.com</title>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/H
YU1BON0/ShowLetter[1].htm:                          <b>mrevilrulez@yahoo.com</b> [<a href="/ym/Logo
ut?YY=90802&.first=1&order=down&sort=date&pos=0&YY=90802">Sign Out</a>]
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/H
YU1BON0/ShowLetter[1].htm:<tr><td class=label nowrap>To:</td><td>mrevilrulez@yahoo.com</td></tr
>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/H
YU1BON0/ShowLetter[1].htm:      <br>Dear mrevilrulez@yahoo.com,<br><br>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/H
YU1BON0/ShowLetter[1].htm:      Welcome to Yahoo! Mail, a smarter way of keeping in touch. With
 a whopping <i>100MB of email storage, message size up to 10MB, and great virus and spam protec
tion</i>, it's hard to believe it's <i>free!</i> Start using your new address right away: <b>mr
evilrulez@yahoo.com</b></font>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/H
YU1BON0/last[1].htm:<tr><td colspan=2 align=left><font face="Arial" size=-1 color="#646464"><b>
Your New Yahoo! Mail Address: <font color="#000000">mrevilrulez@yahoo.com</font></b></font></td
></tr>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/H
YU1BON0/login[1].htm:Yahoo! Mail - mrevilrulez@yahoo.com</title>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/H
YU1BON0/login[1].htm:                    <b>mrevilrulez@yahoo.com</b> [<a href="/ym/Logout?YY=78
169&.first=1&YY=78169">Sign Out</a>]
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/P
N0J7OQM/ShowLetter[1].htm:Yahoo! Mail - mrevilrulez@yahoo.com</title>
/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/P
N0J7OQM/ShowLetter[1].htm:                          <b>mrevilrulez@yahoo.com</b> [<a href="/ym/Logo
ut?YY=27630&.first=1&inc=25&order=down&sort=date&pos=0&view=&head=&box=Inbox&YY=27630">Sign Out
</a>]
```



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

To determine how many executable files are in the recycle bin, the contents of the specific directory where Windows stores the identified user's deleted files are listed. The ls command ***'/mnt/loop/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003'*** displays all the files present in that recycle bin folder. By reviewing this list, 4 executable files can be identified and counted, usually with extensions such as .exe


```
┌──(kali㉿kali)-[~/hacking_case]
└─$ firefox '/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BON0/ShowLetter[1].htm'

┌──(kali㉿kali)-[~/hacking_case]
└─$ ls '/mnt/loop/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003'

Dc1.exe  Dc2.exe  Dc3.exe  Dc4.exe  desktop.ini  INFO2

┌──(kali㉿kali)-[~/hacking_case]
└─$ ls  -l '/mnt/loop/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003'

total 12103
-rwxrwxrwx 1 root root 2160043 Aug 25  2004 Dc1.exe
-rwxrwxrwx 1 root root 1324940 Aug 27  2004 Dc2.exe
-rwxrwxrwx 1 root root  442417 Aug 27  2004 Dc3.exe
-rwxrwxrwx 1 root root 8460502 Aug 27  2004 Dc4.exe
-rwxrwxrwx 1 root root      65 Aug 25  2004 desktop.ini
-rwxrwxrwx 1 root root    3220 Aug 27  2004 INFO2
```

29. Are these files really deleted?

No, it is possible to recover them using rifiuti2, it will be installed.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ sudo apt-get install rifiuti2

Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  rifiuti2
0 upgraded, 1 newly installed, 0 to remove and 1890 not upgraded.
Need to get 35.7 kB of archives.
After this operation, 136 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 rifiuti2 amd64 0.7.0-4 [35.7 kB]
Fetched 35.7 kB in 2s (22.7 kB/s)
Selecting previously unselected package rifiuti2.
(Reading database ... 395765 files and directories currently installed.)
Preparing to unpack .../rifiuti2_0.7.0-4_amd64.deb ...
Unpacking rifiuti2 (0.7.0-4) ...
Setting up rifiuti2 (0.7.0-4) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for man-db (2.12.1-2) ...
```

The installed version is verified.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ rifiuti2 -v
rifiuti2 0.7.0
rifiuti2 is distributed under the BSD 3-Clause License.
Information about rifiuti2 can be found on

        https://abelcheung.github.io/rifiuti2/
```

It is observed that now there is the INFO2 file, a hidden file created by rifiuti2 that saves the information of the deleted files.


```
┌──(kali㉿kali)-[~/hacking_case]
└─$ ls -l '/mnt/loop/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003'

total 12103
-rwxrwxrwx 1 root root 2160043 Aug 25  2004 Dc1.exe
-rwxrwxrwx 1 root root 1324940 Aug 27  2004 Dc2.exe
-rwxrwxrwx 1 root root  442417 Aug 27  2004 Dc3.exe
-rwxrwxrwx 1 root root 8460502 Aug 27  2004 Dc4.exe
-rwxrwxrwx 1 root root      65 Aug 25  2004 desktop.ini
-rwxrwxrwx 1 root root    3220 Aug 27  2004 INFO2
```

The information stored in the INFO2 file is observed.

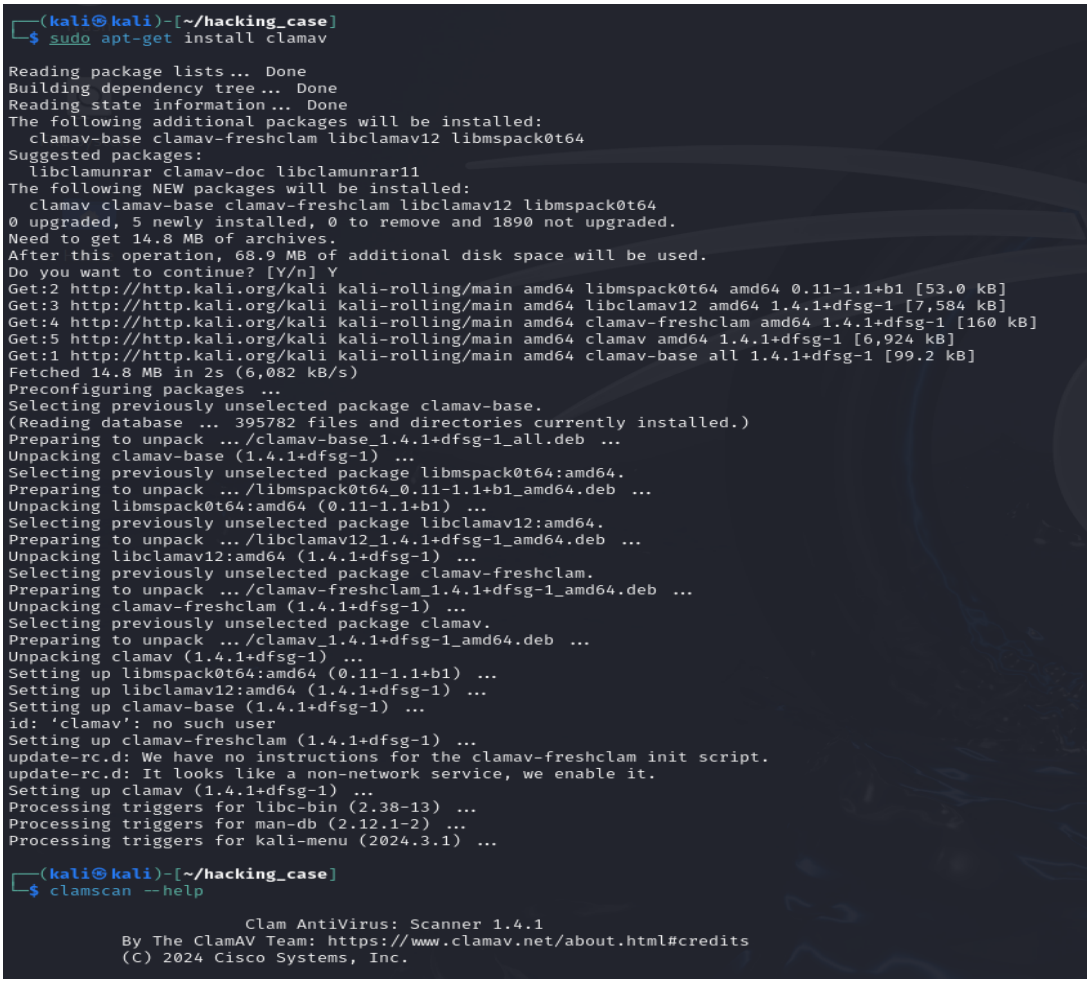
```
┌──(kali㉿kali)-[~/hacking_case]
└─$ rifiuti2 '/mnt/loop/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003/INFO2'

Recycle bin path: '/mnt/loop/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003/INFO2'
Version: 5
OS Guess: Windows XP or 2003
Time zone: Coordinated Universal Time (UTC) [+0000]

Index   Deleted Time    Gone?   Size    Path
1       2004-08-25 16:18:25     No      2160128 C:\Documents and Settings\Mr. Evil\Desktop\lalsetup250.exe
2       2004-08-27 15:12:30     No      1325056 C:\Documents and Settings\Mr. Evil\Desktop\netstumblerinstaller_0_4_0.exe
3       2004-08-27 15:15:26     No      442880  C:\Documents and Settings\Mr. Evil\Desktop\WinPcap_3_01_a.exe
4       2004-08-27 15:29:58     No      8460800 C:\Documents and Settings\Mr. Evil\Desktop\ethereal-setup-0.10.6.exe
```

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

    To determine how many files have been reported as deleted by the file system, the fls ***-rFd -o 63 SCHARDT.dd | wc -l*** command is used. The -d option with fls allows you to list only deleted files, while the recursive -r option searches all directories. The output is sent through a pipe (|) to the wc -l command, which counts the total number of lines, i.e. the total number of deleted files found. According to the result, the system reports that there are 365 deleted files. This allows you to know how many files have been deleted but could be recoverable.

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

    ClamAV is installed and the installed version is verified.



The image being studied is scanned.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ clamscan -r -i "/mnt/loop"
/mnt/loop/My Documents/COMMANDS/enum.exe: Win.Tool.EnumPlus-1 FOUND
/mnt/loop/My Documents/COMMANDS/SAMDUMP.EXE: Win.Trojan.Pwdump-2 FOUND
/mnt/loop/My Documents/COMMANDS/snitch.exe: Win.Trojan.Snitch-1 FOUND
/mnt/loop/My Documents/ENUMERATION/NT/enum/enum.tar.gz: Win.Tool.EnumPlus-1 FOUND
/mnt/loop/My Documents/ENUMERATION/NT/enum/files/enum.exe: Win.Tool.EnumPlus-1 FOUND
/mnt/loop/My Documents/ENUMERATION/NT/Legion/Chrono.dl_: Win.Trojan.Bruteforce-3 FOUND
/mnt/loop/My Documents/ENUMERATION/NT/Legion/NetTools.ex_: Win.Trojan.Spion-4 FOUND
/mnt/loop/My Documents/ENUMERATION/NT/ntreskit.zip: Win.Trojan.Nemo-1 FOUND
/mnt/loop/My Documents/EXPLOITATION/NT/Brutus/BrutusA2.exe: Win.Tool.Brutus-3 FOUND
/mnt/loop/My Documents/EXPLOITATION/NT/brutus.zip: Win.Tool.Brutus-3 FOUND
/mnt/loop/My Documents/EXPLOITATION/NT/Get Admin/GetAdmin.exe: Win.Exploit.WinNT-3 FOUND
/mnt/loop/My Documents/EXPLOITATION/NT/lsadump2/lsadump2.exe: Win.Trojan.Lsadump-1 FOUND
/mnt/loop/My Documents/EXPLOITATION/NT/lsadump2/lsadump2.zip: Win.Trojan.Lsadump-1 FOUND
/mnt/loop/My Documents/EXPLOITATION/NT/netbus/NetBus170.zip: Win.Trojan.Netbus-2 FOUND
/mnt/loop/My Documents/EXPLOITATION/NT/sechole/SECHOLE.EXE: Win.Trojan.Sehole-1 FOUND
/mnt/loop/My Documents/EXPLOITATION/NT/sechole/sechole3.zip: Win.Trojan.Sehole-1 FOUND
/mnt/loop/My Documents/FOOTPRINTING/NT/superscan/superscan.exe: Win.Trojan.Agent-6240252-0 FOUND
/mnt/loop/My Documents/FOOTPRINTING/UNIX/unix_hack.tgz: Unix.Malware.Agent-6781976-0 FOUND
/mnt/loop/Program Files/Cain/Abel.dll: Win.Trojan.Cain-9 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 8701412
Engine version: 1.4.1
Scanned directories: 766
Scanned files: 11305
Infected files: 19
Data scanned: 2214.98 MB
Data read: 1768.03 MB (ratio 1.25:1)
Time: 1846.723 sec (30 m 46 s)
Start Date: 2024:12:11 18:07:50
End Date:   2024:12:11 18:38:37
```

The listed directories and files contain malicious files or exploits, such as hacking tools, trojans, worms, and other types of malware. This suggests that this system is compromised and a complete cleanup is required to remove any threats. In short, the scan result indicates a significant infection on this system that requires immediate attention and corrective actions to remedy the security situation.

Conclusion

Upon investigation, it is concluded that the computer in question was actively used for possibly malicious activities under the alias "Mr. Evil," linked to the registered owner "Greg Schardt." The analysis showed that the Windows XP system had several hacking-related tools installed, such as Cain & Abel, Ethereal, and NetStumbler, along with programs for password recovery and network detection. Internet activity, which includes using IRC channels such as "Elite.hackers" and subscribing to hacking-focused newsgroups, suggests a deliberate intent to engage in unauthorized activities on the network. In addition, data intercepted from a Windows CE device evidences compromised online accounts, and email logs link the user to the alias "mrevilrulez." Although files were deleted, traces still remain in the file system, and the presence of viruses reinforces the hypothesis of malicious use. All of this evidence clearly links the computer and its activities to the operations attributed to Mr. Evil.